Sicherheit in Verwaltungs- und Kliniknetzen

Anforderungen
Möglichkeiten
Empfehlungen

Bericht der Arbeitsgruppe
Verwaltungen und Kliniken im Hochschulnetz

Juni 1998

Bayerisches Staatsministerium
für Unterricht, Kultus, Wissenschaft und Kunst

Soweit in dem vorliegenden Bericht technische oder rechtliche Hinweise gegeben werden, kann keine Haftung übernommen werden. Die technische und die rechtliche Situation im Bereich der Datennetze ändern sich überaus schnell und sind teilweise auch unklar. Im Hinblick auf die rechtliche Beurteilung (insbesondere die Ausgestaltung von Nutzungsordnungen und Einwilligungserklärungen) ist stets die Prüfung durch die Rechtsabteilung der Hochschule und/oder ein entsprechend spezialisiertes Anwaltsbüro unverzichtbar.

Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt.

Der Bericht ist bis auf weiteres auch in elektronischer Form über das Internet abrufbar. Näheres hierzu unter folgender WWW-Adresse:

`http://www.stmukwk.bayern.de/unifh/index.html`

Herausgeber:
Bayerisches Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst
Salvatorstraße 2, 80333 München

Juni 1998

Druck: Gruner Druck GmbH, Sonnenstraße 23b, 91058 Erlangen

Die Veröffentlichung ist auf chlorfreiem und damit umweltfreundlichem Papier gedruckt.

Geleitwort

Vor einem Jahr erschien im Rahmen dieser Schriftenreihe der Bericht einer Arbeitsgruppe, die sich mit Fragen des Zugangs zu den Datennetzen im Hochschulbereich und ihrer Nutzung sowie den damit zusammenhängenden Rechtsfragen befasst hat.[1] Der Bericht ging auch bereits darauf ein, wie man sich gegen mögliche Missbräuche der Netze und der durch sie zugänglichen Ressourcen schützen kann. Im Vordergrund standen dabei Aspekte der Forschung und Lehre. Die Sicherheit der auf Rechnern gehaltenen und zwischen ihnen übertragenen Daten sowie der angewandten Verfahren vor unberechtigtem Zugriff, Verfälschung, Zerstörung oder anderen Formen des Missbrauchs hat im Verwaltungs- und Klinikbereich der Hochschulen besondere Bedeutung. Studenten oder Patienten müssen auf die Richtigkeit der über sie geführten (Prüfungs- oder Befund-)Daten und die darauf gegründeten Verwaltungsakte oder Behandlungsverfahren vertrauen können. Außerdem sind im Falle personenbezogener Daten die Persönlichkeitsrechte der Betroffenen zu wahren.

Wegen der Verflechtung der wissenschaftlichen Aufgaben mit den Verwaltungsaufgaben und aus wirtschaftlichen Gründen lassen sich die Verwaltungs- und Kliniknetze nicht getrennt von der allgemeinen Netzinfrastruktur einer Hochschule realisieren. Im Übrigen benötigen Hochschulverwaltungen und -kliniken zur Erfüllung ihrer Aufgaben in zunehmendem Maße auch Zugang zu öffentlichen Netzen. Diese notwendige Offenheit ist mit der gebotenen informations- und kommunikationstechnischen Sicherheit und den Zielen des Datenschutzes nur schwer zu vereinbaren. Für die einzelne Hochschule oder Klinik ist es keine leichte Aufgabe, einen gangbaren Weg zu finden.

Deshalb habe ich veranlasst, dass eine Gruppe von Fachleuten aus Wissenschaft und Verwaltung, Kliniken und Rechenzentren bayerischer Hochschulen beauftragt wurde, die speziellen Anforderungen von Hochschul- und Klinikverwaltungen an die Netz- und Systemsicherheit zu untersuchen, Lösungsmöglichkeiten aufzuzeigen und Empfehlungen nebst Hinweisen auf den erforderlichen Aufwand und die einzusetzenden Hilfsmittel zu geben. Dankenswerterweise konnte auch auf die im Rahmen des BayernOnline-Projekts BASILIKA gewonnenen Erkenntnisse und auf den Sachverstand des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zurückgegriffen werden.

[1] Hochschulnetze in Bayern, Bericht der Arbeitsgruppe Zugangs- und Nutzungsregelungen für die bayerischen Hochschulnetze, Februar 1997

Der vorliegende Bericht ist das Ergebnis intensiver zweijähriger Bemühungen dieser Arbeitsgruppe. Er stellt dar, wie nach derzeitigem Stand die Netze und informationsverarbeitenden Systeme in den Hochschulverwaltungen und -kliniken bei wünschenswerter und notwendiger Integration in die allgemeine Netzinfrastruktur auf einem angemessenen Sicherheitsniveau betrieben werden können. Möge der Bericht den Entscheidungsträgern der Hochschulen und den mit der Umsetzung der Maßnahmen befassten Personen gute Dienste leisten. Ich danke allen, die der Arbeitsgruppe angehört haben oder in anderer Weise dazu beitrugen, dass dieser Bericht zustandekam.

(Hans Zehetmair)

Bayerischer Staatsminister
für Unterricht, Kultus,
Wissenschaft und Kunst

Stellv. Ministerpräsident

Inhaltsverzeichnis

Einleitung

Ausgangslage

Während die Informationstechnik (IT) in den Hochschulverwaltungen und Universitätskliniken noch in den achtziger Jahren von Zentralrechnern geprägt war, auf denen wenige Sachbearbeiter über sternförmig vernetzte Dialogterminals mit einem begrenzten Spektrum von DV-Anwendungen arbeiteten, hat sich die Situation in den vergangenen Jahren grundlegend gewandelt: Die Mitarbeiter in den Verwaltungen und Kliniken sind nahezu flächendeckend mit Arbeitsplatzrechnern ausgestattet, die als Clients auf verschiedene Server zugreifen und dort verwaltungs- bzw. klinikspezifische DV-Dienste oder aber allgemeine Informations- und Kommunikationsdienste in Anspruch nehmen sollen. Dazu müssen die Arbeitsplatzrechner und Server offensichtlich in ein Netz integriert sein, über das die gewünschten Kommunikationsbeziehungen hergestellt werden können.

Angesichts der besonderen Anforderungen an die Datensicherheit und den Datenschutz für die in diesem Bereich anfallenden Daten (Patienten- und Befunddaten, Studenten- und Prüfungsdaten, etc.) könnte es auf den ersten Blick naheliegend erscheinen, hierfür ein separates, von der übrigen Netzinfrastruktur der Hochschule völlig getrenntes Verwaltungs- bzw. Kliniknetz zu betreiben. Bei näherer Betrachtung erweist sich dieser Weg jedoch aus einer Vielzahl von Gründen als wenig praktikabel:

- Für zahlreiche Mitarbeiter in Hochschulverwaltungen und Universitätskliniken ist die Nutzung von Informations- und Kommunikationsdiensten (vor allem WorldWideWeb und Electronic Mail) mit Partnern im offenen Hochschulnetz und im weltweiten Internet unverzichtbar.
- Im Zuge einer Dezentralisierung von Verwaltungsvorgängen (z.B. Mittelbewirtschaftung durch die Dekanate der Fakultäten und die Zentralen Einrichtungen, Mitwirkung an der Prüfungsverwaltung durch die Fakultäten) sind in steigendem Maße Mitarbeiter außerhalb der Hochschulverwaltung in DV-Verfahren der Verwaltung involviert und müssen deshalb Zugriffsrechte auf Server, Applikationen und Daten der Verwaltung erhalten.
- Unter dem Aspekt der Ausweitung des Dienstleistungsangebots, aber auch der Ausschöpfung möglichen Rationalisierungspotentials werden Verwaltungsanwendungen zunehmend für Selbstbedienungsfunktionen (wie z.B. Rückmeldeverfahren in der Studentenverwaltung, Auskünfte über die zur eigenen Person gespeicherten

Daten) geöffnet. Dazu muss von öffentlich zugänglichen Arbeitsplatzrechnern aus auf Server und Daten der Verwaltung zugegriffen werden können.

- Nicht selten ist eine Hochschulverwaltung bzw. Universitätsklinik auf mehrere Gebäude oder gar auf verschiedene Standorte verteilt. Für den Zusammenschluss der dadurch gegebenen Netzinseln zu einem Gesamtnetz bieten sich schon aus ökonomischen Gründen die in der Regel bereits vorhandenen Netzverbindungen des offenen Hochschulnetzes und des deutschen Wissenschaftsnetzes (WiN) an.

Da also einerseits eine Anbindung von Verwaltungs- und Kliniknetzen an die offene Netzinfrastruktur der Hochschulen und damit an das weltweite Internet zur effizienten Erfüllung der anstehenden Aufgaben und darüber hinaus aus Gründen der Wirtschaftlichkeit unumgänglich ist und andererseits die Gewährleistung der Vertraulichkeit und Integrität von Daten bei ihrer Speicherung und Übertragung, die Verfügbarkeit von IT-Systemen und -Diensten sowie die Ordnungsmäßigkeit und Nachweisbarkeit der Nutzung der IT in Verwaltungs- und Kliniknetzen einen hohen Stellenwert besitzen, ergeben sich besondere Anforderungen an die IT-Sicherheit des Gesamtsystems.

Auftrag an die Arbeitsgruppe und Zielsetzung des Arbeitsberichts

Zur Behandlung dieses Problemkreises wurde im März 1996 vom Bayerischen Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst eine Arbeitsgruppe mit Fachleuten aus Wissenschaft, Rechenzentren, Verwaltungen und Kliniken bayerischer Hochschulen sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eingesetzt und gebeten, eine mögliche Netztrennung durch die Bildung Virtueller Privater Netze (VPN), die Netzabsicherung durch Firewalls sowie die Verschlüsselung vertraulicher und sensibler Daten zu erörtern und weitergehende Überlegungen zu Zugangs- und Zugriffskontrollen innerhalb des Klinik- bzw. Verwaltungssubnetzes, zu organisatorischen und administrativen Maßnahmen zur Verbesserung der IT-Sicherheit sowie zu Fragen der Netzüberwachung und des System- und Netzmanagements anzustellen.

Nach intensiven Beratungen legt diese Arbeitsgruppe nunmehr ihren Abschlussbericht vor. Sie möchte damit

- konkrete, unmittelbar in die Praxis umsetzbare Empfehlungen zur Verbesserung der IT-Sicherheit geben,
- das Wissen über grundlegende Bestandteile von IT-Sicherheitslösungen wie Firewall-Systeme, Verschlüsselung, gesicherte Basisdienste und Betriebssystemfunktionen, Zugangs- und Zugriffskontrolle oder Sicherheitsmanagement durch eine ausführliche Darstellung vertiefen sowie

- das Projekt BASILIKA („Bayerische Sicherheitslösung für Dienstangebote in offenen Kommunikationsnetzen“) als integrierenden, umfassenden Lösungsansatz für IT-Sicherheit vorstellen.

Angesichts der rasanten technologischen Entwicklung in diesem Bereich können dabei die Aussagen insbesondere zu konkreten Sicherheitstools und -prozeduren allenfalls als Beschreibung der momentanen Situation gewertet werden.

Übersicht über den Bericht

Der vorliegende Bericht gliedert sich in drei größere Abschnitte, in **Empfehlungen**, **Grundlagen** sowie **Lösungsansätze**, die durch diese Einleitung, ein Glossar sowie ein Stichwortverzeichnis abgerundet werden. Literaturhinweise werden themenspezifisch am Ende jedes einzelnen Kapitels zusammengestellt.

In den **Empfehlungen** werden quasi als Resümee der nachfolgenden Kapitel deren wesentliche Erkenntnisse und Ergebnisse in konkrete Hinweise und Vorschläge zur Verbesserung der IT-Sicherheit umgesetzt. Da die unterschiedlichen strukturellen Ausgangssituationen an den einzelnen Hochschulen in der Regel auch unterschiedliche Schwerpunktsetzungen bei der Auswahl und Umsetzung dieser Empfehlungen nach sich ziehen, wird bewusst auf die Festlegung von Prioritäten und Stufenplänen verzichtet. Stattdessen werden in diesem Teil des Berichts die in den einzelnen Kapiteln enthaltenen Empfehlungen nach einem Gliederungsschema zusammengefasst, das sich an den besonders gefährdeten bzw. mit vertretbarem Aufwand bereits wirksam zu schützenden Bereichen des IT-Gesamtsystems orientiert. Die Darstellung beginnt mit den grundlegenden Empfehlungen zur Aufstellung eines IT-Sicherheitskonzepts, das an den Anfang jeglicher Bemühungen um die IT-Sicherheit zu setzen ist. Daran schließen sich Hinweise zum Schutz der Arbeitsplatzrechner und Server (zunächst unter den Bedingungen des lokalen Betriebs unabhängig von einer Netzintegration) und Vorschläge für die Absicherung der Datenübertragung sowie zur Zugangs- und Zugriffskontrolle bei Arbeitsplatzrechnern und Servern an. Empfehlungen zu organisatorischen Maßnahmen, die einen wesentlichen Beitrag zur Verbesserung der IT-Sicherheit leisten, zum Sicherheitsmanagement, das als Teil des Netz- und Systemmanagements die Wirksamkeit der getroffenen Sicherheitsmaßnahmen überwacht, zum personellen und finanziellen Aufwand für die IT-Sicherheit sowie zur Einrichtung eines Kompetenzzentrums für IT-Sicherheit in Bayern runden diesen ersten Teil des Berichts ab.

Der Teil **Grundlagen** stellt in den Kapiteln 1 bis 3 dar, auf welcher Basis eine Analyse des gegenwärtigen IT-Sicherheitsniveaus sowie Maßnahmen zu seiner Verbesserung aufbauen müssen. Dazu werden in Kapitel 1 Leitlinien für die Entwicklung und Umsetzung eines IT-Sicherheitskonzepts erarbeitet, das am Anfang jeglicher Bemühungen um IT-Sicherheit stehen muss. Kapitel 2 versucht anhand der IT-Basisdienste sowie der typischen Anwendungen die konkreten Anforderungen aus dem Verwaltungs- und Klinikbereich an die Netz- und Systemsicherheit herauszuarbeiten. Schließlich beschreibt Kapitel 3 die aus drei Umfragen unter den Verwaltungen und Kliniken der bayerischen Hochschulen gewonnenen

Erkenntnisse über die aktuelle Situation der Netze und Netzanwendungen im Verwaltungs- und Klinikbereich.

Im Abschnitt **Lösungsansätze** werden in den Kapiteln 4 bis 12 für verschiedene Bereiche und Aspekte der IT-Sicherheit Komponenten, Methoden und Verfahren dargestellt, die als Bausteine für eine umfassende Sicherheitslösung verwendet werden können. So beschreibt Kapitel 4 Möglichkeiten zur Virtualisierung der Netze, mit denen isolierte Netzinseln zu Virtuellen Privaten Netzen (VPN) verbunden werden können. Kapitel 5 widmet sich der Netzabsicherung durch Firewalls und beschreibt und bewertet die Leistungsfähigkeit der verschiedenen Konfigurationen von Firewall-Systemen. In Kapitel 6 werden die unterschiedlichen Ansätze und Anwendungsfelder für die Verschlüsselung vertraulicher oder sensibler Daten dargestellt. Unter der Überschrift Sichere Betriebssysteme und Basisdienste beschreibt Kapitel 7 Sicherheitsmechanismen in Betriebssystemen und beleuchtet dabei vor allem die verbreiteten Server-Betriebssysteme UNIX und WINDOWSNT. Außerdem wird dort eine detaillierte Übersicht über sichere Kommunikationsprotokolle und Basisdienste gegeben. Um Zugangs- und Zugriffskontrollen bei DV-Anwendungen im Klinik-/Verwaltungsbereich geht es in Kapitel 8. Dort werden Mechanismen für die Benutzeridentifikation und Authentifizierung dargestellt und Lösungsmöglichkeiten für Zugriffskontrollen zu unterschiedlichen Anwendungen aufgezeigt. Kapitel 9 untersucht den Beitrag des Netz- und Systemmanagements zur Systemsicherheit und bietet eine umfangreiche Zusammenstellung von Systemen und Werkzeugen zum Sicherheitsmanagement sowie zur Überwachung von Netzen und Systemen. Organisatorische und administrative Maßnahmen zur Verbesserung der Sicherheit in lokalen Netzen sind Gegenstand der Darstellungen in Kapitel 10; sie beschreiben ein weites Spektrum von Ansatzpunkten, an denen derartige Maßnahmen einen wesentlichen Beitrag zur Verbesserung der IT-Sicherheit leisten können. Der integrierte Lösungsansatz im Projekt BASILIKA, der in Kapitel 11 skizziert wird, stellt die verschiedenen Sicherheitskomponenten und -ansätze in einen konzeptionellen Rahmen und bietet damit eine Gesamtlösung zur Gewährleistung einer umfassenden IT-Sicherheit an. Abschließend widmet sich Kapitel 12 der Zertifizierung von Sicherheitslösungen und beschreibt die Aktivitäten verschiedener Zertifizierungsinstanzen vor allem auf dem Sektor der Sicherheitszertifizierung von gängigen Betriebssystemen und Firewall-Lösungen.

Mitglieder der Arbeitsgruppe und weitere Beteiligte

Die vom Bayerischen Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst eingesetzte Arbeitsgruppe bestand aus den Herren

- Franz X. Eberl,
  Zentrale Verwaltung der Technischen Universität München
- Dr. Alexander Horsch,
  Institut für Medizinische Statistik und Epidemiologie
  der Technischen Universität München
- Dr. Heinrich Kersten,
  Bundesamt für Sicherheit in der Informationstechnik, Bonn

- Prof. Dr. Herbert Kopp,
  Fachhochschule Regensburg
- Christian Rossa,
  Rechenzentrum der Universität Würzburg
- Dr. Günther Schuller,
  Zentralverwaltung der Universität Würzburg
- Dr. Wolfgang A. Slaby,
  Leiter des Rechenzentrums der Kath. Universität Eichstätt
  (Vorsitz)
- Michael Slopianka,
  Regionales Rechenzentrum Erlangen der Universität Erlangen-Nürnberg
  bzw. Bayerische Landesbank
- Reinhold Staubach,
  Verwaltung der Universität Regensburg
- Prof. Dr. Joachim Swoboda,
  Lehrstuhl für Datenverarbeitung der Technischen Universität München

Das Bayerische Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst war beteiligt durch die Herren

- Ministerialrat Norbert Willisch
- Studiendirektor Johann Winter

Während der gesamten Sitzungsperiode erfuhr die Arbeitsgruppe tatkräftige Unterstützung durch die Herren

- Bernhard Brandel,
  Rechenzentrum der Kath. Universität Eichstätt
- Marcel Weinand,
  Bundesamt für Sicherheit in der Informationstechnik, Bonn

Die Erörterungen in den Sitzungen wurden durch folgende Vorträge unterstützt:

- Uwe Ellermann (DFN-CERT, Hamburg):
  „Firewalls und Internet-Sicherheit“
- Bernhard Esslinger (Fa. SAP, Walldorf):
  „Sicherheit bei SAP R/3“
- Dr. Ansgar Heuser (Bundesamt für Sicherheit in der Informationstechnik, Bonn):
  „Datenschutz durch Verschlüsselung“

- Monika Horak
  (Lehrstuhl für Datenverarbeitung der Technischen Universität München):
  „Chipkartensysteme“ und
  „Sicherheitsmanagement als Bestandteil des Netz- und Systemmanagements“
- Helmut Krämer (Fa. Data General, Schwalbach):
  „Sicheres UNIX? – Sicheres UNIX!“
- Dr. Lutz Marten (Zentralverwaltung der Universität Würzburg):
  „Bericht über das Projekt BASILIKA“
- Norbert Pohlmann (Fa. KryptoKom, Aachen):
  „Krypto-Router und Krypto-Firewalls“
- Michael Slopianka
  (Regionales Rechenzentrum Erlangen der Universität Erlangen-Nürnberg):
  „Datensicherheit im Netz: Firewalls und Krypto-Router“
- Dr. Gerhard Weck (Fa. Infodas, Köln):
  „Aufteilung und Überwachung von Zugriffsrechten in Client/Server-Betriebssystemen“

Ein besonderer Dank gebührt Herrn Bernhard Brandel, der die Sitzungsergebnisse regelmäßig festhielt, die Schlussredaktion organisierte und die abschließende Layout- und Satzgestaltung besorgte, sowie Frau Theresia Stalker für die endgültige Aufbereitung des Berichts als Postscript-Dokument.

Empfehlungen

In den einzelnen Kapiteln des vorliegenden Arbeitsberichts, in denen zu spezifischen Aspekten der IT-Sicherheitsproblematik jeweils abgegrenzte Lösungen vorgestellt werden, werden an Ort und Stelle auch Empfehlungen zur konkreten Umsetzung der dargestellten Lösungsansätze sowie zum Einsatz der beschriebenen Sicherheitstools ausgesprochen. Dass dabei das Ziel einer umfassenden Gesamtlösung für die IT-Sicherheit nicht aus den Augen verloren werden darf, macht Kapitel 11 deutlich, welches sich der Darstellung des integrierten Lösungsansatzes im Projekt BASILIKA (“Bayerische Sicherheitslösung für Dienstangebote in offenen Kommunikationsnetzen”) widmet.

Darüber hinaus erscheint es der Arbeitsgruppe sinnvoll, dem Bericht einen gesonderten Empfehlungsteil voranzustellen, der die wesentlichen Erkenntnisse und Ergebnisse der nachfolgenden Kapitel ohne Anspruch auf Vollständigkeit in konkrete Hinweise zur Verbesserung der IT-Sicherheit umsetzt. Dabei orientiert sich die Darstellung dieser Empfehlungen an den Stellen im IT-Gesamtsystem, die einer besonderen Sicherheitsbedrohung ausgesetzt sind bzw. an denen sich wirksame Maßnahmen zur Verbesserung der IT-Sicherheit mit angemessenem Aufwand ergreifen lassen; sie gliedert sich in die folgenden Abschnitte:

- IT-Sicherheitskonzept (Sicherheitspolitik)
- Schutz der Arbeitsplatzrechner und Server
- Absicherung der Datenübertragung
- Zugangs- und Zugriffskontrolle bei Arbeitsplatzrechnern und Servern
- Organisatorische Maßnahmen
- Sicherheitsmanagement
- Personeller und finanzieller Aufwand für die IT-Sicherheit
- Kompetenzzentrum für IT-Sicherheit
- Zusammenfassung

Auch wenn es eine absolute Sicherheit beim Einsatz von IT-Systemen nicht geben kann, so lässt sich dennoch durch die konsequente Anwendung der hier vorgeschlagenen technischen und organisatorischen Maßnahmen ein nach gegenwärtigen Maßstäben akzeptables Sicherheitsniveau erreichen. Wegen der ständigen Veränderungen in der IT-Infrastruktur jeder Hochschule, der rasanten Entwicklung bei den IT-Sicherheitsprozeduren und -werkzeugen aber auch bei den gegen die IT-Sicherheit gerichteten Bedrohungen bedarf es allerdings kontinuierlicher Anstrengungen in der Aktualisierung des IT-

Sicherheitskonzepts sowie in der Verbesserung der anzuwendenden Sicherheitsmaßnahmen, um das einmal erreichte Sicherheitsniveau mindestens zu halten, möglichst jedoch weiter zu verbessern.

IT-Sicherheitskonzept (Sicherheitspolitik)

Ausgangspunkt jeglicher Aktivitäten im Bereich der IT-Sicherheit muss die Erstellung eines **IT-Sicherheitskonzepts** sein. Darin werden die schutzbedürftigen Objekte und Werte, die gegen sie gerichteten Bedrohungen und das angestrebte Sicherheitsniveau (IT-Sicherheitsziele) definiert und die organisatorischen Rahmenbedingungen (IT-Sicherheitsrichtlinien) und technischen Maßnahmen (IT-Sicherheitsprozeduren) festgelegt, mit denen die IT-Sicherheitsziele angestrebt werden.
[siehe Kapitel 1]

- Die IT-Sicherheitsrichtlinien müssen rechtlich abgesichert sein, was von der Rechtsabteilung der Hochschule gegebenenfalls unter Hinzuziehung von Fachjuristen zu überprüfen ist; sie müssen politisch in der Institution durchsetzbar sein, was die Einbindung der Hochschulleitung wie der Personalvertretung in ihren Entstehungsprozess zwingend erforderlich macht; sie müssen schließlich zusammen mit den daraus resultierenden IT-Sicherheitsprozeduren auch technisch realisierbar sein.
- Alle betroffenen Benutzer der IT-Infrastruktur sind detailliert über die für sie verbindlichen IT-Sicherheitsrichtlinien zu informieren und auf deren Einhaltung zu verpflichten; durch regelmäßige Fortbildungsmaßnahmen ist ein entsprechendes Sicherheitsbewusstsein aufzubauen und zu stärken.
- Aufgrund der ständigen Veränderungen in der IT-Infrastruktur der Hochschule, der rasanten Entwicklung bei den IT-Sicherheitsprozeduren und -werkzeugen, aber auch bei den gegen die IT-Sicherheit gerichteten Bedrohungen kann das IT-Sicherheitskonzept kein statisches, ein für alle Mal festgelegtes Regelwerk sein, sondern muss kontinuierlich weiterentwickelt und aktualisiert werden. Insbesondere aber nach Eintritt eines konkreten Sicherheitsvorfalls ist das IT-Sicherheitskonzept unter Berücksichtigung der bei der Behandlung dieses Schadensereignisses gewonnenen Erfahrung dahingehend zu modifizieren, dass ein erneutes Auftreten desselben Schadensereignisses wirksam verhindert oder zumindest weiter erschwert wird.
- Wesentlicher Bestandteil des IT-Sicherheitskonzepts muss ein **Notfallplan** sein, der das Procedere beim Eintritt sicherheitsrelevanter Ereignisse detailliert festlegt. Dieser Notfallplan soll Regeln für die Identifizierung eines Sicherheitsvorfalls enthalten, die Zuständigkeiten, die Informationspolitik und die Kontaktstellen festlegen sowie Handlungsanweisungen für die konkreten Maßnahmen zur Schadensbegrenzung, zur Beseitigung der Ursachen und zur Beweissicherung bis hin zur Wiederherstellung der Systemintegrität enthalten.

- Zur Entwicklung und kontinuierlichen Fortschreibung des IT-Sicherheitskonzepts, zur Behandlung von Sicherheitsvorfällen sowie zur Koordinierung aller mit der IT-Sicherheit zusammenhängenden Aktivitäten ist ein **Sicherheitsmanagement-Team** in der Hochschule zu bilden, das sich aus IT-Spezialisten, dem Datenschutzbeauftragten und Vertretern der Hochschulleitung zusammensetzt. Dabei ist offenkundig, dass sowohl punktuell für die Erstellung und Durchsetzung des IT-Sicherheitskonzepts als auch kontinuierlich für seine Realisierung, Überwachung und Fortschreibung sowie für die Behandlung und spätere Aufarbeitung von konkreten Sicherheitsvorfällen personelle Kapazitäten in ausreichender Größenordnung zur Verfügung stehen müssen.
- Wegen der Gleichartigkeit der IT-Sicherheitsziele in den Verwaltungen bzw. Kliniken der bayerischen Hochschulen erscheint es sinnvoll, im Rahmen zweier Pilotprojekte für jeden der beiden Bereiche ein IT-Sicherheitskonzept prototypisch erarbeiten zu lassen, das den entsprechenden Einrichtungen der übrigen Hochschulen als Muster und Ausgangsbasis für das eigene IT-Sicherheitskonzept dienen kann.

Schutz der Arbeitsplatzrechner und Server

Auch ohne die Integration in ein offenes Netz sind Arbeitsplatzrechner und Server bereits unter den Bedingungen eines lokalen Betriebs vielfältigen Bedrohungen ausgesetzt, die sich gegen die Vertraulichkeit und Integrität der auf diesen Systemen abgelegten Daten sowie gegen die Sicherheit der eingesetzten Betriebssysteme und systemnahen Software richten. Diesen Bedrohungen muss mit geeigneten Maßnahmen begegnet werden.

- Zum **Schutz gegen Viren** sollte der Gebrauch mobiler Datenträger auf ein unumgänglich notwendiges Maß beschränkt werden. Jede auf einen Arbeitsplatzrechner zu übernehmende Datei ist vor dem Import auf möglichen Virenbefall zu untersuchen. Für besonders schutzwürdige Datenbereiche sollten Serialisierungssysteme bzw. selbstentladende, verschlüsselte Datenträger eingesetzt werden. Dem neuen Gefährdungspotential durch *Makroviren* ist durch Einsatz geeigneter aufeinander abgestimmter lokaler bzw. servergestützter Programme entgegenzuwirken. Bei Bedarf aufrufbare Virenscanner sind im Rahmen eines umfassenden Virenschutzkonzepts ebenso bereitzustellen wie systemresidente Virenwächter und dienste-integrierte Internet-Virenscanner, die aus dem Netz empfangene Dateien automatisch auf Schadensfunktionen untersuchen.
  [siehe Kapitel 10]
- Die Erzeugung insbesondere personenbezogener und sensitiver Daten sollte auf das unbedingt notwendige Maß beschränkt werden. Außerdem ist durch Anonymisierung, wo immer diese möglich erscheint, eine Reduzierung des Datenschutzrisikos anzustreben.
- Wenn jedoch auf Arbeitsplatzrechnern oder Servern vertrauliche oder besonders schutzwürdige Daten lokal gespeichert werden, so sind diese durch **Verschlüsselung** mit einem kryptographischen Verfahren anerkannter Leistungsfähigkeit gegen

die Verletzung der Vertraulichkeit oder Integrität zu sichern. Wegen des erhöhten Diebstahlrisikos gilt dies insbesondere für mobile Arbeitsplatzrechner (Laptops, Notebooks), bei denen gegebenenfalls Verfahren zur lokalen Verschlüsselung der gesamten Festplatte vorzusehen sind.

Bei der Ablage verschlüsselter Dokumente ist außerdem sicherzustellen, dass bei Verhinderung des Dokumenten- bzw. Schlüsselinhabers andere autorisierte Personen Zugriff auf den Inhalt dieser Dokumente erlangen können.
[siehe Kapitel 6]

- Durch Verlagerung auf einen separaten Server ist der Testbetrieb vom Produktionsbetrieb strikt zu trennen. Auf dem Produktionsrechner dürfen keine Entwicklungswerkzeuge verbleiben.
  [siehe Kapitel 10]
- Zur Verbesserung der **Sicherheit von Betriebssystemen und systemnaher Software** bei UNIX- oder WINDOWSNT-Servern sollte zunächst die Menge der möglichen Angriffspunkte reduziert werden. Dies wird zum einen dadurch erreicht, dass Betriebssystemfunktionen, die zur Erbringung der vom Server erwarteten Dienste nicht benötigt werden, entfernt oder zumindest gesperrt werden, zum andern dadurch, dass für die verbleibenden Systemfunktionen vom DFN-CERT empfohlene Sicherheitspatches umgehend angewendet werden.
  [siehe Kapitel 7]

  Bei besonders hohen Sicherheitsanforderungen (z.B. im klinischen Bereich) sollte gegebenenfalls der Einsatz einer auf höherem Level (B2, E4) sicherheitszertifizierten Betriebssystemvariante in Erwägung gezogen werden.
  [siehe Kapitel 12]

Absicherung der Datenübertragung

Da Daten während ihrer Übertragung über offene Netze Angriffen gegen ihre Vertraulichkeit und Integrität ausgesetzt sind, müssen entweder die Übertragungswege besonders abgesichert oder die Daten selbst durch geeignete Verschlüsselungsmaßnahmen geschützt werden.

- Eine Kopplung von lokalen Netzen über öffentliche oder auch private Netze zur Bildung eines **Virtuellen Privaten Netzes (VPN)** sollte mit Hilfe logischer Kanäle (Tunnel) erfolgen. Mit zunehmender Verbreitung des IP next generation (IPng, IPv6) sollten die mit diesem Protokoll bereitgestellten Sicherheitsoptionen (Authentication Header (AH) bzw. Encapsulating Security Payload Header (ESP)) auch konsequent für die Bildung und Absicherung solcher Tunnel eingesetzt werden.
  [siehe Kapitel 4]
- Für eine darüber hinaus besonders gesicherte Verbindung von Teilnetzen bzw. die gesicherte Anbindung einzelner Arbeitsplatzrechner an ein Teilnetz über die grundsätzlich unsicheren Netzverbindungen des Hochschulnetzes oder des deutschen Wissenschaftsnetzes ist der dedizierte **Einsatz von Krypto-Boxen** vorzusehen, die den

gesamten Datenverkehr zwischen den Teilnetzen bzw. zwischen dem Teilnetz und dem darin zu integrierenden Arbeitsplatzrechner verschlüsseln. Dabei ist Verfahren und Produkten der Vorrang zu geben, die eine nach heutigen Erkenntnissen ausreichende Kryptierungssicherheit bieten und darüber hinaus möglichst ein Sicherheitszertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) besitzen.
[siehe Kapitel 4 und 6]

- Da die Standardisierung bei Techniken und Protokollen für **Virtuelle Netze (VLANs)** in vielen Bereichen noch nicht abgeschlossen ist, muss ihr Einsatz derzeit auf überschaubare und homogene Netzumgebungen beschränkt bleiben.

  Um allerdings überhaupt die Voraussetzungen für den Einsatz von Switches und den Aufbau von VLANs zu schaffen, muss der Ausbau einer strukturierten Verkabelung in den Hochschulen mit Nachdruck vorangetrieben werden. Da die Hochschulen mit der Finanzierung dieses Ausbaus der Netzinfrastruktur überfordert sein dürften, ist eine Weiterführung des Netzinvestitionsprogramms (NIP) dringend erforderlich.
  [siehe Kapitel 4]

- Insbesondere dort, wo eine Absicherung der Datenübertragung mit Hilfe von Krypto-Boxen nicht möglich ist, sind **kryptographisch besonders gesicherte Basisdienste und Übertragungsprotokolle** wie SSL, S-HTTP, SSH, etc. zur Realisierung von Standardfunktionen wie Telnet, Remote Shell, WorldWideWeb, X-Window, FTP, etc. vorzusehen.
  [siehe Kapitel 7]

- Für den Austausch von Dateien mit vertraulichem oder besonders schützenswertem Inhalt sollte ein **leistungsfähiges Verschlüsselungsverfahren** wie PGP (Pretty Good Privacy), PEM (Privacy Enhanced Mail) oder S/MIME (Secure Multipurpose Internet Mail Extensions) verwendet werden. Bei der Erzeugung und Verwaltung des eigenen Schlüsselpaares ist u.a. darauf zu achten, dass der private Schlüssel sicher aufbewahrt und keinem Dritten zugänglich wird. Insbesondere verbietet sich deshalb die Verwahrung auf Mehrbenutzersystemen, wo der Zugriff Fremder nicht ausgeschlossen ist. Die verwendete Schlüssellänge sollte z.B. beim RSA-Verfahren 2048 Bit nicht unterschreiten.

  Zusätzlich lässt sich ein asymmetrisches Verschlüsselungsverfahren dazu verwenden, ein Dokument mit einer **digitalen Unterschrift (Signatur)** zu versehen. Davon sollte immer dann Gebrauch gemacht werden, wenn die Integrität eines übersandten Dokuments oder die Identität des Absenders zweifelsfrei nachgewiesen werden soll.
  [siehe Kapitel 6]

Zugangs- und Zugriffskontrolle bei Arbeitsplatzrechnern und Servern

Nur den jeweils dazu Berechtigten ist der Zugang und Zugriff auf Arbeitsplatzrechner, Server und Anwendungen zu gewähren. Dabei ist der Umfang an Zugriffsrechten auf

das zur Erfüllung der jeweiligen Aufgabe notwendige Minimum zu beschränken. Diese Ziele lassen sich mit einer Kombination von Maßnahmen aus unterschiedlichen Bereichen anstreben.

- Zur Absicherung der Server gegen unberechtigten Zugang von außen, aber auch gegen mögliche Attacken von Innentätern, sind diese Server konzentriert in einem zugangskontrollierten Raum aufzustellen und in **separaten, besonders gesicherten Server-Subnetzen** zu betreiben.
  [siehe Kapitel 7]
- Am Übergang zwischen diesen Server-Subnetzen und dem offenen Hochschulnetz sollte ein **Firewall-System** eingesetzt werden, das aus Packet-Screens und einem dazwischen liegenden Application-Gateway (Bastion) besteht. In Abhängigkeit von der zu erreichenden Sicherheitsstufe bzw. den finanziellen Rahmenbedingungen sollte man dabei möglichst auf eine sicherheitszertifizierte Firewall-Lösung zurückgreifen.

  Diese Firewall sollte nach dem Prinzip konfiguriert sein, dass grundsätzlich jeglicher Datenverkehr verboten ist und nur gewünschte Kommunikationsbeziehungen und Dienste explizit freigegeben werden. Dabei darf der Ausfall einer Firewall-Komponente keinesfalls zum Verlust der Firewall-Funktionalität führen sondern höchstens bewirken, dass kein Datenverkehr mehr möglich ist.
  [siehe Kapitel 5]
- Der Zugang zu den Verwaltungs- bzw. Klinik-Servern im gesicherten Server-Subnetz sollte nur von wohldefinierten Arbeitsplatzrechnern aus und nur für explizit freigegebene Dienste und authentifizierte Nutzer zugelassen werden; dies kann mit Programmen wie z.B. TCP-Wrapper kontrolliert werden.
  [siehe Kapitel 7 und 9]
- Zugangsberechtigungen zu den Servern werden bei den gängigen Server-Betriebssystemen üblicherweise durch mehrfach verwendbare **Passwörter** abgesichert. Die Wirksamkeit dieses Schutzes hängt allerdings wesentlich von der Qualität der verwendeten Passwörter ab und wird zusätzlich noch dadurch beeinträchtigt, dass Passwörter während des Authentifizierungsprozesses in der Regel unverschlüsselt übertragen werden und damit möglichen Abhör-Attacken schutzlos ausgesetzt sind. Deshalb sollten im Verwaltungs- und Klinikbereich **wirkungsvollere Authentifizierungsmethoden** eingesetzt werden; diese reichen von der Verwendung von Einmal-Passwörtern wie z.B. bei S/Key (siehe 7.6.5) über den Einsatz von Challenge-Response-Verfahren zur dynamischen Erzeugung von Zugangsschlüsseln wie z.B. bei SecureShell (SSH) bis hin zur Authentifizierung des Nutzers mittels **Prozessorchipkarten**. Auch für Arbeitsplatzrechner, insbesondere wenn sie öffentlich zugänglich sind und multifunktional eingesetzt werden, ist mit Hilfe von Authentifizierungsverfahren eine wirkungsvolle Zugangskontrolle sicherzustellen.
  [siehe Kapitel 7 und 8]

  Die mit dem üblicherweise notwendigen Zugang zu verschiedenen Servern und Applikationen einhergehende Vervielfachung und damit wesentliche Verschärfung des Authentifizierungsproblems lässt sich nur dadurch vermeiden, dass man alle Authentifizierungsvorgänge zu einem Single-Signon auf einem gesonderten **Authentifizie-**

rungs-Server konzentriert.
[siehe Kapitel 8 und 11]

- Die **Vergabe von Zugriffsrechten** auf Objekte wie Applikationen, Dateien, Datenfelder, etc. sollte nach dem **Least-Privilege-Prinzip** erfolgen, d.h. es sollte nur das Minimum an Zugriffsrechten eingeräumt werden, das zur Abwicklung einer bestimmten Aufgabe/Funktion unbedingt erforderlich ist. Zur Verwaltung und Kontrolle von Zugriffsberechtigungen ist man dabei im Wesentlichen auf die Mechanismen angewiesen, die das Server-Betriebssystem oder die jeweilige Applikation bereitstellen.

  Auch hier erscheint eine Zentralisierung der Verwaltung der nutzerspezifischen Berechtigungsprofile sowie der Überprüfung und Freigabe bzw. Verweigerung von Zugriffsberechtigungen auf einem separaten **Berechtigungs-Server** angeraten. Inwieweit dazu bestehende Directory-Systeme wie die Novell Directory Services (NDS) eine geeignete Basis darstellen, wird u.a. im Projekt BASILIKA eingehend untersucht.
  [siehe Kapitel 8 und 11]
- Ein besonderes Problem stellen die allumfassenden Zugriffsrechte des Systemadministrators dar, dessen Privilegien als Superuser mit allgemein akzeptierten Sicherheitsanforderungen unvereinbar sind. Hier lässt sich allerdings nur dadurch Abhilfe schaffen, dass der Aufgabenkomplex “Systemadministration” in Teilaufgaben zerlegt und zu “Rollen” gebündelt neu zusammengestellt wird, denen das Minimum an für die jeweilige Rolle erforderlichen Zugriffsrechten eingeräumt wird. Diese Möglichkeit der Rekomposition der *root*-Rechte wird bisher nur unzureichend von den gängigen Server-Betriebssystemen unterstützt, weshalb bei hohen Sicherheitsanforderungen auf die sicherheitsoptimierten Varianten der Standard-Betriebssysteme ausgewichen werden muss.
  [siehe Kapitel 10 und 12]

Organisatorische Maßnahmen

Organisatorische und administrative Maßnahmen leisten einen wesentlichen Beitrag zur Erhöhung der Sicherheit in Verwaltungs- und Kliniknetzen. Sie beeinflussen die Verfügbarkeit der IT-Infrastruktur positiv und reduzieren das Gefährdungspotential, das von Innentätern ausgeht. Gegenüber Attacken von außen wirken sie dagegen eher mittelbar. [siehe Kapitel 10]

- Dezentrale DV-Versorgungsstrukturen und neue Netzdienste machen eine **Analyse und Neustrukturierung der DV-Aufgaben** erforderlich. Dabei liegt der Fokus auf folgenden Bereichen:
  - Strukturierung der Geschäftsprozesse unter Nutzung der neuen Dienste;
  - Organisation eines effizienten Benutzerservice;
  - Etablierung eines integrierten Netz-, System- und Sicherheitsmanagements.

- Diese Neustrukturierung muss ihren Niederschlag finden in einer klar geregelten Geschäftsverteilung (Aufgaben, Kompetenzen und Verantwortlichkeiten, Vertretung), insbesondere auch an der Schnittstelle zwischen Fach- und EDV-Abteilung sowie innerhalb von Geschäftsprozessen. Dabei sollten stark strukturierte Verwaltungsprozesse mit hohem Koordinierungsaufwand durch *Workflow-Management-Systeme* unterstützt werden.
- Voraussetzung für eine hohe Verfügbarkeit und ein möglichst reibungsarmes Zusammenwirken von Diensten, Programmen und Daten (aber auch Mitarbeitern) ist neben der Reduktion der Komponentenvielfalt eine Standardisierung von Ablaufprozessen und eingesetzten Systemkomponenten.
- Beschaffungsmaßnahmen insbesondere für strategische Komponenten sind stärker als bisher auch im Hinblick auf ihre Verträglichkeit mit dem Sicherheitskonzept zu bewerten und einer Sicherheitsbeitrags- und Schwachstellenanalyse zu unterziehen. Zumindest für hochgradig sicherheitsrelevante Komponenten sollte zugunsten von **marktgängigen Sicherheitskomponenten und -standards** auf Eigenentwicklungen verzichtet werden. Dabei ist Produkten mit integrierten Sicherheitsfunktionen der Vorrang vor solchen mit nachträglich aufgesetzten oder angelagerten Sicherheitsmodulen zu geben.
- Die Kenntnis und das Bewusstsein über vorhandene Risiken bei der Inanspruchnahme der Netzdienste ist bei jedem einzelnen Nutzer zu verbessern. Dies ist ein permanenter Prozess, der sowohl durch gezielte Schulungs- und Fortbildungsmaßnahmen als auch durch Beratung aus aktuellem Anlass vor Ort vorangebracht werden muss.
- System-, Netz- und Datenbankadministratoren sollten neben einer breiten Wissensbasis ein hohes Maß an Zuverlässigkeit bei der Aufgabenwahrnehmung sowie an Vertrauenswürdigkeit besitzen. Sie sind in besonderem Maße in Fortbildungsmaßnahmen einzubinden und durch leistungsgerechte Bezahlung zu motivieren. Die Erlangung eines Ausbildungszertifikats kann dabei einen weiteren Anreiz darstellen, sich für die Administration der eingesetzten Produkte besonders zu qualifizieren.
- Der Notfallvorsorge für Systeme und Anwendungen mit hohen Verfügbarkeitsanforderungen ist durch ein durchgängiges **Sicherungs- und Wiederanlaufkonzept** Rechnung zu tragen. Die organisatorischen Maßnahmen, die die Aktivitäten zwischen Feststellung des Notfalls und Wiederherstellung der Betriebsbereitschaft planmäßig begleiten, sind im **Notfallhandbuch** niederzulegen.
- Die zeitliche Verfügbarkeit und der Leistungsumfang des **Benutzerservice** sollten in einer Service-Vereinbarung explizit geregelt werden. Zur Verwaltung der Servicefälle und zur Dokumentation ihrer Bearbeitung sollen geeignete Werkzeuge (z.B. Trouble-Ticket-System) eingesetzt werden.
- Den besonderen Risiken durch die zunehmende Zahl der Fernzugriffe (Telearbeit, Fernwartung, etc.) ist durch ein **Remote-Access-Konzept** Rechnung zu tragen, das die organisatorischen Randbedingungen und die einzusetzenden Systemkomponenten festlegt. Die Modalitäten einer Fernwartung sollten mit dem jeweiligen Serviceanbieter in einem eigenen Vertrag geregelt werden.

- Die mögliche Verletzung des Urheberrechts, wettbewerbsrechtlicher Bestimmungen, des Rechts am eigenen Bild oder datenschutzrechtlicher Vorschriften durch Bereitstellung von Informationen auf Servern, auf die über Datennetze zugegriffen werden kann, wirft vielfältige **Haftungsprobleme** auf. Die dagegen ergriffenen organisatorischen Maßnahmen sind zu dokumentieren und dem jeweiligen Stand der Rechtsprechung anzupassen.

Sicherheitsmanagement

Das Sicherheitsmanagement ist Teil des Netz- und Systemmanagements; es wird sowohl mit Hilfe einzelner und spezieller Sicherheitswerkzeuge als auch durch den Einsatz umfassender Management-Plattformen realisiert.
[siehe Kapitel 9]

- Im Rahmen des Sicherheitskonzepts sind die Ziele und Zuständigkeiten für das Sicherheitsmanagement sowie die Details des Sicherheitsberichtswesens festzulegen. Dort sind ebenfalls Regelungen dafür zu treffen, welche Art von Sicherheitswerkzeugen in welchen Zeitabständen eingesetzt werden sollen und wie die dabei gewonnenen Erkenntnisse in Sicherheitsberichte einfließen.
- Als Mindestaufwand an Sicherheitsmanagement sollten die bekannten verfügbaren **Sicherheitswerkzeuge**
  - zum Auswerten von Audit-Dateien auf Versuche des Eindringens in Systeme, des unberechtigten Zugriffs etc.,
  - zur Sicherheitsüberprüfung von Passwörtern (Passwort-Scanner),
  - zur Durchführung von Prüfangriffen durch Sicherheitsverwalter mit Hilfe von Netz- und System-Scannern (z.B. SATAN) bzw. zur Feststellung von Angriffen mit solchen Tools von außen

  immer benutzt werden. Bereits derartige Mindestmaßnahmen können durch die damit möglichen umfassenden Auswertungen eine hohe Wirkung erzielen.
- Eine umfassende **Management-Plattform** sollte unter dem Aspekt der IT-Sicherheit insbesondere folgende Funktionsbereiche unterstützen:
  - Konfigurationsmanagement:
    die zu überwachende Konfiguration aus Hardware und Software einschließlich des Netzes mit seinen Firewalls sowie der Applikationen muss aktuell bekannt sein;
  - Fehlermanagement:
    Fehler sind oft Punkte möglicher Angriffe oder können als Folgen von Angriffen konkrete Hinweise liefern;
  - Leistungsmanagement:
    im Stau können auch Sicherheitsanforderungen nicht mehr erfüllt werden; manche Angriffe zielen auf einen Leistungskollaps mit Ablehnung berechtigter Zugriffswünsche (Denial of Service);

  - spezielles Sicherheitsmanagement.

- Die Auswahl einer geeigneten Plattform für das Netz- und Systemmanagement mit integriertem Sicherheitsmanagement wird in Abhängigkeit von dem Funktionsumfang des Basispakets und den verfügbaren Komponenten an Hardware und Software, von dem Grad der erforderlichen Sicherheit sowie von übergeordneten Planungen zu treffen sein. Dabei ist es zweckmäßig, für die Bestandsanalyse und erste Auswahl auch externe Berater in den Entscheidungsprozess einzubeziehen.
- Von der Sache her ist das Sicherheitsmanagement ein Teil des Netz- und Systemmanagements und muss daher von der mit diesen Aufgaben betrauten Personengruppe wahrgenommen werden. Das schließt nicht aus, dass die Funktionen innerhalb dieser Gruppe geeignet strukturiert und aufgeteilt werden, so dass Häufungen von Verantwortlichkeiten und die Gefahr des Missbrauchs vermieden werden. Eine Trennung innerhalb der operativen Ebene zwischen Netz-/Systemmanager und Sicherheitsüberwacher wird nicht vorgeschlagen; eine Kontrolle der Netzüberwachungsaufgabe sollte vielmehr durch das Berichtswesen und die Verankerung der Verantwortlichkeit für Fragen der IT-Sicherheit in allen Stufen der Hierarchie sichergestellt werden.

Personeller und finanzieller Aufwand für die IT-Sicherheit

Es ist offensichtlich, dass das gewünschte oder erforderliche Maß an IT-Sicherheit ohne den entsprechenden personellen und finanziellen Aufwand nicht zu erzielen ist. Deshalb ist seitens der Hochschulleitung und des zuständigen Ministeriums alles daranzusetzen, die notwendigen Personalstellen und Mittel gegebenenfalls auch durch Umstrukturierung und Umschichtung bereitzustellen und in den jeweiligen Hochschulhaushalten zu verankern.

- Auch wenn zahlreiche Software-Werkzeuge für den Bereich der IT-Sicherheit kostenfrei oder gegen geringe Lizenzgebühren zur Verfügung stehen, so erfordern sicherheitszertifizierte Firewall-Lösungen, Krypto-Boxen, Chipkartensysteme, spezielle Server zur Authentifizierung und Berechtigungsprüfung, Betriebssystemvarianten mit spezifischen Sicherheitsfunktionen u.v.a.m. einen finanziellen Aufwand in nicht unbeträchtlicher Größenordnung.
- Deutlich höher als dieser finanzielle Aufwand ist jedoch der permanent zu investierende personelle Aufwand. Das beginnt mit der Etablierung eines **Sicherheitsmanagement-Teams** zur Entwicklung und kontinuierlichen Fortschreibung des IT-Sicherheitskonzepts, zur Behandlung von Sicherheitsvorfällen sowie zur Koordinierung aller mit der IT-Sicherheit zusammenhängenden Aktivitäten. Das setzt sich fort in der Bereitstellung der notwendigen personellen Kapazität für das Netz-, System- und Applikationsmanagement, dessen Aufwand in hohem Maße von der Homogenität des Rechnernetzes, von der Konfigurationsfreiheit der Arbeitsplatzrechner und der DV-Kompetenz ihrer Benutzer abhängt.

  Als grobe Orientierung für die Größenordnung des Personalaufwands können Erfahrungswerte aus dem Bereich großer Lehrstühle einerseits und dem Bankenbereich andererseits dienen: So sind für die beschriebenen Aufgaben, d.h. für die

Netz-, Rechner- und Anwendungsbetreuung einschließlich Sicherheitsmanagement als Grundausstattung vier Personalstellen erforderlich, die ab mehr als 100 Rechnerarbeitsplätzen volumenabhängig um bis zu drei Personalstellen je 100 Rechnerarbeitsplätze aufzustocken sind. Rund 1/4 bis 1/3 des Aufwands enfällt davon auf den Bereich IT-Sicherheit.

- Zur Kostenoptimierung und Ausschöpfung möglicher Synergieeffekte hält die Arbeitsgruppe die Förderung von Pilotprojekten in den folgenden Bereichen für sinnvoll und erforderlich:
  - Prototypische Erstellung von IT-Sicherheitskonzepten für den Verwaltungs- bzw. Klinikbereich, die den entsprechenden Einrichtungen der Hochschulen als Muster und Ausgangsbasis für das eigene IT-Sicherheitskonzept dienen können;
  - Erprobung und System-Zertifizierung einer Firewall-Lösung in einer typischen Anwendungsumgebung;
  - Auswahl und prototypischer Einsatz eines weit verbreiteten Systemmanagement-Produkts wie Tivoli TME10 oder CA Unicenter TNG zur Bewertung seiner Eignung als Sicherheitsmanagement-System.

Kompetenzzentrum für IT-Sicherheit

Auch wenn auf ein lokales Sicherheitsmanagement-Team an jeder Hochschule nicht verzichtet werden kann, so lassen sich doch eine Reihe von Aufgaben und Aktivitäten zur Verbesserung der IT-Sicherheit *zentral* durchführen. Zu diesem Zweck empfiehlt die Arbeitsgruppe die Einrichtung eines **Kompetenzzentrums für IT-Sicherheit**, welches für die bayerischen Hochschulen sowie gegebenenfalls darüber hinaus für die bayerischen Landesbehörden zentrale IT-Sicherheitsaktivitäten übernimmt, um dadurch

- Arbeit und Aufwand zu sparen sowie entsprechende Synergieeffekte zu erzielen,
- landesweit möglichst einheitliche Sicherheitslösungen zu erhalten und
- durch den Einsatz hauptamtlicher Spezialisten ein höheres Maß an Professionalität und damit ein besseres Sicherheitsniveau zu erreichen.

Neben den im vorangehenden Abschnitt genannten Pilotprojekten zur prototypischen Erstellung von IT-Sicherheitskonzepten für den Verwaltungs- bzw. Klinikbereich, zur Erprobung und System-Zertifizierung einer Firewall-Lösung sowie zum Einsatz eines Systemmanagement-Produkts bieten sich u.a. folgende Aufgaben zur Wahrnehmung durch ein Kompetenzzentrum für IT-Sicherheit an:

- rechtliche Prüfung und Bewertung von IT-Sicherheitskonzepten;
- Ausarbeitung und laufende Aktualisierung von Checklisten für die Analyse und Bewertung von Bedrohungen und Sicherheitsrisiken;
- Marktbeobachtung und -analyse für Sicherheitslösungen;
- Tests angebotener Sicherheitslösungen und Ermittlung von Qualitätsmerkmalen;

- Initiierung oder Durchführung von Produkt- bzw. System-Zertifizierungen;
- Konfektionierung von Sicherheitslösungen nach den Vorgaben der jeweils anfordernden Hochschule einschließlich Installation und Schulung;
- Ausarbeitung von Sicherheits-Checklisten und Leistungsverzeichnissen für Applikationsanbieter (HIS, SAP etc.);
- Übernahme der Funktion eines Computer Emergency Response Teams (CERT), das die örtlichen Sicherheitsmanagement-Teams insbesondere bei Sicherheitsvorfällen und Schadensereignissen wirkungsvoll unterstützt;
- Schulung und Sicherheitstraining.

Darüber hinaus wird in Analogie zum Arbeitskreis „Bayerisches Hochgeschwindigkeits-Netz (BHN)“ die Etablierung eines Arbeitskreises „IT-Sicherheit“ angeregt, in dem die Mitarbeiter der örtlichen Sicherheitsmanagement-Teams untereinander und mit dem Kompetenzzentrum für IT-Sicherheit einen regen Erfahrungsaustausch pflegen, gemeinsame Aktivitäten koordinieren und Kooperationen absprechen.

Zusammenfassung

Ohne ein IT-Sicherheitskonzept für die Anbindung eines Verwaltungs- oder Kliniknetzes an die offene Netzinfrastruktur der Hochschule und damit an das weltweite Internet bleiben jegliche Bemühungen um die IT-Sicherheit bruchstückhaft und ohne klare Zielvorgabe. Deshalb muss die **Erstellung eines IT-Sicherheitskonzepts**, welches die Sicherheitsrisiken analysiert und bewertet, die für die Institution relevanten Sicherheitsziele vorgibt und die organisatorischen Rahmenbedingungen und technischen Sicherheitsmaßnahmen festlegt, mit denen diese Sicherheitsziele angestrebt werden sollen, erster und unverzichtbarer Schritt auf dem Weg zu einem höheren Sicherheitsniveau sein. Ebenso unverzichtbar ist die **Etablierung eines Sicherheitsmanagement-Teams**, ohne das die Entwicklung, Umsetzung und kontinuierliche Fortschreibung des IT-Sicherheitskonzepts, die Koordinierung und Überwachung aller mit der IT-Sicherheit zusammenhängenden Aktivitäten sowie die angemessene Behandlung von Sicherheitsvorfällen nicht möglich ist.

Alle weitergehenden Schritte und Maßnahmen sind anschließend aus dem IT-Sicherheitskonzept zu entwickeln, wobei die spezifische Situation der jeweiligen Hochschulverwaltung bzw. Universitätsklinik zu unterschiedlichen Prioritäten führen wird. Wichtig ist dabei allerdings, dass alle Einzelmaßnahmen nicht isoliert betrachtet sondern auf das Ziel einer integrierten Gesamtlösung für die IT-Sicherheit hin orientiert werden.

Teil I: Grundlagen

Kapitel 1

Leitlinien für die Entwicklung und Umsetzung eines IT-Sicherheitskonzepts

Auch wenn die prototypische Erarbeitung eines IT-Sicherheitskonzepts für Hochschulverwaltungen bzw. Universitätskliniken prinzipiell möglich erscheint und sicherlich äußerst wünschenswert wäre, hätte diese komplexe Aufgabe den Rahmen der Kommissionsarbeit gesprengt. Deshalb beschränkt sich das vorliegende Kapitel darauf, Anregungen, Hinweise und Empfehlungen für die Entwicklung und Umsetzung eines IT-Sicherheitskonzepts zu geben.

1.1 Notwendigkeit und Bestandteile eines IT-Sicherheitskonzepts

1.1.1 Notwendigkeit der Entwicklung eines IT-Sicherheitskonzepts

Noch zu Beginn der achtziger Jahre war die Informationstechnik (IT) im Wesentlichen durch Zentralrechner bestimmt, die in den Rechenzentren in besonders gesicherten Räumen von dafür geschultem Personal betrieben wurden. Verbindungen dieser Rechner über die Grenzen der Institution hinweg waren eher die Ausnahme; die IT-Sicherheit wurde nahezu ausschließlich durch wenige autorisierte Nutzer (insider) gefährdet, die durch unbeabsichtigtes oder auch vorsätzliches Fehlverhalten Probleme heraufbeschworen.

Inzwischen hat sich die IT-Landschaft grundlegend gewandelt: Hunderte, ja tausende von Systemen befinden sich über die Hochschule verteilt in den einzelnen Einrichtungen im Einsatz, zumeist eingebunden in ein lokales Netz, welches wiederum in ein hochschulweites Rechnernetz mit Anschluss an das weltweite Internet integriert ist. Diese Systeme werden in der Regel von nicht zu diesem Zweck eingestellten Mitarbeitern quasi nebenamtlich

und vorwiegend ohne ausreichende Schulung administriert, denen häufig nicht bewusst ist, dass ihr Rechner von überall her Zielscheibe für ein Eindringen in das System, für das Ausspähen sensibler Daten, für deren Diebstahl, Veränderung oder Vernichtung, für das Einschleusen von schadenbringenden Programmen (Viren) und vieles andere mehr sein kann, bei dem der Eindringling ohne wirksame Sicherheitsmaßnahmen ein leichtes Spiel hat. Ohne eine gründliche Analyse der möglichen Bedrohungen, eine Abschätzung ihrer Eintrittswahrscheinlichkeit sowie eine Bewertung des jeweils denkbaren Schadens lässt sich das Risiko für den Betrieb der eigenen IT nicht kalkulieren. Ohne die Festlegung von Verfahren und Handlungsweisen, wie bei Eintritt eines Schadensereignisses zu agieren ist, welche Gegenmaßnahmen, welche Schritte zur Beweissicherung und zur Information der zuständigen Stellen zu unternehmen sind, wird eine überlegte, sachgemäße und den Umständen angemessene Reaktion kaum möglich sein. Dabei genügt es wegen der Anbindung eines Systems an das Internet nicht, wenn sich dessen Systemadministrator ein isoliertes IT-Sicherheitskonzept für sein System zurechtlegt, denn die Kette der im hochschulweiten Rechnernetz bzw. im lokalen Netz der Einrichtung integrierten Systeme ist nur so stark wie ihr schwächstes Glied: Ein nur schwach gesichertes System wird häufig unter Verschleierung der Identität des Eindringlings als Sprungbrett für weitere Attacken gegen andere Systeme im Internet missbraucht, die dann der Institution angelastet werden, die dieses Sprungbrett-System betreibt, mit allen negativen Folgen für die Reputation der Einrichtung bis hin zu rechtlichen Konsequenzen. Deshalb müssen in jedem Subnetz die IT-Sicherheitsziele an dem System mit dem höchsten Schutzbedarf ausgerichtet werden; alle Systeme in diesem Subnetz sollten ein annähernd gleiches Sicherheitsniveau besitzen.

Um den Schutzbedarf eines Systems, einer Anwendung, eines Netzes ermitteln und das angestrebte oder erreichte Sicherheitsniveau einigermaßen abschätzen zu können und um beim Eintreten eines Schadensereignisses angemessen zu handeln, bedarf es also der Entwicklung eines IT-Sicherheitskonzepts. Wegen der möglichen weitreichenden Auswirkungen auf die gesamte Einrichtung muss die Verantwortung für diese Aufgabe von den Entscheidungsträgern der Einrichtung in Zusammenarbeit mit dem IT-Management, d.h. den für das Netz-, System- und Applikationsmanagement Verantwortlichen wahrgenommen werden. Dabei wird das Gelingen dieses Vorhabens wesentlich auch davon beeinflusst, welchen Stellenwert die Hochschul- bzw. Klinikleitung der IT-Sicherheit einräumt und welche personellen und finanziellen Ressourcen dazu bereitgestellt werden.

1.1.2 Wesentliche Bestandteile eines IT-Sicherheitskonzepts

Ein IT-Sicherheitskonzept besteht im Wesentlichen aus folgenden Komponenten:

- IT-Sicherheitsziele
- IT-Sicherheitsrichtlinien
- IT-Sicherheitsprozeduren

IT-Sicherheitsziele

Vor einer möglichen Festlegung der Randbedingungen für den Einsatz der Informationsverarbeitung in einer Institution und insbesondere vor einer konkreten Auswahl der einzusetzenden IT-Sicherheitsprozeduren müssen die Ziele im Hinblick auf die IT-Sicherheit insgesamt und das dabei anzustrebende Sicherheitsniveau festgelegt werden.

Grundlage dafür bildet die sorgfältige Analyse der in die Informationsverarbeitung involvierten Objekte sowie der gegen sie gerichteten Bedrohungen nach folgendem Schema:

- Ermittlung der gegebenenfalls bedrohten, zu schützenden Objekte und Werte;
- Analyse der möglichen Bedrohungen;
- Risikoabschätzung möglicher Bedrohungen
  [Abschätzung ihrer Eintrittswahrscheinlichkeit sowie der möglichen Schadenshöhe];
- Kosten-/Nutzenanalyse für den Aufwand an Sicherheitsmaßnahmen.

Diese Analyse orientiert sich dabei an den folgenden Sicherheitskriterien:

- *Vertraulichkeit (confidentiality):*
  Die Daten und ihre Übertragungswege sind vor unbefugtem Zugriff zu schützen;
- *Integrität (integrity):*
  Die Daten sind vor Veränderung, Verlust oder Zerstörung zu schützen;
- *Verfügbarkeit (availability):*
  Die IT-Systeme und -Dienste müssen in der vorgesehenen Leistungsfähigkeit ohne Beeinträchtigung zur Verfügung stehen;
- *Nachweisbarkeit (verification) bzw. Nicht-Abstreitbarkeit (non-repudiation):*
  Die Urheber jeglicher Aktionen im IT-System müssen zu jeder Zeit identifizierbar und nachweisbar sein;
- *Ordnungsmäßigkeit:*
  Die Nutzung der IT hat nur durch dazu Autorisierte und nur gemäß der vorgegebenen Bestimmung zu geschehen.

IT-Sicherheitsrichtlinien

Die IT-Sicherheitsrichtlinien legen die Rahmenbedingungen und Regeln fest, nach denen eine an den definierten Sicherheitszielen orientierte Informationsverarbeitung zu erfolgen hat. Sie beschreiben insbesondere die Rechte, Pflichten und zulässigen Verhaltensweisen der Benutzer sowie der Systemadministratoren der einzelnen IT-Systeme und der diese verbindenden Netze. Sie sorgen darüber hinaus für eine Klassifizierung der anfallenden Daten im Hinblick auf ihre Schutzwürdigkeit und schreiben verbindlich vor, welche Maßnahmen zur Sicherstellung ihrer Integrität und Vertraulichkeit durchzuführen sind. Außerdem enthalten sie ein Konzept für die Reaktion auf eingetretene Sicherheitsvorfälle (Schadensereignisse) sowie eine Vorgehensweise für die kontinuierliche Fortschreibung des IT-Sicherheitskonzepts einschließlich der Sicherheitsüberprüfung und der Beseitigung von Schwachstellen.

IT-Sicherheitsprozeduren

In Abhängigkeit von dem jeweiligen Entwicklungsstand der Informationstechnologie werden konkrete technische Verfahren und Prozeduren zur Umsetzung der Sicherheitsrichtlinien und zur Realisierung des angestrebten Sicherheitsniveaus festgelegt, die vor allem in den folgenden Bereichen zum Einsatz gelangen:

- *Authentifizierung:*
  gegenseitiger Nachweis der Identität der in einen konkreten Informationsverarbeitungsprozess involvierten Personen und Systeme; Kontrolle des eingesetzten Authentifizierungsmediums (z.B. Chipkarte) gegen Missbrauch, Verlust, Vergesslichkeit;
- *Zugangsregelung:*
  zentrale Zugangskontrolle über alle Systeme und Applikationen einer Einrichtung (zentraler Berechtigungsserver und Single-Signon); Zugangsregelung zu Teilen einer Anwendung; Zeitkontrolle bestehender Client/Server-Verbindungen auf Inaktivität;
- *Zugriffskontrolle:*
  Kontrolle der unterschiedlichen Privilegien für den Zugriff auf Dateien oder einzelne Datenelemente;
- *Bereitstellung zertifizierter Software:*
  zentrale Auslieferung von zertifizierter und beglaubigter Software (trusted software);
- *Abschottung von Subnetzen:*
  Einsatz von Firewalls zur Absicherung von Subnetzen;
- *Verschlüsselung und Signierung von Daten:*
  Verschlüsselung besonders schützenswerter oder gefährdeter Daten bei der Speicherung und/oder Übertragung; Erstellung signierter Dokumente (Notariatsfunktion); Ermöglichung von (rechts-)verbindlichen elektronischen Vorgängen; Verwaltung und Distribution der geheimen und öffentlichen Schlüssel (key management);
- *Sicherheitsmanagement und -überwachung:*
  laufende Dokumentation und Kontrolle aller relevanten Aktionen im IT-Gesamtsystem; gezielte Überprüfung der Wirksamkeit der getroffenen Sicherheitsmaßnahmen.

1.1.3 Organisatorische Rahmenbedingungen für die Erstellung eines IT-Sicherheitskonzepts

Die Vorgehensweise bei der Erstellung eines IT-Sicherheitskonzepts wird nicht unwesentlich von der Struktur und Größe einer Institution beeinflusst. Während es in einer kleinen Universität, in der die Verantwortung für die gesamte Informationsverarbeitung z.B. im Universitätsrechenzentrum konzentriert ist, möglich und sinnvoll ist, durch ein zentrales Sicherheitsmanagement-Team ein für die gesamte Institution verbindliches, zentrales IT-Sicherheitskonzept zu erarbeiten, wird man beispielsweise in einer großen medizinischen Einrichtung, die aus mehreren relativ autonomen Kliniken und medizinischen Instituten besteht, einen anderen Weg beschreiten müssen: Auf der Basis globaler, von allen Teilinstitutionen anerkannter Sicherheitsvorgaben wird jeder Teilbereich sein eigenes Sicher-

heitskonzept entwickeln, das durch ein gemeinsames Sicherheitsmanagement-Team in ein Gesamtkonzept mit verteilter Verantwortlichkeit zu integrieren ist. Bei der Erstellung des IT-Sicherheitskonzepts sollten gegebenenfalls externe Experten in den Erarbeitungsprozess einbezogen werden, zum einen um die Personalkapazitäten der eigenen Institution zu entlasten, zum anderen um einer leicht möglichen Betriebsblindheit gegenüber den Sicherheitsdefiziten der eigenen IT-Infrastruktur entgegenzuwirken.

Wegen der besonderen Verantwortung, die mit der Erstellung, der Realisierung, der Durchsetzung sowie der kontinuierlichen Überwachung und Fortschreibung eines IT-Sicherheitskonzepts verbunden ist, erscheint es sinnvoll, diese Aufgabe nicht einem einzelnen Sicherheits-Administrator sondern einem **Sicherheitsmanagement-Team** zu übertragen, das sich aus IT-Spezialisten, Datenschutzbeauftragtem und Vertretern der Hochschulleitung zusammensetzt. Diese Zusammensetzung bietet eine gute Voraussetzung dafür, dass IT-Sicherheitsrichtlinien aufgestellt werden, die rechtlich abgesichert und politisch in der Institution durchsetzbar sind und die zusammen mit den daraus resultierenden IT-Sicherheitsprozeduren auch technisch realisierbar sind. Dabei ist offenkundig, dass sowohl punktuell für die Erstellung und Durchsetzung des IT-Sicherheitskonzepts als auch kontinuierlich für seine Realisierung, Überwachung und Fortschreibung sowie für die Behandlung und spätere Aufarbeitung von konkreten Sicherheitsvorfällen personelle Kapazitäten in ausreichender Größenordnung zur Verfügung stehen müssen.

Wesentlich für die spätere Akzeptanz des IT-Sicherheitskonzepts ist die frühzeitige Einbindung aller relevanten Gruppen der davon Betroffenen (Personalrat, Benutzervertreter, etc.) in den Entstehungsprozess. Ebenso wichtig ist es, alle Benutzer detailliert über die für sie verbindlichen IT-Sicherheitsrichtlinien zu informieren und durch regelmäßige Fortbildungsmaßnahmen ein entsprechendes Sicherheitsbewusstsein aufzubauen und zu stärken.

1.2 Schritte für die Entwicklung eines IT-Sicherheitskonzepts

1.2.1 Analyse der IT-Sicherheitsrisiken

Wie bereits in Abschnitt 1.1.2 angedeutet wurde, besteht der erste Schritt bei der Entwicklung eines IT-Sicherheitskonzepts darin, auf der Grundlage der festgelegten Sicherheitsziele die Risiken für die IT-Sicherheit abzuschätzen, d.h. die zu schützenden Objekte und Werte sowie die gegen sie gerichteten Bedrohungen zu analysieren. Darüber hinaus sind diese Bedrohungen im Hinblick auf ihre Eintrittswahrscheinlichkeit und mögliche Schadenshöhe zu bewerten.

Personen, Objekte und Werte

Ein wichtiger Bestandteil einer sorgfältigen Risikoanalyse ist die Identifizierung aller Personen, Objekte und Werte, die von Sicherheitsproblemen tangiert werden könnten. Dabei ist ein möglichst hoher Grad an Vollständigkeit anzustreben, was durch den Einsatz systematischer Checklisten, wie sie beispielsweise im IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik /BSI96/ angeboten werden, wesentlich erleichtert wird. Folgende Objektkategorien liegen dabei nahe (nach /Fraser97/):

- *Hardware:*
  CPUs, Boards, Tastaturen, Bandlaufwerke, Diskettenlaufwerke, Terminals, PCs, Workstations, Drucker, Router, Switches, Modems, ISDN-Adapter, Datenleitungen, etc.
- *Software:*
  Betriebssysteme, Utilities, Diagnoseprogramme, Kommunikationsprogramme, Anwendungsprogramme, etc.
- *Personen:*
  Nutzer, Systemadministratoren, Wartungspersonal, etc.
- *Daten:*
  während der Bearbeitung, während des Transits über Datenleitungen, im Online-Zugriff auf einem Datenträger, offline gespeichert auf einem Archiv-/Backup-Datenträger, in einem Datenbank-System;
  Patientendaten, Personaldaten, Forschungsdaten, Protokolldateien, etc.
- *Dokumentationen:*
  über Programme, Hardware, Verfahren der Systemadministration, angewandte IT-Sicherheitsprozeduren, Notfallkonzepte, etc.
- *Materialien:*
  Papier, Formulare, Drucktücher, Magnetbänder, etc.

Bedrohungen

Anhand der bereits aufgezeigten IT-Sicherheitskriterien der *Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit* und *Ordnungsmäßigkeit* lässt sich eine systematische Übersicht über die möglichen Bedrohungen und Gefährdungspotentiale erarbeiten. Zumindest folgende klassischen Bedrohungen sind dabei zu berücksichtigen:

- nicht autorisierter Zugang zu Systemen und Ressourcen;
- unerlaubter Zugriff auf Daten und Programme;
- Diebstahl, Veränderung und Löschung schützenswerter Informationen;
- Attacken, die die Zuverlässigkeit eines Dienstes beeinträchtigen oder seine Erbringung völlig unmöglich machen;
- Verschleierung der eigenen Identität und Beseitigung von Spuren eigener Aktionen durch Fälschung von Identifikationsmerkmalen und Protokolldateien (Audit-Daten).

Um auch hierbei zu einer möglichst umfassenden Auflistung zu gelangen, kann es hilfreich sein, die möglichen Bedrohungen und Gefährdungspotentiale zusätzlich unter einem von den IT-Sicherheitskriterien völlig verschiedenen Kategorienschema zu betrachten, wie es beispielsweise das IT-Grundschutzhandbuch /BSI96/ verwendet:

- *Höhere Gewalt*
- *Organisatorische Mängel*
- *Menschliche Fehlhandlungen*
- *Technisches Versagen*
- *Vorsätzliche Attacken*

Bewertung

Bei der Bewertung der IT-Sicherheitsrisiken geht es darum, die Eintrittswahrscheinlichkeit möglicher Schadensereignisse sowie die Höhe des potentiellen Schadens abzuschätzen. Dabei sind sowohl finanzielle Verluste durch ein Schadensereignis als auch die Kosten für die Wiederherstellung eines ordnungsgemäßen Betriebs der IT-Infrastruktur als auch immaterielle Schäden wie die Minderung des Ansehens oder der Verlust der Vertrauenswürdigkeit zu berücksichtigen.

Je nach möglicher Höhe und Auswirkung eines Schadens wird man die Objekte (IT-Systeme, Anwendungen, etc.) in verschiedene Klassen einteilen, wobei jeder Klasse eine unterschiedliche Stufe des für die Objekte dieser Klasse zu erreichenden Sicherheitsniveaus entspricht (siehe auch Kapitel 2).

Kosten-/Nutzenanalyse

Auch bei Maßnahmen zur Verbesserung der IT-Sicherheit ist das Prinzip der Angemessenheit und Wirtschaftlichkeit zu beachten. Dies bedeutet, dass die Aufwendungen für die Sicherung eines Objekts in einem angemessenen Verhältnis zum Wert des Objekts sowie zur Höhe des möglicherweise bei diesem Objekt eintretenden Schadens stehen müssen.

1.2.2 IT-Sicherheitsrichtlinien: Detailfestlegungen im IT-Sicherheitskonzept

Die IT-Sicherheitsrichtlinien bilden das Regelwerk aus Rahmenbedingungen und konkreten Handlungsanweisungen für den ordnungsgemäßen Einsatz der IT-Systeme und -Verfahren. Sie müssen

- die Rechte, Pflichten und Verantwortungsbereiche von Nutzern, Systemadministratoren und Management klar definieren,
- umsetzbar sein durch organisatorische Maßnahmen, durch Verfahren der Systemadministration, durch Leitfäden und Anleitungen zur ordnungsgemäßen Nutzung,

- durchsetzbar sein, vorrangig mit Hilfe von IT-Sicherheitsprozeduren und -tools, jedoch erforderlichenfalls auch durch Sanktionen.

IT-Sicherheitsrichtlinien treffen Detailfestlegungen in einer Vielzahl von Bereichen:

- Beschaffungen:
  Welche Sicherheitskriterien oder -eigenschaften sind bei der Beschaffung eines IT-Systems in Abhängigkeit vom Einsatzzweck als notwendig oder wünschenswert anzusehen?
- Vertraulichkeit:
  Wie sind schutzwürdige vertrauliche Informationen zu behandeln? Welche Benutzeraktivitäten werden protokolliert und unter welchen Voraussetzungen dürfen diese Daten ausgewertet werden? Wer hat unter welchen Bedingungen umfassenden Zugriff auf die Dateien eines Benutzers?
- Zugang und Nutzung:
  Wer darf welche Ressourcen nutzen? Was ist eine bestimmungsgemäße Nutzung der Ressourcen? Wer ist autorisiert, Zugangs- und Zugriffsrechte zu vergeben und Nutzungsgenehmigungen zu erteilen? Welche Rechte und Pflichten haben die Nutzer eines IT-Systems? Welche besonderen Vorkehrungen sind beim Zugang über öffentliche (unsichere) Netze zu treffen? Wer darf neue Software zur allgemeinen Nutzung in ein IT-System einbringen?
- Authentifizierung:
  Welche Kriterien sind bei der Auswahl von Passwörtern zu beachten? In welchen Situationen bzw. bei welchen Anwendungen sind stärkere Authentifizierungsmechanismen (Einmal-Passwörter, Challenge-Response-Verfahren, SmartCards, etc.) zu verwenden?
- Systemadministration:
  Wer darf auf welchen Systemen das Privileg des Systemadministrators besitzen? Welche Rechte und Pflichten hat das Sicherheitsmanagement-Team gegenüber den Systemadministratoren? Welche Rechte und Pflichten haben Systemadministratoren gegenüber den Nutzern des von ihnen verwalteten Systems? Welche Aktivitäten und Ereignisse auf dem IT-System sind zu protokollieren? Nach welchen Kriterien und mit welchen Hilfsmitteln werden diese Audit-Daten in welchen Intervallen ausgewertet?
- Verfügbarkeit:
  Welchen Grad an Verfügbarkeit der IT-Systeme können die Nutzer erwarten? Durch welche Maßnahmen (redundante Auslegung der Systeme, etc.) wird dies sichergestellt?
- Wartung und Instandhaltung:
  In welcher Form erhält internes oder externes Wartungspersonal Zugang zu den IT-Systemen? Wie werden Wartungsaktivitäten kontrolliert und protokolliert? Dürfen Wartungsaktivitäten nur über die Systemkonsole oder auch über sonstige (unsichere) Datenverbindungen veranlasst werden?
- Information:
  Welche rechtlichen Rahmenbedingungen und Gesetze sind beim Einsatz der IT-

Systeme zu beachten? Welche Sicherheitsvorfälle sind an welche Stellen zu melden? Wer ist verantwortlich für die Benachrichtigung anderer eventuell betroffener Institutionen? Durch wen und in welchem Umfang wird die Öffentlichkeit/Presse über Sicherheitsvorfälle informiert?

Darüber hinaus enthalten die IT-Sicherheitsrichtlinien weitere, nicht zur allgemeinen Veröffentlichung bestimmte Festlegungen über die IT-Sicherheitsverfahren und -prozeduren, die zur Prävention gegen Gefährdungspotentiale und Bedrohungen eingesetzt werden (siehe 1.3), sowie über die konkreten Verfahrensweisen und Maßnahmen, die beim Auftreten von Sicherheitsproblemen zu ergreifen sind (siehe 1.5). Außerdem ist schließlich die Vorgehensweise festzulegen, wie eingetretene Schadensereignisse und die darauf erfolgten Reaktionen im Nachhinein analysiert und aufgearbeitet werden (siehe 1.5.3).

1.2.3 Verbreiten und Interpretieren des IT-Sicherheitskonzepts

Schon in der Phase seiner Entstehung sollte das IT-Sicherheitskonzept mit allen später davon betroffenen Gruppen (Nutzern, Systemadministratoren, Management, etc.) eingehend erörtert werden, um bereits von Anfang an ein möglichst hohes Maß an Akzeptanz zu erreichen. Dies muss insbesondere die rechtzeitige Mitwirkung des Personalrats und des Datenschutzbeauftragten mit einschließen.

Nach der Verabschiedung des IT-Sicherheitskonzepts und vor seiner formellen Inkraftsetzung sind alle Betroffenen in speziellen Informations- und Schulungsveranstaltungen mit den Details des Konzepts und insbesondere mit den IT-Sicherheitsrichtlinien vertraut zu machen. Dabei sollte auch bekannt gegeben werden, auf welche Weise Probleme bei der konkreten Umsetzung des Sicherheitskonzepts oder Verbesserungsvorschläge dem IT-Sicherheitsmanagement-Team mitgeteilt werden können. Um die Wichtigkeit des Themas IT-Sicherheit zu unterstreichen, muss die Hochschulleitung in diesen Informationsprozess mit eingebunden werden.

Mit dem Inkrafttreten des IT-Sicherheitskonzepts sind alle Betroffenen auf dessen Beachtung und auf die Einhaltung der IT-Sicherheitsrichtlinien formell zu verpflichten. Jedem muss dabei deutlich sein, welche Konsequenzen ein Verstoß gegen die IT-Sicherheitsrichtlinien nach sich zieht.

Zur Auslegung und Interpretation des IT-Sicherheitskonzepts in Zweifelsfällen ist eine Schiedsstelle einzurichten. Diese Funktion sollte zweckmäßigerweise vom IT-Sicherheitsmanagement-Team wahrgenommen werden, damit notwendige Auslegungen und Klarstellungen bei der Fortschreibung des IT-Sicherheitskonzepts unmittelbar berücksichtigt werden können.

1.3 Verfahren und Prozeduren zur Prävention gegen Sicherheitsprobleme

Oberstes Ziel eines IT-Sicherheitskonzepts ist es, Sicherheitsprobleme möglichst gar nicht erst entstehen zu lassen. Deshalb kommt organisatorischen Maßnahmen (siehe Kapitel 10) und vor allem technischen Verfahren und Prozeduren, die der Prävention gegen Sicherheitsprobleme und der konkreten Gefahrenabwehr dienen, besondere Bedeutung zu. Wegen der stürmischen Entwicklung sowohl bei Bedrohungen und Gefährdungspotentialen als auch bei den dagegen gerichteten Sicherheitsprozeduren und -tools weist dieser Bereich des IT-Sicherheitskonzepts sicherlich den größten Aktualisierungs- und Fortschreibungsbedarf auf. Deshalb können die im Teil II dieses Berichts aufgezeigten Lösungsansätze in den Bereichen der Virtualisierung der Netze (Kapitel 4), der Netzabsicherung durch Firewalls (Kapitel 5), der Verschlüsselung vertraulicher oder sensibler Daten (Kapitel 6), der sicheren Betriebssysteme und Basisdienste (Kapitel 7), der Zugangs- und Zugriffskontrollen (Kapitel 8) sowie des Netz- und Systemmanagements (Kapitel 9) allenfalls eine Momentaufnahme über die zur Zeit verfügbaren bzw. in nächster Zukunft absehbaren Prozeduren und Tools zur Verbesserung der IT-Sicherheit darstellen. Durch kontinuierliche Beobachtung der einschlägigen Veröffentlichungen muss das IT-Sicherheitsmanagement-Team versuchen, die konkreten Festlegungen und Empfehlungen des IT-Sicherheitskonzepts zu den einzusetzenden Sicherheitstools auf dem aktuellen Stand der Technik zu halten.

1.4 Festlegung der Aktivitäten zur Sicherheitsüberwachung

Selbstverständlich genügt es nicht, von der Wirksamkeit der getroffenen Sicherheitsmaßnahmen überzeugt zu sein. Getreu nach der Devise „Vertrauen ist gut, Kontrolle ist besser“ muss vielmehr eine kontinuierliche Überwachung der IT-Sicherheit erfolgen. Eine detaillierte Festlegung der konkreten Aktivitäten zur Sicherheitsüberwachung gehört daher unverzichtbar zum IT-Sicherheitskonzept.

Ein Ansatzpunkt ist dabei, die ohnehin (zumindest in Ansätzen) vorhandenen Verfahren und Werkzeuge des Netz- und Systemmanagements zu einem integrierten Sicherheitsmanagement zu erweitern. Die hierzu verfügbaren Lösungen und absehbaren Entwicklungen werden im Kapitel 9 ausführlich behandelt.

Ein wichtiger Bereich dieses Sicherheitsmanagements besteht darin, für jedes IT-System festzulegen, welche Ereignisse und Aktivitäten in welcher Form protokolliert werden und in welchen Situationen darüber hinaus ein Alarm ausgelöst wird. Bei der Aufzeichnung solcher Audit-Daten sind verschiedene Aspekte zu berücksichtigen: das Aufzeichnungsmedium (normale Festplatte mit dem Risiko der Manipulation und Löschung der Audit-Daten; einmal beschreibbare CD-ROM; Ausgabe auf Papier über einen Drucker); die Sicherung der Datenübertragung zwischen dem IT-System, in dem die Audit-Daten anfallen, und dem

Aufzeichnungssystem; die Menge der Audit-Daten (Risiko des Überlaufs des für die Aufzeichnung verfügbaren Speicherplatzes) und eventuelle Verfahren zu ihrer Verdichtung; die regelmäßige Auswertung der Audit-Daten unter Zuhilfenahme leistungsfähiger Werkzeuge; die gesicherte Aufbewahrung von Datenträgern mit Audit-Daten; rechtliche Implikationen bei der Aufzeichnung und Auswertung personenbezogener Audit-Daten.

Während Audit-Daten Hinweise auf konkrete Sicherheitsvorfälle geben und damit Reaktionen darauf veranlassen können (siehe 1.5), gehört die Durchführung von Sicherheits-Checks zu den proaktiven Verfahren des Sicherheitsmanagements. Im Rahmen des IT-Sicherheitskonzepts ist hier im Einzelnen festzulegen, welche Werkzeuge zur Sicherheitsüberprüfung von Routern, Firewalls, Betriebssystemen, Diensten, Passwörtern, etc. in welchen Intervallen angewendet werden und wer (Systemadministratoren, Sicherheitsmanagement-Team, externes Test-Team) diese Sicherheits-Checks durchführen darf.

1.5 Konkrete Verfahrensweisen beim Auftreten von Sicherheitsproblemen

Damit beim Auftreten von Sicherheitsproblemen bzw. beim Eintritt eines konkreten Schadensereignisses nicht in Hektik Entscheidungen getroffen und Maßnahmen ergriffen werden, die eventuell den Schaden noch vergrößern, Hinweise auf die Schadensursache(n) oder sonstiges Beweismaterial vernichten, die Sicherung wertvoller Daten verhindern oder den geordneten Wiederanlauf erschweren, bedarf es eines detaillierten Plans zur Behandlung von Sicherheitsvorfällen. Dazu gehören sowohl vorbereitende Planungen und Festlegungen von Verantwortlichkeiten als auch konkrete Handlungsanweisungen für die Bewertung und Behandlung eines laufenden Schadensereignisses als auch schließlich die nachträgliche Aufarbeitung eingetretener Schadensereignisse und ihrer konkreten Behandlung.

1.5.1 Vorbereitende Planungen und Festlegungen

Bei der Behandlung von Sicherheitsvorfällen können eine Reihe ganz unterschiedlicher Zielvorstellungen eine Rolle spielen, wie etwa

- die Ermittlung der Ursache(n) für den Eintritt des Schadensereignisses,
- die zukünftige Vermeidung derselben Bedrohung,
- die Vermeidung einer Eskalation und des Nachsichziehens weiterer Sicherheitsvorfälle,
- die Eingrenzung der Auswirkungen und der Schadenshöhe des Sicherheitsvorfalls,
- die Wiederherstellung eines störungsfreien Betriebs,
- die Ermittlung und Verfolgung des Verursachers,

- die notwendige Aktualisierung des IT-Sicherheitskonzepts sowie der eingesetzten Verfahren, Prozeduren und Werkzeuge.

Da diese Zielvorstellungen gegebenenfalls in Konflikt zueinander stehen können, müssen im IT-Sicherheitskonzept *vorab* Prioritäten festgelegt oder zumindest Kriterien für eine Abwägung im konkreten Einzelfall aufgestellt werden. So sollten beispielsweise Kriterien für die Entscheidung vorgegeben sein, ob eine laufende Attacke weiter beobachtet wird, um den Angreifer zu ermitteln und für die spätere Verfolgung Beweise zu sammeln, oder ob zur Vermeidung größerer Schäden die Attacke sofort gestoppt werden muss (durch Trennung des IT-Systems vom Netz oder durch Abschalten des IT-Systems mit anschließender Sanierung von einem nicht-kompromittierten Backup). Da es angesichts der möglichen Komplexität eines Sicherheitsvorfalls unmöglich sein kann, alle erforderlichen Aktivitäten gleichzeitig durchzuführen, ist auch für die Reihenfolge eine eindeutige Prioritätenvorgabe erforderlich:

1. Schutz von Menschenleben und Gewährleistung der Sicherheit von Personen;
2. Schutz geheimer oder sensibler Daten; Abschotten von Subnetzen und Systemen mit derartigen Daten; Information über ein erfolgreiches Eindringen in derartige Netze, Systeme und Datenbestände an die für diese Bereiche Verantwortlichen;
3. Schutz sonstiger Datenbestände; Abschottung von Subnetzen und Systemen mit derartigen Daten; Information der Systemverantwortlichen über eine erfolgreiche Penetration;
4. Schutz vor Schäden an Hardware und Software;
5. Minimierung von Betriebsunterbrechungen bei Netzen und Systemen.

Zuständigkeiten und Kontaktstellen

Da bei einem konkreten Sicherheitsvorfall verschiedene IT-Systeme einer Institution betroffen sein können, werden bei der Behandlung eines Schadensereignisses verschiedene Systemadministratoren sowie Mitarbeiter des Managements, der Rechtsabteilung, des Pressereferats, etc. involviert sein. Deshalb muss im IT-Sicherheitskonzept festgelegt sein, wer die Gesamtverantwortung für die zu treffenden Einzelentscheidungen und die zu ergreifenden Maßnahmen trägt und den Einsatz der beteiligten Stellen und Personen koordiniert. Außerdem sind die Zuständigkeiten für die Durchführung der konkreten Gegenmaßnahmen, die Einschaltung der Strafverfolgungsbehörden, die Benachrichtigung eventuell mitbetroffener externer Institutionen, die Einbindung externer Sicherheitsexperten wie etwa des Computer Emergency Response Teams des DFN (DFN-CERT) oder die Information der Benutzer und der interessierten Öffentlichkeit festzulegen. Dazu gehört selbstverständlich auch eine Liste dieser Kontaktstellen und -personen mit Adressen, Telefonnummern, Faxnummern und E-Mail-Adressen.

Schon vor Eintritt eines Schadensereignisses sollten diese Kontakte geknüpft und gepflegt werden, damit unter den Extrembedingungen eines Sicherheitsvorfalls auf bereits eingefahrene Kommunikationswege zurückgegriffen werden kann.

1.5.2 Identifizierung und Behandlung eines Sicherheitsvorfalls

Bei Verdacht auf Vorliegen eines Sicherheitsvorfalls sollte man zunächst versuchen, diesen Verdacht zu erhärten. Äußerst hilfreich sind dabei sowohl die Audit-Daten als auch vorbereitete Checklisten mit Beschreibungen möglicher Anzeichen und Symptome.

Parallel zur Identifizierung eines Sicherheitsvorfalls sollte eine Bewertung seines Ausmaßes und seiner möglichen Auswirkungen erfolgen. Auch dafür sollte das IT-Sicherheitskonzept eine an den oben genannten Zielvorstellungen und Prioritäten orientierte Checkliste bereithalten.

Auf der Basis dieser Erkenntnisse und Bewertungen wird der für die Behandlung des Sicherheitsvorfalls Verantwortliche bzw. das damit befasste Team Einzelentscheidungen treffen und Maßnahmen ergreifen mit dem Ziel, die Auswirkungen und Schäden zu begrenzen und möglichst bald die vollständige Kontrolle über die betroffenen Systeme zurückzuerlangen. Zur Unterstützung dieser Phase der Notfallbehandlung sollte das IT-Sicherheitskonzept Entscheidungs- und Abwägungshilfen für typische Problem-Szenarien anbieten.

Insbesondere sind dabei folgende Entscheidungen und Maßnahmen vorzusehen:

- Entscheidungen, welche Stellen (Systemadministratoren betroffener Systeme, Rechtsabteilung, Strafverfolgungsbehörden, Pressereferat, DFN-CERT, betroffene externe Institutionen, etc.) über den Sicherheitsvorfall zu informieren sind und umgehende Kontaktaufnahme zu diesen Stellen;
- Bildung/Aktivierung einer Arbeitsgruppe, die diesen konkreten Sicherheitsvorfall bearbeitet;
- Eingrenzung und Abschottung des Angriffs auf die IT-Sicherheit;
- Beseitigung der Ursachen für den Eintritt des Schadensereignisses;
- Sicherung von Beweismaterial;
- Wiederaufnahme des Betriebs in einem gesicherten Zustand;
- weitere Beobachtung und intensive Überwachung der in den Sicherheitsvorfall involvierten Netze und Systeme.

Wo dies möglich ist, sollte das IT-Sicherheitskonzept dazu konkrete Handlungsanweisungen geben.

1.5.3 Aufarbeitung eingetretener Schadensereignisse und ihrer konkreten Behandlung

Um aus den bei der Identifizierung und konkreten Behandlung eines eingetretenen Schadensereignisses gesammelten Erfahrungen für eventuelle spätere Sicherheitsvorfälle zu lernen, ist eine abschließende Aufarbeitung eines jeden Schadensereignisses und seiner Behandlung unverzichtbar. Im IT-Sicherheitskonzept sollten dazu Festlegungen getroffen

werden, in welcher Weise die exakte Abfolge der Ereignisse (Entdeckungsmethode, Informationsentscheidungen, eingeschaltete Stellen, getroffene Maßnahmen, Schadensausmaß, etc.) zu dokumentieren ist. Auf der Basis einer solchen Dokumentation sind im Lichte des konkreten Sicherheitsvorfalls

- eine neue Risikoanalyse,
- eine Ergänzung des IT-Sicherheitskonzepts um zusätzliche Sicherheitsprozeduren und -verfahren

durchzuführen, die geeignet sind, ein erneutes Auftreten desselben Schadensereignisses wirksam zu verhindern oder zumindest weiter zu erschweren. Schließlich ist zu entscheiden, ob die weitere Verfolgung des Verursachers dieses Sicherheitsvorfalls wünschenswert und aufgrund der Beweislage auch erfolgversprechend ist.

1.6 Empfehlungen zum IT-Sicherheitskonzept

- Ausgangspunkt jeglicher Aktivitäten im Bereich der IT-Sicherheit muss die Erstellung eines **IT-Sicherheitskonzepts** sein, in dem die für die Institution relevanten IT-Sicherheitsziele definiert und die organisatorischen Rahmenbedingungen (IT-Sicherheitsrichtlinien) und technischen Maßnahmen (IT-Sicherheitsprozeduren) festgelegt werden, mit denen diese IT-Sicherheitsziele angestrebt werden.
- Wesentlicher Bestandteil des IT-Sicherheitskonzepts muss ein **Notfallplan** sein, der das Vorgehen beim Eintritt sicherheitsrelevanter Ereignisse detailliert festlegt. Dieser Notfallplan soll Regeln für die Identifizierung eines Sicherheitsvorfalls enthalten, die Zuständigkeiten, die Informationspolitik und die Kontaktstellen festlegen sowie Handlungsanweisungen für die konkreten Maßnahmen zur Schadensbegrenzung, zur Beseitigung der Ursachen, zur Beweissicherung bis hin zur Wiederherstellung der Systemintegrität enthalten.
- Die IT-Sicherheitsrichtlinien müssen rechtlich abgesichert sein, was von der Rechtsabteilung der Hochschule gegebenenfalls unter Hinzuziehung von Fachjuristen zu überprüfen ist; sie müssen politisch in der Institution durchsetzbar sein, was die Einbindung der Hochschulleitung wie der Personalvertretung in ihren Entstehungsprozess zwingend erforderlich macht; sie müssen schließlich zusammen mit den daraus resultierenden IT-Sicherheitsprozeduren auch technisch realisierbar sein.
- Alle betroffenen Benutzer der IT-Infrastruktur sind detailliert über die für sie verbindlichen IT-Sicherheitsrichtlinien zu informieren; durch regelmäßige Fortbildungsmaßnahmen ist ein entsprechendes Sicherheitsbewusstsein aufzubauen und zu stärken.
- Aufgrund der ständigen Veränderungen in der IT-Infrastruktur der Hochschule, der rasanten Entwicklung bei den IT-Sicherheitsprozeduren und -werkzeugen aber auch bei den gegen die IT-Sicherheit gerichteten Bedrohungen kann das IT-Sicherheitskonzept kein statisches, ein für alle Mal festgelegtes Regelwerk sein, sondern muss kontinuierlich weiterentwickelt und aktualisiert werden. Insbesondere aber nach Eintritt eines

konkreten Sicherheitsvorfalls ist das IT-Sicherheitskonzept unter Berücksichtigung der bei der Behandlung dieses Schadensereignisses gewonnenen Erfahrung dahingehend zu modifizieren, dass ein erneutes Auftreten desselben Schadensereignisses wirksam verhindert oder zumindest weiter erschwert wird.

- Zur Entwicklung und kontinuierlichen Fortschreibung des IT-Sicherheitskonzepts, zur Behandlung von Sicherheitsvorfällen sowie zur Koordinierung aller mit der IT-Sicherheit zusammenhängenden Aktivitäten ist ein **Sicherheitsmanagement-Team** in der Hochschule zu bilden, das sich aus IT-Spezialisten, dem Datenschutzbeauftragten und Vertretern des Managements zusammensetzt. Dabei ist offenkundig, dass sowohl punktuell für die Erstellung und Durchsetzung des IT-Sicherheitskonzepts als auch kontinuierlich für seine Realisierung, Überwachung und Fortschreibung sowie für die Behandlung und spätere Aufarbeitung von konkreten Sicherheitsvorfällen personelle Kapazitäten in ausreichender Größenordnung zur Verfügung stehen müssen.

1.7 Literatur

Die angegebene Literatur enthält hervorragende Anleitungen zur Erstellung eines IT-Sicherheitskonzepts; sie sollte bei der konkreten Erarbeitung eines derart komplexen Regelwerks unbedingt zu Rate gezogen werden.

/BSI96/ Bundesamt für Sicherheit in der Informationstechnik:
„IT-Grundschutzhandbuch 1996“,
Schriftenreihe zur IT-Sicherheit, Band 3
ISSN 0947-093X

/Holbrook91/ Holbrook, P. / Reynolds, J.:
„Site Security Handbook, RFC 1244“,
July 1991

/Fraser97/ Fraser, B. (ed.):
„Site Security Handbook, RFC 2196 “,
September 1997
`ftp://ds.internic.net/rfc/rfc2196.txt`

/Sturm97/ Sturm, T.:
„Eine Sicherheitspolitik für offene Netze“,
Diplomarbeit Universität Erlangen-Nürnberg, Februar 1997

Kapitel 2

Anforderungen aus dem Verwaltungs- und Klinikbereich an die Netz- und Systemsicherheit

Bei der Anbindung der sensiblen Bereiche Hochschulverwaltungen und Universitätskliniken an ungeschützte öffentliche Netze müssen eine Reihe von Anforderungen an die Sicherheit gestellt werden. Geltende Gesetze und Verordnungen bilden dafür den rechtlichen Rahmen. Auf sie soll in Abschnitt 2.1 eingegangen werden. In Abschnitt 2.2 wird die Vorgehensweise bei der Anforderungsbetrachtung erläutert. Bei der Diskussion der Anforderungen wird zwischen Basisdiensten im Internet, die von der Hochschulverwaltung oder der Klinik genutzt werden (Abschnitt 2.3), und Diensten, die von der Verwaltung oder Klinik im Internet für ihre Kunden angeboten werden (Abschnitt 2.4), unterschieden. Als besonderes Szenario muss die Verbindung abgesicherter Verwaltungs- oder Kliniknetze über unsichere öffentliche Netze hinweg betrachtet werden (Abschnitt 2.5). In Abschnitt 2.6 finden sich Literaturhinweise.

2.1 Der rechtliche Rahmen

Die Anforderungen von Verwaltungen und Kliniken an die Sicherheit der IT-Anbindung an öffentliche Netze ergeben sich zunächst einmal für beide Bereiche gleichermaßen aus den einschlägigen Gesetzen und sonstigen rechtlichen Rahmenbedingungen. Bei Überschneidungen haben jeweils Vorrang das Strafgesetzbuch (StGB), das Sozialgesetzbuch (SGB), die Länderdatenschutzgesetze (z.B. BayDSG) sowie, für den Klinikbereich wichtig, die Länderkrankenhausgesetze (z.B. BayKrG). Neue, für die elektronische Kommunikation äußerst bedeutsame rechtliche Grundlagen sind das Telekommunikationsgesetz (TKG), die Gesetze und Verordnungen zur elektronischen Signatur (SigG, SigVO) und die in der Entwicklung befindliche Verordnung über Elektronische Unterschrift (VEU). Eine Kommission des Bayerischen Staatsministeriums für Unterricht, Kultus, Wissenschaft und

Kunst, die sich mit Zugangs- und Nutzungsregelungen für die bayerischen Hochschulnetze beschäftigte, hat einen Bericht /BSTUKWK97/ erstellt, der die rechtlichen Rahmenbedingungen für den Datenverkehr innerhalb einer Hochschule beschreibt.

2.1.1 Ausspähen von Daten

In §202a StGB wird der Straftatbestand des Ausspähens vertraulicher Daten definiert. Hier heißt es:

> *(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.*
>
> *(2) Daten im Sinn des Abs. 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.*

Auf die Datenübermittlung wird hier also expressis verbis hingewiesen.

2.1.2 Ärztliche Schweigepflicht

Die sogenannte ärztliche Schweigepflicht, die bei der Einhaltung des Datenschutzes im Gesundheitswesen eine zentrale Rolle spielt, leitet sich ab von §203 StGB Verletzung von Privatgeheimnissen. Dort heißt es:

> *(1) Wer unbefugt ein Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- und Geschäftsgeheimnis, offenbart, das ihm als 1. Arzt, [...] 2. Berufspsychologen [...] 3. Rechtsanwalt, [...] 6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.*

Man vergleiche dazu auch §353b StGB Verletzung von Dienstgeheimnissen.

2.1.3 Computerbetrug

Betrügerische Handlungen im Zusammenhang mit computergespeicherten Daten werden im §263a StGB als Straftatbestand formuliert. Dort heißt es:

> *(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs [...] durch Verwendung unrichtiger Daten, durch unbefugtes Verwenden von Daten [...] beeinflusst, wird mit Freiheitsstrafe bis zu 5 Jahren oder mit Geldstrafe bestraft.*

2.1.4 Datenmanipulation

Im Zusammenhang mit dem Manipulieren von Daten definiert das StGB mehrere Straftatbestände. Die Fälschung beweiserheblicher Daten regelt §269 StGB. Er lautet:

> *(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.*
>
> *(2) Der Versuch ist strafbar.*
>
> *(3) §267 Abs. 3 ist anzuwenden (Urkundenfälschung).*

In §270 StGB wird des weiteren festgelegt, dass der Täuschung im Rechtsverkehr die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleichsteht. Zur Datenveränderung führt §303a aus:

> *(1) Wer rechtswidrig Daten [...] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.*

Zur Sachbeschädigung heißt es in §303:

> *(1) Wer rechtswidrig eine fremde Sache beschädigt oder zerstört, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.*

Als weiteren Tatbestand findet man in §303b die Computersabotage:

> *(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er 1. eine Tat nach 303a Abs. 1 begeht oder 2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.*

In jedem der drei zuletzt genannten Tatbestände ist bereits der Versuch strafbar.

2.1.5 Gesundheitsstrukturgesetz

Für die Kliniken brachte das Gesundheitsstrukturgesetz in Form der Regelungen im SGB V – Krankenversicherungen §§284-305 erhebliche Veränderungen ihrer rechtlichen Rahmenbedingungen. Im Kontext der Datenkommunikation ergab sich als einschneidende Änderung die in §301 neu geregelte Datenübermittlung an die Krankenkassen. Die elektronische Übermittlung fallbezogener Leistungsdaten wurde für alle Kliniken zur Pflicht.

2.1.6 Outsourcing im Krankenhaus

Die Verarbeitung von medizinischen Patientendaten, also Daten der medizinischen Dokumentation (Anamnese, Diagnosen, Therapieverläufe) im Auftrag ist gemäß Art. 27 BayKrG in Bayern nur in einem anderen Krankenhaus zulässig. Diese Beschränkung gilt nicht für die Daten der Krankenhausverwaltung.

2.1.7 Zweckbindung bei Patientendaten

Patientendaten dürfen nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden. Jegliche andere Nutzung, z.B. für Forschungszwecke oder im Rahmen von Informationsdiensten, etwa im WWW, bedarf der Einwilligung des Patienten. Probleme ganz besonderer Art werfen in diesem Zusammenhang klinische Multicenterstudien auf.

2.1.8 Online-Übertragung personenbezogener Daten

In Art. 8 BayDSG Einrichtung automatischer Abrufverfahren heißt es hierzu:

> *(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten an Dritte durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.*
>
> *(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann.*

Unter die personenbezogenen Daten fallen insbesondere Patientendaten. Dies ist in *Art. 27 BayKrG Datenschutz* ausdrücklich geregelt. Dort heißt es:

> *(1) Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich der Krankenhäuser. Soweit in diesem Gesetz nichts anderes bestimmt ist, sind auf Patientendaten die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden.*

2.2 Definition der Anforderungen

Die rechtlichen Rahmenbedingungen stellen in unterschiedlichen Kontexten und unter Erfüllung unterschiedlicher Zwecke drei Grundqualitäten in den Mittelpunkt aller Betrachtungen:

- die Vertraulichkeit von Information,
- die Integrität von Information,

- die Verfügbarkeit von Information.

Angriffe auf eine dieser Grundqualitäten von Information werden entsprechend dem Schweregrad der Folgen zum Straftatbestand erhoben. Es besteht also grundsätzlich die Anforderung, durch geeignete Maßnahmen mögliche Bedrohungen dieser Grundqualitäten abzuwenden bzw. das Risiko des Eintretens zu minimieren.

In den folgenden Abschnitten werden in enger Anlehnung an /IABG97/ verschiedene Szenarien einer Nutzung von Internetdiensten durch Verwaltungen und Kliniken sowie Szenarien für Dienstangebote der Verwaltungen und Kliniken für ihre Kunden mit ihren kennzeichnenden Eigenschaften und typischen Bedrohungen bezüglich Vertraulichkeit, Integrität und Verfügbarkeit vorgestellt.

Sicherheit ist nicht absolut und in jeder noch so teuren Sicherheitslösung verbleibt ein Restrisiko. Bei der Güterabwägung von Investitionen in Sicherheitsinfrastruktur versus Sensibilität der zu schützenden Daten ist es daher erforderlich, eine Klassifikation der zu schützenden Dateninhalte nach dem Schweregrad der Folgen einer Verletzung der genannten Grundqualitäten für den Empfänger, Eigentümer oder Betroffenen vorzunehmen. Der in /DFN96/ gegebenen Klassifikation folgend, unterscheiden wir fünf **Schutzstufen:**

(A) Frei zugängliche Daten; Beispiel: Adressbücher.

(B) Personenbezogene Daten, deren Missbrauch keine besondere Beeinträchtigung des Betroffenen erwarten lässt; Beispiel: beschränkt-öffentliche Ausschreibung.

(C) Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann; Beispiel: Einkommen, Sozialleistungen, Ordnungswidrigkeiten.

(D) Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen *erheblich* beeinträchtigen kann; Beispiel: Unterbringung in Anstalten, Straffälligkeit, Schulden, Pfändungen.

(E) Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann; Beispiel: Sensible Patientendaten; Daten über Personen, die Opfer einer Straftat sein könnten.

Während bei dieser Einteilung die Wahrung der Vertraulichkeit, also der Datenschutz das Kriterium ist, zielt die folgende Einteilung in **Sicherheitsstufen** auf die Gefahren des Verlusts von Integrität und Verfügbarkeit von Informationen:

(A) Daten, deren Modifikation, Verlust oder Missbrauch keine besondere Beeinträchtigung erwarten lässt, d.h. der Verlust ist mit geringem Aufwand ausgleichbar.

(B) Daten, deren Modifikation, Verlust oder Missbrauch die betriebliche Handlungsfähigkeit beeinträchtigt, d.h. der Verlust ist mit vertretbarem Zeit- und Mitteleinsatz ausgleichbar.

(C) Daten, deren Modifikation, Verlust oder Missbrauch die betriebliche Handlungsfähigkeit *erheblich* beeinträchtigt, d.h. zur Schadensabklärung und -beseitigung sind erheblicher Zeit- und Mitteleinsatz erforderlich.

(D) Daten, deren Modifikation, Verlust oder Missbrauch die Hochschule oder die Klinik als solche beeinträchtigt, d.h. Schadensabklärung und -beseitigung sind sehr umfangreich und nicht kalkulierbar.

(E) Daten, deren Modifikation, Verlust oder Missbrauch die Hochschule oder die Klinik als solche in ihrer Existenz gefährdet, d.h. bleibender Schaden ist zu erwarten bzw. eine Schadensbeseitigung ist nicht garantierbar.

2.3 Nutzung von Basisdiensten des Internet durch Verwaltung und Klinik

Ein großer Teil der Kommunikation im Bereich von Verwaltungen und Kliniken wird bereits heute durch Dienste im Hochschulnetz abgewickelt, die nicht aufgabenspezifisch sondern vielmehr als Basisdienste universell einsetzbar sind. Die wichtigsten dieser Dienste sind Electronic Mail (E-Mail), WorldWideWeb (WWW), File Transfer Protocol (FTP) und Dialoganwendungen. Wir bezeichnen diese Dienste als **I-Basisdienste,** weil sie vom Inneren des geschützten Netzes aus genutzt werden und weil es universelle Internetdienste sind.

2.3.1 Nutzung von Electronic Mail

E-Mail gehört zu den am meisten genutzten Diensten des Internet. Bei der Benutzung von E-Mail aus einem Verwaltungs- oder Kliniknetz heraus, d.h. beim Versenden und Empfangen von Nachrichten nach bzw. von außen, gibt es eine Reihe von Bedrohungen:

(1) Angriff auf die Mailserver (SMTP) durch Überfluten der Server mit E-Mails oder durch Angriffe auf die privilegiert ablaufenden Mailprogramme (Beispiel: die Programmierfehler in *sendmail*).

(2) Einschleusen von Viren und damit Gefahr des Integritätsverlusts auf dem Client über Dokumente oder Programme, die als E-Mails empfangen werden (Beispiel: Makroviren); dabei sind auch andere, mit dem Client intern vernetzte Rechner des inneren Netzes gefährdet.

(3) Die übertragenen Nutzdaten sind in ihrer Vertraulichkeit und Integrität vielfältig bedroht: vertrauliche Inhalte können ausgespäht und verfälscht werden; sie können so manipuliert werden, dass das Schicken bzw. das Empfangen einer Nachricht nicht nachgewiesen werden kann.

(4) Die übertragenen Protokolldaten sind ebenfalls in ihrer Integrität gefährdet, denn es ist möglich, durch Manipulation des E-Mail-Headers eine Absenderangabe zu fälschen.

Die Daten, die über E-Mail kommuniziert werden, können prinzipiell allen Schutz- und Sicherheitsstufen angehören.

2.3.2 Nutzung von WWW

Das WorldWideWeb (WWW) hat sich zum wichtigsten Informationsmedium im Internet entwickelt und wird auch in Verwaltungen und Kliniken bereits heute intensiv genutzt. Die WWW-Dienste bergen viele Risiken:

(1) Durch übertragene Protokoll- und Nutzdaten sind Integrität und Vertraulichkeit des WWW-Clients im inneren Netz (ähnlich wie bei E-Mail) bedroht. Durch Einbruch über den WWW-Client werden auch andere, mit ihm vernetzte Rechner des Verwaltungs- oder Kliniknetzes bedroht.

(2) Die Vertraulichkeit von übertragenen sensitiven Nutzdaten, z.B. Kreditkartennummern für Bestellvorgänge, ist gefährdet.

(3) Übertragene Nutzdaten können Viren, Trojanische Pferde usw. enthalten und damit die Integrität von Daten im Intranet gefährden.

(4) Das HTTP-Protokoll erlaubt das Anstoßen von Aktionen auf dem WWW-Client, etwa das Starten von Viewern für bestimmt Dateitypen sowie von Java-Applets, JavaScript und ActiveX und damit Angriffe auf die Integrität des Clients.

Wie bei E-Mail können auch bei WWW die kommunizierten Daten prinzipiell allen Schutz- und Sicherheitsstufen angehören.

2.3.3 Nutzung von FTP

Die Industrie geht zunehmend dazu über, ihren Kunden Software und deren Updates mittels Dateitransfer über FTP anzubieten. Mittlerweile ist dies in vielen Bereichen der bequemste und mitunter sogar der einzige Weg, aktuelle Versionen zu erhalten. Ein wichtiges Beispiel sind Gerätetreiber. Eine andere für den wissenschaftlichen Betrieb an den Universitäten und Fachhochschulen bedeutsame Anwendung von FTP ist die elektronische Einreichung von Tagungs- und Kongressbeiträgen. Immer mehr Veranstalter gehen wegen ihrer zahlreichen Vorteile (z.B. die schnelle Übermittlung der Dokumente sowie ihre einfache elektronische Weiterverarbeitung, etwa für Abstract- oder Tagungsband) zu dieser Form über. Die Bedrohungen gestalten sich völlig analog zu denen bei der Nachrichtenübermittlung via E-Mail. Die einzige Ausnahme bilden die Protokolldaten. Beim FTP gibt es hier keine Bedrohung für den FTP-Client und das Intranet.

Meist gehören die per FTP kommunizierten Daten einer niedrigen Schutzstufe (z.B. Software) aber einer hohen Sicherheitsstufe (verfälschte oder verseuchte Software kann schlimme Folgen für das Unternehmen haben) an.

2.3.4 Nutzung von Dialoganwendungen

Bei Dialoganwendungen, in denen der Arbeitsplatz in der Verwaltung oder Klinik als Terminal einer im Internet laufenden Anwendung bzw. eines entfernten Rechners fungiert (Terminalemulation), ergibt sich folgendes Bedrohungsszenario:

(1) Für den Dialog-Client selbst besteht keine unmittelbare Bedrohung.

(2) Dagegen sind die übertragenen Nutzdaten, z.B. Passwörter oder die Daten aus einer Patientenaufnahmemaske, in ihrer Vertraulichkeit gefährdet.

(3) Durch die Übertragung von sogenannten Steuerzeichen vom Dialog-Server an den Dialog-Client ist dessen Integrität bedroht, da solche Zeichen unerwünschte Aktionen, z.B. die Umschaltung von Zeichensätzen, anstoßen können.

2.4 Anbieten von Diensten der Verwaltung oder Klinik für Kunden im Internet

Die Verwaltungen und Kliniken bieten ihren Kunden, den Mitarbeitern und Studenten der Hochschule, den Patienten und Bürgern, eine Reihe von Dienstleistungen an. Viele dieser Dienstleistungen bestehen in der Vermittlung oder dem wechselseitigen Austausch von Informationen, eignen sich also prinzipiell dafür, über Datennetze abgewickelt zu werden. Ein Vorteil für beide Seiten ergibt sich, wenn dadurch die Verfügbarkeit der Dienstleistung erhöht, Zeit eingespart oder ihre Qualiltät verbessert werden kann.

Die technische Umsetzung der Dienste kann im einfachen Fall durch Internet-Basisdienste wie z.B. E-Mail oder WWW erfolgen. Wir bezeichnen sie in dieser Funktion als **E-Basisdienste,** weil sie von Externen, also von Kunden der Verwaltung oder Klinik, genutzt werden, um deren spezifische Dienste in Anspruch zu nehmen. Im aufwendigen Fall werden die Dienste über dedizierte Anwendungen im Dialogbetrieb angeboten. Im dabei heute gängigen Szenario einer Client/Server-Architektur ist der WWW-Browser auf dem Kunden-Client kein E-Basisdienst im Sinne obiger Definition.

2.4.1 Allgemeine Informationsdienste

Unter allgemeinen Informationsdiensten versteht man die Bereitstellung von Informationen, die eine Hochschulverwaltung oder Universitätsklinik frei publiziert, um potentielle Kunden auf ihre Angebote und die Voraussetzungen ihrer Nutzung zu informieren. Es handelt sich dabei typischerweise um Daten der Schutzstufe A und der Sicherheitsstufe B. Eine Hochschulverwaltung informiert so etwa über die angebotenen Studiengänge, über den Lehrkörper der Hochschule, über Immatrikulationstermine, Vortragsveranstaltungen und vieles mehr. Universitätskliniken informieren über ihre Fachabteilungen, stellen medizinische Neuerungen vor, berichten über Erfahrungen oder bieten Patienteninformation zu bestimmten diagnostischen Verfahren und Therapien an.

In Bezug auf Sicherheit gibt es hier keinen Unterschied zwischen Verwaltungen und Kliniken. In beiden Bereichen ist die angebotene Information ausschließlich öffentliche Information, die, soweit sie personenbezogen ist, nur Angaben enthält, zu deren Bekanntmachung die betreffende Person ausdrücklich ihre Zustimmung gegeben hat. Kennzeichnend für das

Szenario der allgemeinen Informationsdienste ist also, dass *keine Vertraulichkeit erforderlich* ist. Vielmehr widerspricht sie dem Charakter der angebotenen Information. Diese soll ja gerade jedem frei zugänglich gemacht werden.

Das zweite Kennzeichen dieser Informationsdienste ist die Tatsache, dass *keine Identifizierung und Authentifizierung der Kunden* notwendig ist. Aus Datenschutzgründen ist sie auch gar nicht erwünscht.

Welche Bedrohungen ergeben sich aus der Bereitstellung allgemeiner Informationsdienste?

(1) Der Informationsserver der Verwaltung oder Klinik, i. Allg. ein HTTP-Server, ist in seiner Verfügbarkeit bzw. Integrität bedroht durch mögliche Penetration, durch Veränderung der Informationsinhalte auf den WWW-Seiten oder durch Verfügbarkeitsattacken.

(2) Da die Kunden-Clients überwiegend unsichere PC-Endgeräte sind, dürfen sich die übrigen Komponenten nicht auf die Integrität von Programmen oder Daten sowie auf die Wahrung der Vertraulichkeit von Informationen auf diesen Rechnern verlassen. Daher dürfen z.B. keine Passwörter auf den Kunden-Clients abgelegt werden.

(3) Andere mit dem Informationsserver vernetzte Rechner im Verwaltungs- oder Kliniknetz sind prinzipiell bedroht durch den Anschluss an ein öffentliches unsicheres Netz, des weiteren durch die Folgen einer Penetration des Informationsservers.

(4) Die angebotenen Nutzdaten sind von Manipulationen durch Dritte bedroht, die einen Imageverlust für den Anbieter zur Folge haben können.

(5) Hinsichtlich der übertragenen Protokolldaten besteht keine Bedrohung.

2.4.2 Auskunftsdienste

Im Unterschied zu allgemeinen Informationsdiensten, die einen einseitigen Informationsfluss vom Anbieter zum anonymen Kunden ermöglichen, stellen Auskunftsdienste eine prinzipiell vertrauliche Beratungssituation zwischen Verwaltung oder Klinik und dem anonymen Kunden her. Beispiele für Auskunftsdienste sind Vorabberechnung der zu erwartenden Rentenbezüge oder Diabetikerberatung. Auskünfte müssen im Spezialfall sogar juristisch belastbar sein (Beispiel: Elektronisches Handelsregister). Die Daten gehören in der Regel je nach Auskunftsart den Schutz- und Sicherheitsstufen B oder C an.

Kennzeichnende Merkmale von Auskunftsdiensten sind: Die *Vertraulichkeit der ausgetauschten Daten* muss gewährleistet werden. Man benötigt *keine Identifikation und Authentifizierung* des Kunden. Hingegen kann die *Authentifizierung des Dienstservers* gegenüber dem Kunden notwendig sein (juristisch belastbare, verbindliche Auskünfte).

Entsprechend den höheren Anforderungen kommen zusätzlich zu den bei allgemeinen Informationsdiensten bestehenden noch folgende neue Bedrohungen hinzu. Zu (1): Vorspiegelung des Dienstes durch Angriff auf den Dienstserver. Zu (4): Die übertragenen Nutzdaten sind in ihrer Vertraulichkeit und Integrität bedroht durch Abhören, durch Attacken, bei denen sich ein Angreifer zwischen die Kommunikationspartner schiebt, oder

durch Penetration des Dienstservers, der dann fehlerhafte Auskünfte erteilt. Zu (5): Die übertragenen Protokolldaten sind in ihrer Vertraulichkeit bedroht, indem ein unberechtigter Dritter die Authentizität des Dienstservers gegenüber dem Kunden vortäuscht. Ferner können Protokolldaten zum Aufbau eines virtuellen privaten Kanals abgehört werden.

2.4.3 Selbstbedienung für Verwaltungs- und Klinikkunden

Dieses Szenario deckt personenspezifische Dienste ab, bei denen jedoch keine vertraulichen Informationen bereitgestellt werden und auch keine Unterschriften geleistet werden müssen. Beispiele für Selbstbedienungsdienste sind etwa die Rückmeldung von Studenten für das nächste Semester oder die Anmeldung zu einem Seminar. Typische Schutz- und Sicherheitsstufen für Daten dieses Szenarios sind A bis C.

Kennzeichen von Selbstbedienungsdiensten sind also: Keine vertrauliche Information; keine Identifikation und Authentifizierung des Kunden notwendig; Authentifizierung des Dienstservers gegenüber dem Kunden kann erforderlich sein; keine Verbindlichkeit und Nachweisbarkeit der Transaktion erforderlich.

Die Bedrohungen umfassen diejenigen der allgemeinen Informationsdienste und zusätzlich, da es sich um personenspezifische Dienste handelt, die eine Authentifizierung des Dienstservers erforderlich machen, die folgenden. Zu (4): Die übertragenen Nutzdaten sind in ihrer Integrität bedroht durch Attacken, bei denen sich der Angreifer zwischen die Kommunikationspartner schiebt, ferner durch Penetration des Dienstservers, der dann fehlerhaft arbeitet und eine erfolgreiche Transaktion meldet, die in Wirklichkeit fehlgeschlagen ist (Beispiel: Exmatrikulation trotz erfolgter Rückmeldung). Zu (5): Die übertragenen Protokolldaten sind in ihrer Vertraulichkeit und Integrität bedroht durch Abhören und Vortäuschung des Dienstservers gegenüber dem Kunden durch einen Dritten.

2.4.4 Auskunftsdienste zur eigenen Person

Dieses Szenario kombiniert Auskunftsdienst und Selbstbedienung, um dem Kunden Informationen zu seiner Person zugänglich zu machen. Die Daten können vertraulich und sehr sensitiv sein. Entsprechend gehören sie den Schutzstufen B (z.B. Adressen) bis E (z.B. besonders sensible medizinische Diagnosen) an. Auskunftsdienste zur eigenen Person spielen im Zusammenhang mit der informationellen Selbstbestimmung der Bürger eine besondere Rolle. Sie muss gewährleisten, dass der Bürger jederzeit vollständige Auskunft über alle zu seiner Person gespeicherten Daten erhalten kann.

Auskunftsdienste dieser Art sind wie folgt gekennzeichnet: Vertrauliche, personenspezifische Informationen müssen geschützt werden; Identifikation und Authentifizierung des Kunden sind erforderlich; Authentifizierung des Dienstservers gegenüber dem Kunden kann notwendig sein; die Verbindlichkeit und Nachweisbarkeit der Transaktion sind nicht notwendig.

Die Bedrohungen für Dienstserver, Dienstclient, andere mit dem Dienstserver vernetzte Rechnersysteme, übertragene Nutz- und Protokolldaten entsprechen den zusammengefassten Bedrohungen bei Auskunftsdiensten und Selbstbedienung.

2.4.5 Dienste mit rechtsverbindlichen Transaktionen

Kennzeichen der Dienste, die rechtsverbindliche Transaktionen einschließen, ist es, dass sich einer oder beide Partner rechtlich verpflichten. In welchen Fällen dabei eine Unterschrift geleistet werden muss, ist zwar gesetzlich nicht geregelt, im Allgemeinen wird aber meist dann eine Unterschrift verlangt, wenn die Transaktion weiterreichende rechtliche Konsequenzen hat, etwa bei Beglaubigungen oder Verträgen. Die Daten gehören je nach ihrem Inhalt den Schutz- und Sicherheitsstufen B bis E an, wobei Schutzstufe und Sicherheitsstufe im Einzelfall sehr unterschiedlich sein können. Beispiele für Dienste dieser Art sind die elektronische Einkommenssteuererklärung (Schutzstufe B, Sicherheitsstufe D), die elektronische Diplomarbeit (Schutzstufe A, Sicherheitsstufe D), die Abgabe einer eidesstattlichen Versicherung (Schutz- und Sicherheitsstufen D oder E), elektronische Übertragung von Patientendaten zwischen Klinik und Hausarzt (Schutz- und Sicherheitsstufen D oder E).

Folgende Merkmale kennzeichnen das Szenario: Schutz der Vertraulichkeit der Daten ist erforderlich; ebenso die Identifikation und Authentifizierung des Kunden; des weiteren ist hier auch die Authentifizierung des Dienstservers gegenüber dem Kunden zwingend notwendig; schließlich bedarf es der Absicherung der Verbindlichkeit und Nachweisbarkeit der Transaktion.

Zunächst bestehen dieselben Bedrohungen wie für Auskunftsdienste zur eigenen Person. Zusätzlich sind die übertragenen Nutzdaten durch Fälschung der elektronischen Unterschrift des Kunden bedroht.

2.4.6 Dienste mit finanziellen Transaktionen

Zu den Diensten, bei denen es zu finanziellen Transaktionen kommt, also auf elektronischem Wege gezahlt wird, gehören zum Beispiel Zahlungen an das Studentenwerk, elektronische Einbezahlung von Gebühren, etwa für das Ausstellen amtlicher Dokumente oder das Begleichen einer Klinikrechnung. Finanzielle Transaktionen erscheinen bei Verwaltungen und Kliniken in der Regel als Zusatz zu anderen Szenarien.

Kennzeichen sind: Identifikation und Authentifizierung des Kunden sowie Authentifizierung des Dienstservers gegenüber dem Kunden sind erforderlich; die Integrität der Daten, die das „elektronische Geld“ repräsentieren, muss sichergestellt sein.

Die Bedrohungen sind im Wesentlichen deckungsgleich mit denen rechtsverbindlicher Transaktionen. Spezifische Bedrohungen sind die Fälschung von Geldbeträgen oder die Umleitung von Geldflüssen durch Änderung des Adressaten durch einen Angriff auf die Nutzdaten. Ebenso könnten die Protokolldaten zum Geldaustausch verfälscht werden.

2.5 Datenübertragung zwischen abgesicherten Netzen über das unsichere öffentliche Netz

Der sehr häufige Fall von Verwaltungen oder Kliniken mit verteilten Standorten, deren lokale Netze über ein offenes ungesichertes Netz hinweg zu einem Gesamtnetz („Corporate Network“) verbunden werden sollen, wird durch dieses Szenario beschrieben. Ein Spezialfall ist der Telearbeitsplatz, bei dem sich ein Mitarbeiter von außen, etwa von zu Hause, mit dem Verwaltungs- oder Kliniknetz verbindet, um mit Anwendungen zu arbeiten, die zur Erfüllung seiner dienstlichen Aufgaben notwendig sind. Hier besteht des Mitarbeiter-„Netz“ aus nur einem Rechner, es gelten aber dieselben Bedrohungen wie bei Verbindung echter lokaler Netze.

Die Kennzeichen des Szenarios sind: Vertraulichkeit der übertragenen Daten ist zu gewährleisten; Vorkehrungen zum Schutz der Integrität der übertragenen Daten sind zu treffen; die Kommunikationspartner müssen sich gegenseitig identifizieren und authentifizieren.

Es bestehen folgende Bedrohungen: Die Rechnersysteme innerhalb der sicheren Netze sind bedroht durch den Anschluss an das unsichere Netz an sich, sowie durch Penetration des Kommunikationsendpunkts; die übertragenen Nutzdaten sind in ihrer Integrität und Vertraulichkeit bedroht durch Abhören (bei Übertragung über öffentliches Netz immer möglich), durch Attacken, bei denen sich ein Dritter zwischen die Kommunikationspartner schiebt („man in the middle“), durch Penetration der Kommunikationsendpunkte. Die übertragenen Protokolldaten sind bedroht durch Abhören der Identifikation und Authentifizierung, durch Fälschung der Identifikations- und Authentifizierungsdaten, durch Abhören der Daten zum Aufbau eines virtuellen Kanals (z.B. Schlüssel, session key).

2.6 Literatur

/BSTUKWK97/ Bayer. Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst:
„Hochschulnetze in Bayern — Zugang, Nutzung, Schutz vor Missbrauch und damit zusammenhängende Rechtsfragen, Bericht der Arbeitsgruppe Zugangs- und Nutzungsregelungen für die bayerischen Hochschulnetze“
München, Februar 1997

/IABG97/ IABG:
„Sicherheitsvalidierung BASILIKA. Generisches Sicherheitskonzept.“
IABG, November 1997

/DFN96/ Deutsches Forschungsnetz – DFN –:
„Koexistenz von Verwaltung und Wissenschaft in hochschulweiten Backbone-Netzen unter besonderer Berücksichtigung des Datenschutzes und der Verfahrens- und Datensicherheit.“
DFN-Bericht Nr. 80, Januar 1996

Kapitel 3

Situation der Netze und Netzanwendungen im Verwaltungs- und Klinikbereich

Um den Bedarf für Empfehlungen zur sicheren Anbindung von Verwaltungs- und Kliniknetzen an die allgemeinen Hochschulnetze festzustellen, wurden Umfragen an den bayerischen Universitäten (zur Netzinfrastruktur im Mai 1996 und zu Netzdiensten und Anwendungen im Dezember 1996) und Fachhochschulen (Oktober 1996) durchgeführt. Die Bestandsaufnahme diente auch der Bestimmung der Schwerpunkte des Berichts sowie des Detaillierungsgrades der Ausführungen zu bestimmten Themen.

Von den 16 universitären Organisationseinheiten (Verwaltungen und Kliniken) beteiligten sich an der Befragung zur Netzinfrastruktur 13 (81%), an der Umfrage zu Diensten und Anwendungen 11 (69%). Von den 15 Fachhochschulen beteiligten sich 12 (80%) an der Befragung. Die Ergebnisse liefern damit ein zuverlässiges Bild der Lage.

Alle Verwaltungen und Kliniken sind vernetzt oder werden in naher Zukunft vernetzt. Die Mehrzahl der Kliniken und Hochschulverwaltungen verfügt zudem heute schon über eine Anbindung an das Hochschulnetz. Über die Hälfte der Befragungsteilnehmer nutzt Electronic Mail (E-Mail), WorldWideWeb (WWW), Telnet und File Transfer Protocol (FTP) zur Abwicklung ihrer Routineaufgaben. Bibliotheksdienste, Fachinformationsdatenbanken und Studentenverwaltung gehören neben Standardbürosoftware zu den meistgenutzten Anwendungen.

Auf die im Rahmen der Netzinfrastrukturerhebung gestellte Frage nach den Erwartungen der Hochschulen an den Bericht der Kommission ergab sich der Wunsch nach konkreten Empfehlungen zum Sicherheitskonzept und zu technischen Sicherheitstools sowie nach Lösungsvorschlägen zu den Sicherheitsproblemen geöffneter Verwaltungs- und Kliniknetze, und zwar differenziert nach Gefährdungsklassen, unter Berücksichtigung der anfallenden Kosten und der rechtlichen Vorschriften (vgl. 3.1.1).

3.1 Universitäten

Es wurden zwei getrennte Umfragen an die Universitäten verschickt. Die erste Umfrage betraf den Stand der Netzinfrastruktur. Ferner wurden die Erwartungen an den von der Kommission zu erarbeitenden Bericht und seine Empfehlungen erfragt.

Die zweite Umfrage erhob die Situation in Bezug auf Netzdienste und Verwaltungs- und Klinikanwendungen, die öffentliche Netze benutzen. Außerdem wurde der Bedarf am Einsatz weiterer Dienste und Anwendungen erhoben.

Es wurden bei beiden Umfragen alle Universitätsverwaltungen und -kliniken in Bayern, das sind 16 Organisationseinheiten, über die Kanzler der Universitäten angeschrieben. Auf die erste Umfrage antworteten 13, auf die zweite 11 Adressaten. Dies entspricht Rücklaufquoten von 81% bzw. 69%.

Die Umfrageergebnisse zeigten einen starken Bedarf an Empfehlungen zum Thema der sicheren Anbindung an öffentliche Netze auf. Die Mehrzahl der antwortenden Einrichtungen verfügen bereits über eine Anbindung an öffentliche Netze und nutzen auch schon Basisdienste, vor allem (über die Hälfte der Teilnehmer an der Befragung) E-Mail, WWW, Telnet und FTP zur Abwicklung ihrer Routineaufgaben.

3.1.1 Netze und Netzstrukturen

Teilnehmer und Rücklauf

An der 1. Umfrage beteiligten sich 82% der bayerischen Universitätsverwaltungen und 80% der Kliniken (Tabelle 3.1).

Art der Einrichtung	Angefragt	Rücklauf	in %
Verwaltungen	11	9	82%
Kliniken	5	4	80%
gesamt	16	13	81%

Tabelle 3.1: Rücklauf der 1. Befragung

Umfrageergebnisse zur Vernetzung

Die bayerischen Universitäten wurden, getrennt für Verwaltungen und Kliniken, nach dem Stand der Vernetzung befragt. Dabei wurde unterschieden zwischen Ist- und Planzustand und dem Grad der Netzöffnung (Lokales Netz, Vernetzung mit dem Hochschulnetz, Vernetzung mit dem Internet). Die Hochschulen wurden im Einzelnen zu folgenden Themen befragt:

- Stand der Vernetzung
- mögliche Vernetzungshindernisse
- aus der Vernetzung resultierende Sicherheitsprobleme
- Bestehen einer Sicherheitspolitik
- Konfigurationsskizze zur Netztopologie
- Wünsche an die Arbeitsgruppe
- optional: Weitere Unterlagen zur Vernetzung
- besondere Vernetzungsprobleme

Die Ergebnisse (mit Stand Mai 1996) werden im Folgenden dargestellt und kommentiert.

Stand der Vernetzung

Alle Verwaltungen und Kliniken der Universitäten sind vernetzt oder werden in Zukunft vernetzt. Die Mehrzahl der Einrichtungen besitzt Netze mit Kopplung an das Hochschul- und Wissenschaftsnetz. Zusätzlich existieren lokale Netze ohne Kopplung bzw. Netze mit minimaler Kopplung, d.h. es sind nur ausgewählte Netzdienste freigegeben (z.B. E-Mail). Keine Hochschule verzichtet generell wegen Sicherheitsproblemen auf eine Vernetzung.

In der Tabelle 3.2 sind die Ergebnisse dargestellt. Die %-Angaben beziehen sich auf den gesamten Rücklauf von 16 Organisationseinheiten zu 100%. Dadurch, dass u.U. parallele Netze bei einigen Organisationseinheiten bestehen, ergeben sich bei der bestehenden Vernetzung Mehrfachangaben für einzelne Institutionen und damit Prozentangaben > 100.

Art der Vernetzung	bestehende Vernetzung		geplante Vernetzung	
lokales Netz	3	19%	2	13%
Netz verbunden mit Universitätsnetz	8	50%	3	19%
Netz verbunden mit Wissenschaftsnetz / Internet	10	63%	5	31%
gesamt	21	131%	10	63%

Tabelle 3.2: Verwaltungs- und Kliniknetze, Stand und Planung

Die Verwaltungen und Kliniken wurden befragt, ob in Zukunft wegen Sicherheitsproblemen generell auf eine Vernetzung bzw. Öffnung der Netze verzichtet werde. Diese Frage wurde von allen Einrichtungen verneint.

Mögliche Vernetzungshindernisse

Die Verwaltungen und Kliniken wurden nach möglichen Vernetzungshindernissen befragt. Im Gegensatz zur Feststellung, dass auf eine Vernetzung nicht verzichtet werde, nannten hier 3 Einrichtungen (19%) Vernetzungshindernisse. Möglicherweise wurde hier nicht unterschieden zwischen lokaler Vernetzung und Öffnung lokaler Netze.

Aus der Vernetzung resultierende Sicherheitsprobleme

Die Verwaltungen und Kliniken der Universitäten wurden befragt, welche Sicherheitsprobleme sie als Resultat der Vernetzung sehen aber für tolerierbar halten, und welche Sicherheitsmaßnahmen ergriffen wurden oder geplant sind.

Die Universitäten nennen unterschiedliche Gefährdungsbereiche in den vorgeschlagenen Kategorien Arbeitsplatz, Datenübertragung, Zentrale Rechner und Sonstiges. Es zeigt sich, dass ein jeweils partielles Wissen über Sicherheitsrisiken und mögliche Maßnahmen besteht. Nach Anzahl der Nennungen lassen sich die in Tabelle 3.3 dargestellten Schwerpunkte erkennen.

DV-Bereich	Probleme
Arbeitsplatzrechner / Clients	Authentifizierung des Benutzers, Datenschutz bei lokaler Datenhaltung
Datenübertragung im Netz	Datenverschlüsselung
Zentrale Rechner / Server	Zugangskontrolle
Sonstiges / Netzkopplung	Kopplung lokaler Netze mit öffentlichen Netzen

Tabelle 3.3: Sicherheitsprobleme

Bestehen einer Sicherheitspolitik

Mit dieser Frage wurde festgestellt, ob an den Universitäten der Schutzbedarf analysiert und Sicherheitsmaßnahmen festgelegt wurden, ob also ein sogenanntes Sicherheitskonzept erarbeitet wurde. Das Ergebnis ist in Tabelle 3.4 zusammengestellt.

Zum Teil bestehen Sicherheitskonzepte, Ansätze dazu oder werden erarbeitet. Bei den übrigen Universitäten gibt es noch keine explizite, umfassende Sicherheitspolitik. Einzelne Maßnahmen werden jedoch durchgeführt, z.B. Schutz der Datenbankserver durch einen Firewall-Rechner.

Sicherheitskonzept	Anzahl	Anteil
besteht	1	6%
besteht in Ansätzen	1	6%
wird erarbeitet	4	25%
gibt es nicht	10	63%
gesamt	16	100%

Tabelle 3.4: Sicherheitskonzepte

Wünsche an die Arbeitsgruppe

Die Universitäten wurden befragt, welche Wünsche sie an die Arbeitsgruppe haben. Soweit aus den kurzgehaltenen Antworten und Stichworten gefolgert werden kann, lassen sich die Wünsche so zusammenfassen:

Die Universitäten wünschen Lösungsvorschläge zu den Sicherheitsproblemen geöffneter Verwaltungs- und Kliniknetze

- differenziert nach Gefährdungsklassen
- unter Berücksichtigung der anfallenden Kosten und
- der rechtlichen Vorschriften.

Besondere Vernetzungsprobleme

Die Antworten zur Frage nach speziellen Problemen zeigen eine Besonderheit vor allem der „alten“ Universitäten, die sich aus der geographischen Struktur der Hochschulen ergibt, nämlich verteilte Verwaltungen und Kliniken. Beispiele sind die Verwaltung der Universität Erlangen-Nürnberg mit den Standorten Erlangen und Nürnberg und die Verwaltung der TU München mit den Standorten München und Weihenstephan. Eine Beschränkung auf lokale Netze ist hier aus strukturellen und Kostengründen nicht möglich. Die Datenübertragung zwischen den verteilten Verwaltungsdienststellen erfolgt z.T. über öffentliche Netze mit den damit verbundenen Sicherheitsrisiken.

3.1.2 Nutzung und Planung von Basisdiensten und Anwendungen

Rücklauf

An der 2. Umfrage beteiligten sich 73% der bayerischen Universitätsverwaltungen und 60% der Universitätskliniken (Tabelle 3.5).

Art der Einrichtung	Angefragt	Rücklauf
Verwaltungen	11	8 (73%)
Kliniken	5	3 (60%)
gesamt	16	11 (69%)

Tabelle 3.5: Rücklauf der 2. Befragung

Umfrageergebnis Basisdienste

Bei den Basisdiensten E-Mail, WWW, Telnet, Domain Name Service (DNS), Network News Transport Protocol (NNTP), Zeitdienst (time), Network File System (NFS), Remote Procedure Call (RPC), Remote Login (rlogin), Remote Shell (rsh), Novell Directory Services (NDS), usw. wurde unterschieden, ob sie aus der Verwaltung oder der Klinik heraus durch Mitarbeiter der Organisationseinheit genutzt werden (sog. I-Dienste) oder ob sie von Externen benutzt werden, um mit der Organisationseinheit zu kommunizieren (sog. E-Dienste). Diese Unterscheidung wurde bereits im Kapitel 2 bei der Definition der Anforderungen verwendet. Sie dient des Weiteren der klaren Begriffsbildung: Nicht der Dienst allein ist entscheidend, sondern die Richtung des Hauptinformationsflusses.

I-Dienst	heute im Einsatz		geplant	gewünscht, aber nicht geplant
	Anzahl	Anteil	Anzahl	Anzahl / Grund
E-Mail	9	82%	—	—
WWW	9	82%	—	—
Telnet	8	73%	1	—
Filetransfer	6	55%	1	—
Client/Server	3	27%	1	—
DNS	3	27%	—	—
NNTP	2	18%	—	—
time	2	18%	—	—
NFS	2	18%	—	1 / Personalmangel

Tabelle 3.6: Umfrageergebnis Basisdienste intern nach extern (I-Basisdienste)

Es wurde ein Ranking der heute eingesetzten Basisdienste vorgenommen. Die Ergebnisse sind in Tabelle 3.6 (I-Dienste) und Tabelle 3.7 (E-Dienste) zusammengestellt. Spitzenreiter sind erwartungsgemäß E-Mail und WWW. E-Mail wird sowohl als I-Dienst wie als E-Dienst bei 82% der Antwortenden genutzt. Der E-Mail-Verkehr gestaltet sich also ausgewogen von intern nach extern und vice versa. WWW dagegen wird bei fast doppelt so vielen Einrichtungen (82%) als I-Dienst zur Informationsbeschaffung benutzt gegenüber einer nur 42%-igen Nutzung als E-Dienst zur Informationsbereitstellung von der Organisation für Externe. Noch deutlicher ist dieses Ungleichgewicht bei Telnet: 73% der Einrichtungen nutzen es als I-Dienst, um sich auf externen Servern einzuloggen, nur 27% gestatten das Einloggen Externer auf Servern ihrer Einrichtung. FTP nimmt mit 55% Nutzung als I-Dienst und 45% Nutzung als E-Dienst eine ausgewogene Zwischenposition ein. Client/Server-Kommunikation nimmt mit 27% Nutzung als I-Dienst und 9% Nutzung als E-Dienst jeweils Rang 5 ein. Die übrigen Basisdienste spielen keine nennenswerte Rolle, lassen aber deutlich einen Überhang der Nutzung als I-Dienste (18-27%) gegenüber der Nutzung als E-Dienste (0-9%) erkennen.

E-Dienst	heute im Einsatz		geplant	gewünscht, aber nicht geplant
	Anzahl	Anteil	Anzahl	Anzahl
E-Mail	9	82%	—	—
WWW	5	45%	2	—
Filetransfer	5	45%	1	—
Telnet	3	27%	1	—
Client/Server	1	9%	4	—
X-Window	1	9%	—	—
RPC	—	—	—	1
Remote Login	—	—	—	1
Remote Shell	—	—	—	1
NDS	—	—	1	—

Tabelle 3.7: Umfrageergebnis Basisdienste extern nach intern (E-Basisdienste)

Umfrageergebnis Verwaltungsanwendungen

Gefragt war der heutige und geplante Einsatz von Verwaltungsanwendungen unter Nutzung öffentlicher Netze. Es kristallisieren sich vier solche Anwendungen als Spitzenreiter heraus (Tabelle 3.8): Bibliotheksdienste (87%), externe Fachinformationsdatenbanken (75%), Telefonverzeichnis (62%) sowie Fax- und Voicemail (50%). Mit 2–3 Nennungen (25–37%) folgten die Anwendungen Studentenverwaltung, Standard-Bürosoftware, Haushalts- und Kassenverfahren, Prüfungsverwaltung und Zahlungswesen auf den Plätzen 5–9. Der Einsatz der genannten Anwendungen ist bei 1–3 jeweils anderen Verwaltungen immerhin in Planung. Eine Verwaltung gab mehrfach Personalmangel als Grund für den Nichteinsatz gewünschter Basisdienste und Anwendungen an.

Rang	Verwaltungsanwendung mit Nutzung öffentlicher Netze	heute im Einsatz		geplant	gewünscht, aber nicht geplant
		Anzahl	Anteil	Anzahl	Anzahl / Grund
1	Bibliotheksdienste	7	87%	1	—
2	Externe Fachinformationsdatenbanken	6	75%	3	—
3	Telefonverzeichnis	5	62%	3	—
4	Fax- & Voicemail	4	50%	2	—
5	Studentenverwaltung	3	37%	3	—
6	Standard-Bürosoftware	3	37%	—	1 / Personalmangel
7	Haushalts- und Kassenverfahren	2	25%	2	1
8	Prüfungsverwaltung	2	25%	3	—
9	Zahlungswesen	2	25%	1	—

Tabelle 3.8: Umfrageergebnis Verwaltungsanwendungen.
[Die Prozentangaben beziehen sich auf den Rücklauf von 8 Fragebögen (=100%)]

Umfrageergebnis Klinikanwendungen

Die Umfrage bei den Universitätskliniken steht mit 3 Antworten bei 5 Adressaten auf wenig solider Grundlage. Dennoch zeichnet sich ein plausibles Bild der Situation ab (Tabelle 3.9). Spitzenreiter der Klinikanwendungen, die öffentliche Netze verwenden, sind wie bei den Verwaltungen die Bibliotheksdienste. Sie wurden von allen (100%) Anwortenden angegeben. Mit jeweils 2 Nennungen (66%) folgen die externen Fachinformationsdatenbanken und die Standard-Bürosoftware. Die Anwendung Telefonverzeichnis wird derzeit einmal eingesetzt, ihr Einsatz ist an den beiden anderen Hochschulen geplant. Es folgen die Lehrveranstaltungsplanung und die Fernwartung via Telearbeitsplatz mit je einem Einsatz und einer Planung. Fax- und Voicemail ist an allen 3 Kliniken geplant, Kostenübernahmesicherung an zweien, Gebäude- und Raumverwaltung an einem. Ein Klinikum lässt Fernwartung durch eine externe Firma zu.

Rang	Klinikanwendung	heute im Einsatz		geplant	gewünscht, aber nicht geplant
		Anzahl	Anteil	Anzahl	Anzahl
1	Bibliotheksanwendungen	3	100%	—	—
2	Externe Fachinformationsdatenbanken	2	66%	—	—
3	Standard-Bürosoftware	2	66%	—	—
4	Telefonverzeichnis	1	33%	2	—
5	Lehrveranstaltungsplanung	1	33%	1	—
6	Fernwartung via Telearbeitsplatz	1	33%	1	—
7	Fernwartung über externe Firma	1	33%	—	—
8	Fax- & Voicemail	—	—	3	—
9	Kostenübernahmesicherung	—	—	2	—
10	Gebäude- & Raumverwaltung	—	—	1	—

Tabelle 3.9: Umfrageergebnis Klinikanwendungen.
[Die Prozentangaben beziehen sich auf den Rücklauf von 3 Fragebögen (=100%)]

Auswertung der Netstat-Informationen

Bei fast allen eingesandten Listen über die auf den Servern verfügbaren Kommunikationsdienste (Ports) ist erkennbar, dass das Dienstangebot der Server nicht geprüft und die angebotenen Dienste nicht auf das notwendige Minimum reduziert wurden. Neben Diensten, die vor allem zum Test von Servern zur Verfügung gestellt werden (*chargen*, *discard*, *echo*, sowie rpc-basiert *sprayd*), werden auch risikobehaftete Dienste vom Server angeboten. Bei den meisten Systemen wird der Dienst Trivial File Transfer Protocol (TFTP) angeboten, der meist für den Boot-Vorgang von „dummen“ Geräten im Netz verwendet wird. Der Zugriff auf die Dateien findet hierbei ohne Authentifizierung statt, einzige Voraussetzung ist die Kenntnis des Dateinamens bzw. des Pfades dorthin. In neueren Versionen wird als Standardkonfiguration das Root-Verzeichnis dieses Dienstes in einen separaten Bereich gelegt, damit kein unbefugter Zugriff (lesend wie schreibend) auf Systemdateien möglich ist.

Diverse Tools zur Prüfung der Netzsicherheit, u.a. SATAN, zeigen auf, welche der angebotenen Dienste risikobehaftet sind und ausgeschaltet bzw. sicher(er) konfiguriert werden

sollten. Andere Dienste, die von den meisten (angegebenen) Servern angeboten werden, werden in der Regel in einem UNIX-Verbund genutzt, um Informationen zwischen den Rechnern im Verbund auszutauschen. Zu diesen Informationsdiensten gehören u.a. *rquotad* (Auskünfte über die Belegung von Plattenplatz) und *rusersd* (Auskünfte über eingeloggte Benutzer). Es ist jeweils die Frage zu klären, inwieweit solche Dienste notwendig bzw. sinnvoll sind.

Die Konfiguration der Dienste, die über den Internet Superserver (*inetd*) bei Anforderung gestartet werden, befindet sich auf UNIX-Systemen i. Allg. in der Datei /etc/inetd.conf. Teilweise ist dem netstat-Ausdruck zu entnehmen, welche Dienste gerade aktiv genutzt werden (erkennbar am state: established). Auffallend ist die z.T. häufige Nutzung des telnet- bzw. rlogin-Zugangs zu den angegebenen Servern. Dies weist darauf hin, dass diese Server nicht in einem reinen Client/Server-Umfeld genutzt werden. Zwei Hochschulen geben an, dass die angebotenen Dienste nicht von extern zugreifbar sind. Bei dieser Sichtweise wird übersehen, dass diese Dienste jedoch weiterhin im geschützten Netz angeboten werden und somit die Gefahr eines Insiderangriffs besteht.

3.2 Fachhochschulen

Die vorliegende Bestandsaufnahme ist das Ergebnis einer Umfrage unter den bayerischen Fachhochschulen im Oktober 1996. Insgesamt haben 12 der 15 Fachhochschulen den Fragebogen beantwortet (80%). Die Ergebnisse liefern damit ein zuverlässiges Bild der Lage.

3.2.1 Netze und Netzstrukturen

Stand und künftiger Ausbau der Vernetzung

Etwa die Häfte der Verwaltungsnetze ist an das Hochschulnetz und das Internet angeschlossen, für den überwiegenden Rest ist dies für die Zukunft geplant. Prinzipielle Einwände gegen eine Verbindung mit externen Netzen haben drei Fachhochschulen.

Sicherheitsmaßnahmen

Es werden eine Reihe von Sicherheitsproblemen erkannt (technische und personenbezogene) und sinnvolle Lösungsvorschläge dafür gemacht. In zwei Fällen wird von Einzelmaßnahmen zur Verbesserung der Sicherheit berichtet, eine konsequente Sicherheitspolitik gibt es aber nirgendwo.

Beratungsbedarf

Zwei Drittel der Fachhochschulen haben Beratungsbedarf, vor allem in folgenden Bereichen:

- sichere Verbindung von Standorten, sowie von der Koordinierungsstelle an der FH Regensburg zu allen Fachhochschulen

- Maßnahmen gegen Angriffe „von außen“, z.B. bei der Einrichtung von Firewalls
- Verschlüsselungstechniken bei der Datenübertragung
- Einführung technischer Planstellen im Verwaltungsbereich

Lokale Besonderheiten

An vielen Fachhochschulen sind die Verwaltungen auf mehrere Standorte verteilt. Außerdem gibt es seit kurzem eine Koordinierungsstelle an der FH Regensburg, die technischen Support an allen Fachhochschulen leistet und dafür Zugang über das Netz zu diesen benötigt.

Sicherheitsmaßnahmen

Zwei Drittel der Fachhochschulen berichten von konkreten Aktivitäten oder Überlegungen zu technischen Sicherheitsmaßnahmen. Diese reichen von der physischen Isolierung des Verwaltungsnetzes, der Protokoll-Trennung durch Einschränkung des Zugangs zu Verwaltungsdaten auf das IPX-Protokoll bis zum Betrieb von Firewall-Lösungen.

3.2.2 Anwendungen

Bereiche, in denen mindestens die Häfte der Fachhochschulverwaltungen Software einsetzt oder für die nächsten zwei Jahre einzusetzen plant, sind:

- Studentenverwaltung, Prüfungsverwaltung, Zulassung, Praxissemesterverwaltung
- Bibliothek (Sokrates)
- Haushaltsaufstellung, Mittelbewirtschaftung
- Stellen- und Personalverwaltung
- Raum- und Gebäudeverwaltung, Lehrraumverwaltung
- Inventarisierung
- Textverarbeitung, Adressen
- Hochschulwahlen

Im Einzelnen ergaben sich die in Tabelle 3.10 zusammengestellten Ergebnisse. Beim Ranking wurde die Anzahl der Fachhochschulen, die eine Anwendung heute nutzen, als ein Hauptkriterium verwendet. Bei gleicher Anzahl wurde die Anzahl der Nennungen für die geplante Einführung innerhalb der nächsten zwei Jahre als Sortierkriterium verwendet.

Rang	Anwendung	heute im Einsatz		geplant bis 9/98
		Anzahl	Anteil	Anzahl
1	Textverarbeitung, Dokumentenverwaltung	12	100%	0
1	Bibliotheksrechner/Sokrates	12	100%	0
2	Studentenverwaltung	9	75%	3
3	Zulassungswesen	9	75%	2
3	Mittelbewirtschaftung	9	75%	2
4	Adressverteiler und Adressdatenbanken	9	75%	0
5	Inventarisierung	8	67%	3
6	Prüfungsverwaltung	7	58%	5
7	Praxissemesterverwaltung	5	42%	4
8	Raum- und Gebäudeverwaltung	5	42%	1
8	Verteilungsverfahren (Bewirtschaftung) für Sondermittel	5	42%	1
9	Hochschulwahlen	4	33%	3
10	Haushaltsaufstellung	4	33%	2
11	Telefonverzeichnis	4	33%	1
12	(Lehr-)Raumvergabe	3	25%	5
13	Betriebstechnik, Gebäudeleittechnik, Energieverbrauch	3	25%	2
14	Kapazitätsberechnung	3	25%	1
14	Fernmeldeabrechnung	3	25%	1
15	Stellenverwaltung / -bewirtschaftung	2	17%	4
15	Personalverwaltung	2	17%	4
16	Lehrveranstaltungsplanung	2	17%	3
17	Gefahrstoffkataster	1	8%	2
17	Projekt- und Forschungsdatenbank	1	8%	2

Rang	Anwendung	heute im Einsatz		geplant bis 9/98
		Anzahl	Anteil	Anzahl
18	Kassenverfahren	1	8%	1
18	Studenten-Informationssystem	1	8%	1
19	Sicherheitsverwaltung	1	8%	0
19	allgemeine Planungsverfahren	1	8%	0
20	Personalratswahlen	0	—	2
20	Lagerverwaltung	0	—	2
21	Bezügeverfahren	0	—	1
21	RLV-Überwachung	0	—	1
22	Seminarplatzvergabe	0	—	0

Tabelle 3.10: Umfrageergebnis Anwendungen an den Fachhochschulen.
[Die Prozentangaben beziehen sich auf den Rücklauf von 12 Fragebögen (=100%)]

Teil II: Lösungsansätze

Kapitel 4

Virtualisierung der Netze

4.1 Überblick

Virtuelle Netze werden in Zukunft eine wichtige Rolle bei der Sicherung der Datenübertragung im Rahmen eines IT-Sicherheitskonzepts spielen. Von entscheidender Bedeutung für einen konkreten Einsatz wird aber die jeweilige vorhandene Netzinfrastruktur sein. Aus diesem Grund steht am Anfang dieses Kapitels eine Skizzierung der aktuellen Struktur der Hochschulnetze, gefolgt von einer kurzen Charakterisierung der im Einsatz befindlichen Netztechnologien. Danach werden die unterschiedlichen Konzepte für virtuelle Netze näher vorgestellt.

4.2 Netze und Netzstrukturen in den bayerischen Hochschulen

In den meisten Hochschulen entstanden schon sehr frühzeitig vereinzelt Netzinseln. Seit etwa 1990 erfolgt ein systematischer Ausbau der Netzinfrastrukturen in den Hochschulen, entscheidend gefördert durch das Netzinvestitionsprogramm (NIP) des Bundes und der Länder auf der Basis des Berichts der Netzkommission.

Zur Beschreibung der komplexen Struktur der hochschulinternen Rechnernetze kann man eine Hierarchie der Netzebenen definieren, die der Struktur der Versorgungsebenen entspricht:

- **Etagennetze**

  An ein Etagennetz ist im Allgemeinen die DV-Ausstattung einer Benutzergruppe (Lehrstuhl, Institut, Fachbereich) angeschlossen. Typischerweise handelt es sich hierbei um Arbeitsplatzrechner und lokale Server. Die Standardtechnologie ist derzeit Ethernet mit einer Übertragungsrate von 10 Mbit/s. Die Etagenverkabelung wird in

Abhängigkeit von der lokalen Infrastruktur vorwiegend mit Koaxialkabel- oder Twisted-Pair(TP)-Technik durchgeführt. Unter bestimmten Umständen werden schon derzeit Lichtwellenleiter (LWL) bis zum Arbeitsraum bzw. Arbeitsplatz installiert.

- **Gebäudenetze**

  Ein Gebäudenetz verbindet die einzelnen Etagennetze eines Gebäudes. Die Technologie ist in der Regel Ethernet mit 10 Mbit/s und nur in Ausnahmefällen Fast-Ethernet bzw. Fiber Distributed Data Interface (FDDI) mit bis zu 100 Mbit/s. Die vertikale Gebäudeverkabelung mit der Anbindung der Etagennetze wird heute bereits überwiegend in Lichtwellenleiter-Technik ausgeführt. Damit ist es möglich, die Übertragungsraten dem aktuellen Bedarf anzupassen.

- **Campusnetze**

  Ein Campusnetz verbindet die Gebäudenetze einer Hochschule, die auf dem gleichen Gelände liegen. Im Allgemeinen sind die Campusnetze in Lichtwellenleiter-Technik ausgeführt. Die Übertragungsrate beträgt z.B. beim Einsatz von FDDI 100 Mbit/s. An den Übergängen zu den Gebäudenetzen sind Router installiert, die eine Einteilung in Subnetze unterstützen.

  Die Topologien und die Dimensionierungen der Campusnetze erlauben im Allgemeinen den parallelen Betrieb unterschiedlicher Netz-Technologien, wie Ethernet, FDDI, Asynchronous Transfer Mode (ATM), aber auch proprietäre Kanalkopplungen.

- **Stadtnetze**

  Sind die Bereiche einer Hochschule über eine Stadt verteilt, dann verbindet ein Stadtnetz die einzelnen Campusnetze und die nicht in ein Campusnetz integrierten Gebäudenetze miteinander. In der Regel sind die Stadtnetze schon aufgrund der Entfernungen in Lichtwellenleiter-Technik ausgeführt und langfristig angemietet. Die Realisierung erfolgt zumeist in Form eines oder mehrerer FDDI-Ringe mit einer Übertragungsrate von 100 Mbit/s. Ergänzt werden diese LWL-Netze durch angemietete Datenleitungen mit den typischen Übertragungsraten von 64 kbit/s und 2 Mbit/s.

  Ein paralleler Betrieb unterschiedlicher Netz-Technologien ist hier im Allgemeinen aus Kostengründen nicht möglich.

- **Weitverkehrsnetze**

  Die Anbindung an die nationalen und internationalen Netze wird im Hochschulbereich vorwiegend über das deutsche Wissenschaftsnetz (WiN / B-WiN) durchgeführt, zumeist mit Anschlusskapazitäten von 2 Mbit/s, 34 Mbit/s oder 155 Mbit/s.

- **Außenzugänge zum Hochschulnetz**

  Der Zugang von häuslichen Arbeitsplatzrechnern von Hochschulmitarbeitern und Studierenden zum Hochschulnetz ist in der Regel über Kommunikationsserver mit ISDN- und/oder Wählmodem-Zugängen realisiert. Eine analoge Schnittstelle erlaubt jeweils nur eine Verbindung zur gleichen Zeit. Die Übertragungsrate ist dabei von der Leistungsfähigkeit der eingesetzten Modems abhängig (z.Zt. bis 56 kbit/s). Bei den digitalen Schnittstellen ist zwischen S_0 (mit 2 Nutzkanälen) und S_{2M} (mit 30 Nutzkanälen) zu unterscheiden. Jeder Nutzkanal ermöglicht eine Verbindung mit einer Übertragungsrate von 64 kbit/s.

Die heutigen Hochschulnetze sind gekennzeichnet durch Ethernet und FDDI. Migrationen zu neuen Technologien stehen bevor. Ein stufenweiser Umstieg auf ATM auf allen Netzebenen und die Integration von virtuellen LANs sind als nächste Innovationsschritte erkennbar bzw. in Teilbereichen bereits im Gange.

4.3 Entwicklungen der Netztechnologie

Die Architekturkonzepte von Netzen haben sich im Verlauf der letzten 20 Jahre rasant weiterentwickelt. Dies ist in erster Linie auf den raschen Anstieg der Rechnerzahlen, den stetig wachsenden Kommunikationsbedarf und die Verfügbarkeit von herstellerunabhängigen Standards und Quasi-Standards zurückzuführen.

Einzelne LANs

Die LAN-Architekturen brachten deutliche Verbesserungen der Leistung im lokalen Bereich und der Zuverlässigkeit im Vergleich zu den früheren meist proprietären Netzen, die über serielle Leitungen arbeiteten.

Bridge-basierte LANs

Durch den Einsatz von Bridges wurde die Installation größerer LANs unterstützt. Durch die Isolierung des lokalen Unicast-Verkehrs (Punkt-zu-Punkt-Verbindungen; ein Unicast-Paket enthält die Media Access Control (MAC)-Adressen von Quellen- und Zielrechner) auf Teile des Netzes wurde die Netzbelastung eingegrenzt.

Jedoch können bridge-basierte Netze Broadcast-Stürme (lawinenartige Ausbreitung von Einer-an-Alle-Nachrichten, verursacht durch fehlerhafte Broadcast-Pakete) nicht verhindern.

Router-basierte Netze

Die Einführung der router-basierten Netze wurde durch verschiedene Faktoren getrieben. Neben dem schnellen Wachstum der Netze und dem Wunsch nach einer logischen Aufteilung der Netze spielte die starke Verbreitung der Client/Server-Lösungen eine große Rolle.

Durch den Einsatz von Routern erreicht man eine Unterteilung eines Netzes in Subnetze für Abteilungen, Arbeitsgruppen, u.ä. und damit auch eine Isolierung des Datenverkehrs der Arbeitsgruppe. Durch das Bearbeiten der Daten auf der Schicht 3 des OSI-Modells ist es möglich, Broadcast-Stürme zu verhindern.

Switch-basierte Netze

Der Einsatz von Switches im LAN-Bereich eröffnet die Möglichkeit, Arbeitsplatzrechner und Server über Standard-Netzanbindungen (Ethernet, Token-Ring, FDDI) dediziert, d.h. mit garantierter Bandbreite und ohne ein Konkurrieren mit anderen Endgeräten, anzuschließen und führt bei gut geplantem Einsatz zu einer deutlichen Steigerung der Durchsatzraten. Die Kopplung der LAN-Switches untereinander über Standard-Netzanbindungen ist möglich.

Ziel der switch-basierten Netze ist es, jedes Endgerät dediziert ans Netz anzuschließen (d.h. die Verkehrsströme der einzelnen Endgeräte voneinander zu entkoppeln) und die Bandbreite dem jeweiligen Bedarf anzupassen.

In einem weiteren Schritt werden die LAN-Switches über ATM-Switches miteinander verbunden. Mittels spezieller Techniken (z.B. LAN Emulation) ist das Zusammenarbeiten von Rechnern aus dem LAN-Bereich und ATM-Rechnern möglich.

4.4 Switches

Im Folgenden soll näher auf Switch-Techniken eingegangen werden. Wie schon in 4.3 erwähnt, kann man die Switches grob in LAN-Switches und ATM-Switches unterteilen.

LAN-Switches

In den bestehenden Netzen, die größtenteils router-basiert ausgerichtet sind, entstehen viele Engpässe unter anderem durch protokollbedingte Kollisionen und die relativ geringe Performance der Router. Ein LAN-Switch ist eine Netzkomponente, die normalerweise den Datenverkehr auf die beteiligten Partner (verbindungsorientiert auf Port-Basis) beschränkt. Er kann — stark vereinfacht — mit einer Multiport-Bridge verglichen werden. Das Vermitteln der Information erfolgt zwischen Ports kollisionsfrei über eine Switchmatrix und die Backplane.

Die Switching-Verfahren lassen sich grob in drei Kategorien einteilen:

- *Cut-Through-Verfahren*
- *Store-and-Forward-Verfahren*
- *Cell-Oriented-Verfahren.*

Das **Cut-Through-Switching-Verfahren (CT-Switches)** erlaubt, betrachtet man alle Ausprägungen der LAN-Switches, die kürzesten Latenzzeiten, da bei jedem Paket lediglich eine Analyse bezüglich Quellen- und Zieladresse durchgeführt wird, so dass bereits nach dem Empfang der ersten 12 Bytes eine Verbindung durchgeschaltet werden kann.

Die Nachteile der CT-Switches liegen einerseits darin, dass sie nur auf MAC-Adressen-Ebene switchen können, und andererseits im Weiterleiten fehlerhafter Pakete.

Die Arbeitsweise des **Store-and-Forward-Switching-Verfahrens (SF-Switches)** ist vergleichbar mit der von Routern und Bridges. Die SF-Switches empfangen das gesamte Paket, speichern es in einem internen Puffer und können somit neben der Ermittlung von Quellen- und Zieladresse auch eine Fehlererkennung sowie weitere Paketbearbeitungsprozeduren durchführen.

Der Nachteil dieser Switches liegt in den sehr hohen Durchlaufzeiten. In extremen Fällen sind die Durchlaufzeiten bis zum Faktor 12 höher als bei den CT-Switches. Ein kontinuierlicher Datenfluss kann nicht garantiert werden, was Einfluss auf die Qualität insbesondere bei Sprach- und Videoanwendungen und anderen zeitkritischen Datenanwendungen hat. Andererseits sind SF-Switching-Verfahren für höhere Funktionalitäten jedoch unabdingbar.

Die **Cell-Oriented-Switching-Verfahren (CO-Switches)** vereinen die Vorteile der CT- und der SF-Switches. Je nach Hersteller werden die ankommenden Pakete in Zellen von 48 bis 64 Bytes zerlegt und sofort weitertransportiert. Die Durchlaufzeiten vergrößern sich bei den CO-Switches im Vergleich zu den CT-Switches um etwa den Faktor 4 bis 5.

Der große Vorteil der CO-Switches liegt darin, dass durch den Transport gleich langer Zellen die Kontinuität des Datenflusses gewahrt bleibt. Ihr Einsatz ist insbesondere dann zu empfehlen, wenn im Backbone-Bereich ATM eingesetzt wird.

Neben der obigen sind auch noch andere Klassifizierungen der Switches möglich. So kann man zum Beispiel zwischen Layer-2- und Layer-3-Switches unterscheiden. Während die Layer-2-Switches mit MAC-Adressen oder port-basierend arbeiten, können die Layer-3-Switches Informationen der Schicht 3 auswerten, sie agieren protokollsensitiv.

ATM-Switches

Ein ATM-Netz besteht aus einer Reihe von ATM-Switches, die über ATM-Links miteinander verbunden sind. ATM-Netze arbeiten grundsätzlich verbindungsorientiert. Das bedeutet, dass vor einem Datentransfer zwischen den Kommunikationspartnern eine virtuelle Verbindung über das Netz aufgebaut werden muss. Dabei wird zwischen virtuellen Pfaden und virtuellen Kanälen unterschieden, wobei über einen virtuellen Pfad mehrere virtuelle Kanäle definiert sein können.

Hauptaufgabe eines ATM-Switches ist es, eine Zelle über einen Link zu empfangen, mit Hilfe einer Übersetzungstabelle den Ausgangsport zu bestimmen und die Zelle zum Ausgangslink zu übertragen. Der Aufbau der Übersetzungstabellen wird durch die beiden grundsätzlichen Arten der ATM-Verbindungen bestimmt, den permanenten virtuellen Verbindungen (Permanent Virtual Circuits, PVCs) und den gewählten virtuellen Verbindungen (Switched Virtual Circuits, SVCs).

Alle ATM-Zellen haben eine Länge von jeweils 53 Bytes, davon sind 48 Bytes Daten. Diese relativ kurzen Zellen ermöglichen kurze Latenzzeiten. Das ist wichtig bei hohen Anforderungen an die Güte des Übertragungsdienstes (Quality of Service [QoS]). Es werden fünf Service-Klassen unterschieden. Jeder Service-Klasse kann eine Dienst-Kategorie zugeordnet werden.

Service-Class A: Constant Bit Rate (CBR)
Dienste: Sprache und Video mit konstanter Bit Rate

Service-Class B: Real-Time Variable Bit Rate (rt-VBR)
Dienste: Sprache und Daten mit variabler Bit Rate

Service-Class C: Non-Real-Time Variable Bit Rate (nrt-VBR)
Dienste: verbindungsorientierter Datenverkehr
(z.B. X.25, Frame Relay, SNA,...)

Service-Class D: Available Bit Rate (ABR)
Dienste: verbindungsloser Datenverkehr
(z.B. TCP/IP, IPX, ...)

Service-Class X: Unspecified Bit Rate (UBR)
Dienste: Dienste, die nach dem *Best-Effort*-Prinzip erbracht werden.

4.5 Virtuelle Netze (VLANs)

Motivation für die Virtualisierung der Netze

Die rasante Zunahme der Anzahl der Rechner, die Steigerung des Durchsatzvermögens der Rechner, die Zentralisierung von Hochleistungs-Servern, die Zunahme von bandbreitenintensiven Anwendungen (z.B. Client/Server) sowie die Einführung zeitabhängiger Anwendungen (Multimedia) sind der Motor für die aktuellen Entwicklungen im Netzbereich, die mit den daraus resultierenden Anforderungen Schritt zu halten versuchen.

Mit der Zunahme der Komplexität der Unternehmen (auch der Hochschulen) sind Netzkonzepte gefragt, die eine einfache Abbildung der internen Organisation auf die Netztopologie erlauben und dabei u.a. die Bildung dynamisch verteilter Arbeitsgruppen unterstützen. Dafür ist es erforderlich, sich von der physischen Struktur der Netze zu lösen und eine logische Struktur über der physischen zu definieren.

Im Folgenden werden einige Ziele genannt, die man durch die Virtualisierung der lokalen Netze und die Einführung entsprechender Techniken (VLAN-Techniken) erreichen möchte.

- **Flexibilität der Netze**
  - Bildung von Projektteams und Abtrennen der projektbezogenen Kommunikation vom restlichen Netzverkehr,
  - automatisches Erkennen von Verlagerungen einzelner Endgeräte,
  - Integration von Heimarbeitsplätzen und kleineren ausgelagerten Stellen,

  - Zuordnung von zentral installierten Servern zu räumlich getrennten Arbeitsgruppen.

- **Leistungsfähigkeit der Netze**

  Durch den Einsatz von Switches kann man den bekannten Kapazitätsengpässen aus den bridge- bzw. router-basierten Netzen schon recht effektiv begegnen. Durch den Einsatz von VLAN-Techniken kann man zusätzlich die Broad- und Multicasts auf die Bereiche beschränken, die zum gleichen VLAN gehören.

- **Sicherheit in den Netzen**

  Mit Hilfe der VLAN-Techniken erreicht man, dass im Allgemeinen alle Daten (auf der Ebene 2) innerhalb eines virtuellen Netzes verbleiben. Überlappen sich mehrere unterschiedliche virtuelle Netze auf einem physischen Segment, so besteht natürlich dennoch die Möglichkeit, Daten anderer virtueller Netze zu empfangen.

  Will man die VLAN-Technik dafür nutzen, um Datenströme verschiedener logischer Netze vollständig voneinander zu trennen, dann muss man konsequenterweise dafür Sorge tragen, dass entweder alle Stationen eines physischen Netzsegments zum selben VLAN gehören oder, wenn erforderlich, bei der Vernetzung der Wechsel zu einer hierarchischen Struktur mit dedizierten Netzverbindungen vollzogen wird.

VLAN-Konzepte

Virtuelle Netze (VLANs) sind eine konsequente Antwort auf die oben beschriebenen Anforderungen an die Kommunikationstechnik. Nach IEEE 802.1q, dem in Vorbereitung befindlichen Standard, ist ein virtuelles Netz eine logische Gruppierung beliebiger Endgeräte innerhalb einer mit Hilfe von Bridges aufgebauten Netzinfrastruktur. Danach ist es in einem virtuellen Netz möglich, beliebige Netzteilnehmer aus möglicherweise unterschiedlichen physischen Netzsegmenten zu einem logischen Netz zu vereinen, ohne dafür das Netz physisch umstrukturieren zu müssen. Aufgabe der VLAN-Implementierung ist es, dafür Sorge zu tragen, dass alle Daten, auch Broad- und Multicasts, in einem virtuellen Netz bleiben. Damit entspricht ein virtuelles Netz einer *Broadcast-Domain*, wie sie von der klassischen Ethernet-Technik her bekannt ist. Innerhalb eines virtuellen Netzes werden die Daten über Bridges geleitet. Somit sind VLANs „flache“ Netze ohne Hierarchien. Router-Funktionalität wird nur eingesetzt, um verschiedene virtuelle Netze miteinander zu verbinden.

Das Sichten der derzeit angebotenen VLAN-Lösungen macht deutlich, dass es sehr unterschiedliche Ansätze gibt, die Zugehörigkeit zu einem VLAN zu definieren. Art und Umfang der Implementierung sind derzeit noch herstellerabhängig. Im Folgenden werden nach einem in diesem Bereich eingeführten Klassifizierungsschema vier Klassen von VLANs betrachtet. Andere Klassifizierungen wären ebenfalls möglich.

- ***Port-basierte VLANs (Klasse 1)***

  Dies ist die einfachste Form eines virtuellen Netzes. Hier werden beliebige physische Ports eines Switches einem virtuellen Netz zugeordnet. Neuere Implementierungen unterstützen dabei auch eine Ausdehnung eines VLANs auf mehrere Switches.

Port-basierte VLANs erlauben nicht den Betrieb von mehreren VLANs auf einem physischen Segment bzw. einem Switch-Port. Außerdem werden Verlagerungen von Endgeräten in ein anderes physisches Segment nicht automatisch erkannt.

- ***MAC-basierte VLANs (Klasse 2)***

  Bei dieser Form werden Endgeräte einem VLAN über die MAC-Adresse, die an die Netzkarte gebunden ist, zugeordnet. MAC-basierte VLANs erlauben den Betrieb von mehreren virtuellen Netzen auf einem physischen Segment. Umzüge eines Endgeräts in ein anderes physisches Segment werden über die MAC-Adresse automatisch erkannt.

  MAC-basierte VLANs erlauben aber nicht, dass Endgeräte (z.B. Server) mehreren virtuellen Netzen angehören. Außerdem ist der erforderliche Administrationsaufwand, bedingt durch die Notwendigkeit der Pflege einer großen Anzahl kryptischer MAC-Adressen, sehr hoch.

- ***Layer-3-basierte VLANs (Klasse 3)***

  Hier werden Protokolltypen oder Netzschichtadressen (z.B. Subnetz-Adressen) für die Zuordnung zu einem virtuellen Netz benutzt. Diese Funktionalität ist nicht mit dem Routing zu verwechseln. Layer-3-basierte VLANs arbeiten protokollsensitiv. Sie eignen sich besonders für Protokolle wie TCP/IP, IPX, weniger für Apple-Talk und DECnet und gar nicht für nicht vermittelbare Protokolle wie NetBIOS. Layer-3-basierte VLANs ermöglichen ein recht hohes Maß an Flexibilität und sie sind leichter zu administrieren als MAC-basierte VLANs.

  Der gravierende Nachteil der Layer-3-basierten VLANs ist die relativ hohe Anforderung an die Performance der Switches.

- ***Policy-basierte VLANs (Klasse 4)***

  In einem ersten Ansatz erlauben die policy-basierten VLANs eine Kombination der drei oben angeführten VLAN-Klassen. Die Zuordnung erfolgt über MAC-Adressen und/oder über Netzschichtadressen. Zusätzlich können dann noch, abhängig von der jeweiligen proprietären Implementierung, weitere Teile der Frames (z.B. das Ethernet-Protokoll-Typ-Feld) für die Zuordnung zu virtuellen Netzen herangezogen werden.

Während die virtuellen Netze der Klassen 1 – 3 mittlerweile von fast allen LAN-Switch-Herstellern unterstützt werden, sind die Ansätze für policy-basierte VLANs bisher proprietär.

Damit die Kommunikation sowohl innerhalb eines virtuellen Netzes als auch zwischen verschiedenen virtuellen Netzen funktioniert, ist es erforderlich, dass die benötigten Informationen (Adresstabellen) bei den beteiligten Switches sich immer in einem konsistenten Zustand befinden. Dazu müssen regelmäßig Informationen über das Netz ausgetauscht werden. Dieser Informationsabgleich wird meistens über proprietäre Verfahren bewerkstelligt. Es gibt dazu mindestens drei unterschiedliche Verfahren, die im Folgenden kurz erläutert werden.

- ***Adressabgleich***

  Die beteiligten Switches tauschen regelmäßig in sehr kurzen Abständen die Adresstabellen aus. Wird ein neuer Teilnehmer am Netz erkannt, dann ergänzt der Switch, an den der Teilnehmer angeschlossen ist, seine Adresstabelle und sendet eine Nachricht mit hoher Priorität an die anderen Switches.

  Deutliche Nachteile dieses regelmäßigen Austausches der Adresstabellen sind, zumindest bei großen Netzen, das sehr hohe Verkehrsaufkommen und die Synchronisationsprobleme. Die Implementierungen sind herstellerspezifisch.

- ***Frame-Tagging***

  Beim Frame-Tagging-Verfahren wird jedem Datenpaket ein kurzes Datenfeld, ein sogenanntes ‘Tag’, hinzugefügt. Dieses Tag liefert die Information, zu welchem virtuellen Netz das Datenpaket gehört. Dieses Verfahren produziert allerdings einen relativ großen Overhead für die Synchronisation der Datenpakete. Hinzu kommt bei Paketen mit maximaler Länge die Problematik, dass das Hinzufügen eines Tags zu fehlerhaften Paketen führt, die vernichtet werden. Auch für dieses Problem gibt es herstellerspezifische Lösungen.

  Auf der Suche nach herstellerunabhängigen Lösungen haben sich einige Hersteller entschlossen, Teile des nach dem Standard IEEE 802.10 (Secure Data Exchange) erweiterten MAC-Frames für das Frame Tagging zu nutzen. Hier ist auch definiert, wie Pakete maximaler Größe geteilt und später wieder zusammengesetzt werden müssen. Dieses Verfahren ist für Ethernet, FDDI, Token Ring und High-level Data Link Control (HDLC) definiert.

  Auch der Ansatz der Layer-3-basierten Zuordnung zu virtuellen Netzen ist eine Variante des Frame-Tagging-Verfahrens. Dieses Verfahren setzt aber sehr hohe Leistungsfähigkeit der Switches und umfangreiche Protokollkenntnisse des Netzadministrators voraus.

- ***Zeitmultiplexverfahren***

  Das dritte Verfahren basiert darauf, dass das die Switches verbindende Backbone in Kanäle fester Bandbreite aufgeteilt wird. Jedes virtuelle Netz erhält exklusiv einen oder mehrere dieser Slots für die Übertragung der Daten. Damit muss jeder Switch nur wissen, welche Slots welchem virtuellen Netz zugeordnet sind. Der bei den beiden anderen Verfahren beschriebene Overhead entfällt, jedoch bleibt ungenutzte Bandbreite brach liegen, da sie anderen VLANs nicht zur Verfügung steht. Um eine möglichst optimale Auslastung zu erhalten, ist eine stetige Beobachtung und Anpassung erforderlich.

  Es ist zu erwarten, dass in dem Standard IEEE 802.1q das Frame-Tagging-Verfahren favorisiert wird. Die in der Entscheidung befindlichen Vorschläge grenzen sich aber deutlich von dem oben beschriebenen Verfahren nach IEEE 802.10 ab. Damit soll verhindert werden, dass VLAN-spezifische Aspekte die Bestrebungen für Sicherheitsstandards beeinflussen.

4.6 Virtuelle LANs in einer verteilten Umgebung

Dort wo bereits ein historisch gewachsenes Netz vorhanden ist, muss bei der Einführung der VLAN-Technik diese neue Netztechnologie in ein bestehendes, gewachsenes Umfeld integriert werden. Ein leistungsfähiges Backbone ist heute selbstverständlicher Bestandteil eines Netzes. Durch den Einsatz von VLAN-Techniken wird die Belastung im Backbone-Bereich enorm wachsen. Eine Aufgabe des Backbones ist dabei, für eine Ortstransparenz der angeschlossenen Benutzer zu sorgen.

Im Folgenden wird auf Entwicklungen für die Kopplung von virtuellen Netzen über ein ATM-Backbone eingegangen. Die Möglichkeit der Kopplung über FDDI nach IEEE 802.10 ist weiter oben (Frame-Tagging-Verfahren) beschrieben. Dieses Verfahren wird dem zu erwartenden Standard IEEE 802.1q nicht genügen.

- ***Multiprotocol Encapsulation***

  Bereits im Juli 1993 wurden im RFC 1483 die Spezifikationen für „Multiprotocol Encapsulation“, auch bekannt unter „Bridge and Router Tunnels“, festgelegt. In diesem RFC werden Methoden beschrieben, wie Netzverkehr protokolltransparent über ein ATM-Netz transportiert werden kann. Für diesen Zweck werden PVCs als Tunnel definiert. Durch Multiprotocol Encapsulation kann keiner der Vorteile von ATM (z.B. QoS, SVCs, Routing-Fähigkeit) genutzt werden.

- ***Classical IP***

  Im Januar 1994 wurden im RFC 1577 die Spezifikationen für „Classical IP and ARP over ATM“ veröffentlicht. Ziel dieses RFCs ist es, den IP-Verkehr möglichst effektiv über ATM-Netze zu transportieren unter Einbeziehung von direkt ans ATM angeschlossenen Endgeräten. Classical IP kann sowohl PVCs als auch SVCs nutzen. In dem RFC-Dokument wird aufgezeigt, wie ein ATM-Netz als logisches IP-Subnetz (LIS) in eine geroutete Netzumgebung eingebunden werden kann.

  Die Kommunikation von Endgeräten ist nur innerhalb eines logischen IP-Subnetzes definiert. Für den Übergang zwischen unterschiedlichen logischen IP-Subnetzen werden Router eingesetzt. Es ist allerdings auch möglich, ein Endgerät in mehreren logischen IP-Subnetzen einzutragen.

  Ein gewichtiger Nachteil von Classical IP ist, dass die Integrationsmöglichkeit von ATM rein auf die IP-Umgebung beschränkt bleibt. Zudem werden keine ATM-spezifischen Eigenschaften genutzt. Das ATM-Netz unterstützt lediglich den Einsatz von PVCs und SVCs.

- ***LAN Emulation***

  LAN Emulation (LANE) wurde Mitte 1995 durch das ATM-Forum veröffentlicht. Hauptziele der Entwicklung waren neben der Aufhebung der Beschränkung auf IP auch ein sanftes Zusammenwachsen von ATM-Netzen und bestehenden LANs.

  Nach den Festlegungen im Standard erlaubt LANE eine protokolltransparente Kopplung von herkömmlichen LANs über ATM sowie die Kommunikation mit direkt an das ATM-Netz angeschlossenen Endgeräten. Dabei gaukelt LANE der herkömmlichen

LAN-Umgebung vor, es handele sich bei ATM lediglich um ein weiteres 802.x-LAN. Das bedeutet, dass LANE eine Service-Schicht für die Netzschicht (Schicht 3) definiert, die identisch ist mit der existierender LANs. Dadurch können die vorhandenen Endgeräte und Applikationen ohne Modifikation weiter benutzt werden.

Da LAN Emulation auf der OSI-Schicht 2 angesiedelt ist, unterstützt es sowohl alle routbaren als auch die nicht routbaren Protokolle. In dem Standard ist weiterhin festgelegt, wie Endgeräte mit gleicher Netzzugangstechnik und wie Ethernet- oder Token-Ring-Endgeräte mit ATM-Endgeräten über ein ATM-Netz kommunizieren. LANE definiert jedoch nicht, wie Ethernet- und Token-Ring-Endgeräte über ein ATM-Netz miteinander Daten austauschen können. Außerdem ist die Behandlung von FDDI-Frames nicht definiert. Hier muss zunächst eine Umwandlung in Ethernet- bzw. Token-Ring-Frames durchgeführt werden.

Die LAN Emulation ist in Form einer Client/Server-Architektur definiert und besteht aus zwei Komponenten:

- LAN Emulation Client (LEC),
- LAN Emulation Service.

Der LAN Emulation Service zerfällt logisch in drei Server-Bestandteile:

- LAN Emulation Configuration Server (LECS),
- LAN Emulation Server (LES),
- Broadcast and Unknown Server (BUS).

Die LAN Emulation Service-Funktionen können sowohl zentral auf einem ATM-Switch oder einem entsprechend geeigneten System als auch verteilt über das Netz implementiert werden. Die Server haben die Aufgabe, sowohl Unicasts als auch Broad- und Multicasts zu vermitteln und die LECs bei der Ermittlung von ATM-Zieladressen zu unterstützen.

Für jedes emulierte LAN muss ein LES existieren, der die Rolle einer Kommando- und Kontrollzentrale wahrnimmt. Ihm fällt die Aufgabe zu, MAC-Adressen zu registrieren und aufzulösen. Der BUS ist zuständig für die Übertragung aller Broad- und Multicasts und des *unknown unicast*-Verkehrs innerhalb des emulierten LANs. Für jedes emulierte LAN muss ebenfalls ein BUS implementiert sein. Ein LECS ist die Kontrollinstanz für die gesamte Umgebung. Er hält Konfigurations-Informationen über das ATM-Netz bereit und liefert die Adressen der LES an interessierte Clients. Ein LECS kann alle emulierten LANs in einem Netz bedienen.

Der LEC befindet sich in jedem direkt angeschlossenen Endgerät oder *Edge-Device* (z.B. Bridge, Router). Sind in einem Endgerät oder Router mehr als ein LEC implementiert, dann kann dieses Gerät an mehr als einem emulierten LAN teilnehmen.

Die oben beschriebenen Spezifikationen sind mit LAN Emulation Version 1.0 verfügbar. Die Version 2.0, die einen erweiterten Funktionsumfang aufweisen wird, befindet sich in der Standardisierungsphase.

- ***Multiprotocol over ATM***

  Multiprotocol over ATM (MPOA) ist ein weiterer Ansatz, der sich in der Spezifizierung durch das ATM-Forum befindet. MPOA setzt auf einer Reihe von Spezifikationen anderer Produkte auf, darunter auch LAN Emulation, Classical IP und Next-Hop Routing Protocol.

  Vereinfacht dargestellt hat MPOA drei große Ziele:

  1. Definition eines leistungsfähigen Weges mit kurzen Latenzzeiten, um IP und andere Protokolle durch ein ATM-Netz zu routen.
  2. Möglichkeit für den Netzmanager, virtuelle Netze über Routergrenzen hinweg zu definieren, ohne Rücksicht auf die physischen Gegebenheiten im Netz.
  3. Möglichkeit der Nutzung von ATM-spezifischen Fähigkeiten (z.B. Quality of Service).

  Ein großer Unterschied zum LANE besteht darin, dass MPOA mehr auf Layer-3-Netze ausgerichtet ist. Es ist zu erwarten, dass MPOA abwärtskompatibel zu LANE sein wird. Die erste Phase der Spezifizierung von MPOA wurde im Herbst 1997 von der MPOA-Arbeitsgruppe des ATM-Forums beendet. Derzeit ist jedoch noch nicht absehbar, wann mit interoperablen MPOA-Implementierungen für den Einsatz in einer heterogenen Umgebung zu rechnen sein wird.

4.7 Virtualisierung durch Krypto-Kanäle

Neben den oben beschriebenen Virtualisierungstechniken gibt es auch noch andere Möglichkeiten, logische Teilnetze innerhalb eines Gesamtnetzes zu definieren und zu realisieren. Die hier beschriebene Lösungsvariante basiert auf dem Einsatz von Krypto-Boxen und PC-basierten Krypto-Lösungen, die unterschiedliche Sicherheitsdienste (z.B. Vertraulichkeit, Authentifizierung, Zugangskontrolle, Rechteverwaltung, ...) anbieten. Ausführungen zum Thema „Verschlüsselung“ befinden sich im Kapitel 6. Im Folgenden sollen anhand von Beispielen Einsatzmöglichkeiten für Krypto-Boxen vorgestellt werden.

1. **Aufbau einer gesicherten Kommunikation zwischen ausgewählten Endgeräten innerhalb eines LAN-Segments:**

   Die Bildung von logischen Bereichen innerhalb eines LAN-Segments kann man durch den gezielten Einsatz von Krypto-Boxen erreichen, eventuell ergänzt durch PC-basierte Krypto-Lösungen. Mit Hilfe der verschlüsselten Übertragung der Daten zwischen definierten Kommunikationspartnern erzielt man eine Quasi-Virtualisierung

des Netzes. Neben der Verschlüsselung bieten die Krypto-Boxen im Allgemeinen noch zusätzlich eine Reihe weiterer Sicherheitsdienste.

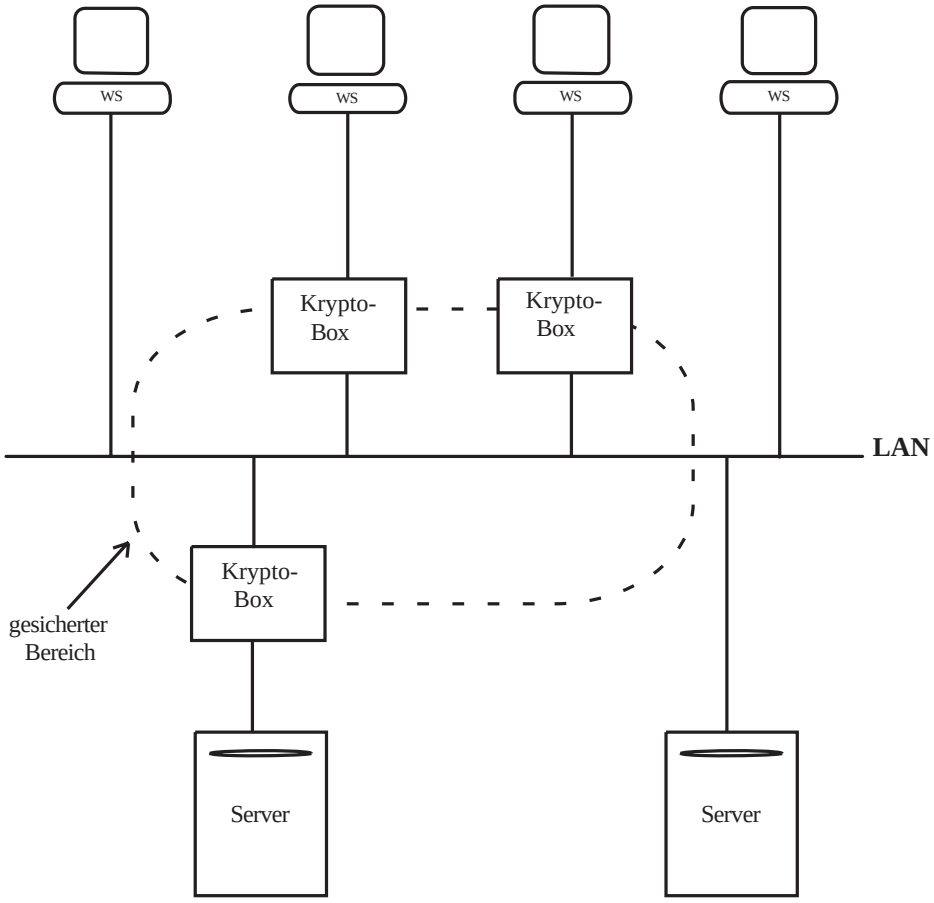


Abbildung 4.1: Gesicherte Kommunikation innerhalb eines LAN-Segments

2. Aufbau einer gesicherten Kommunikation zwischen mehreren LAN-Segmenten über offene (öffentliche und/oder private) Netze:

Die Bildung von logischen Bereichen, die sich über mehrere LAN-Segmente erstrecken und zudem über öffentlich zugängliche Netze verbunden sind, erreicht man durch den Einsatz von Krypto-Boxen an den Übergängen von den zu schützenden zu den öffentlich zugänglichen Netzen und den zusätzlichen Einsatz von Routing-Funktionalität. Neben Filtermechanismen (siehe auch Kapitel 5) erlauben die Router auch das Definieren von logischen Kanälen (Tunneling auf Layer 3), die einen verdeckten Informationsaustausch zwischen Kommunikationspartnern bzw. Teilnetzen

ermöglichen. Neben den reinen Verschlüsselungsboxen gibt es auch Produkte, die neben der Verschlüsselung zusätzlich auch die Routing-Funktionalität beinhalten.

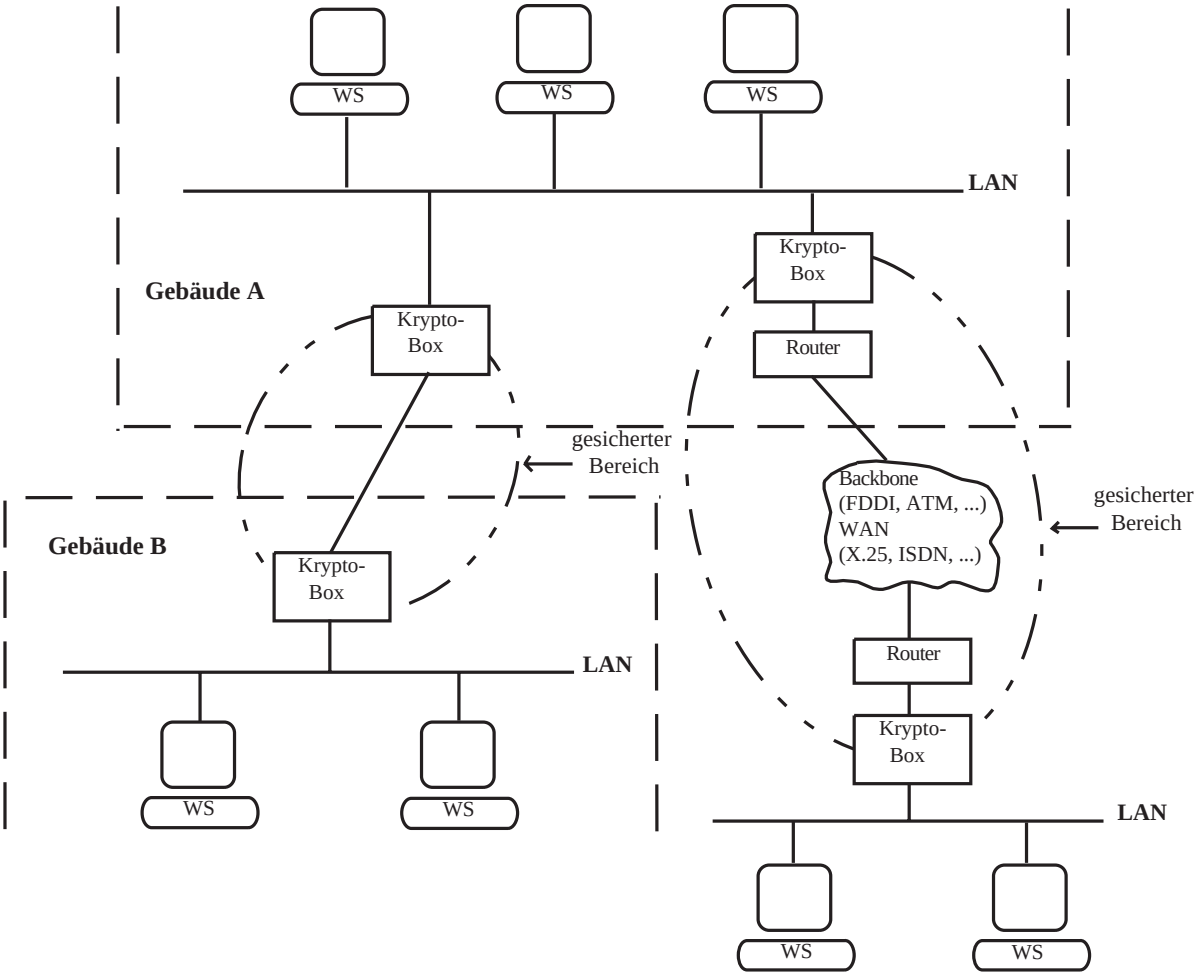


Abbildung 4.2: Gesicherte Kommunikation zwischen mehreren LAN-Segmenten über offene Netze

3. Aufbau einer gesicherten Kommunikation innerhalb eines Gesamtnetzes:

Durch die Kombination der in 1. und 2. beschriebenen Möglichkeiten können logische Teilnetze mit einem gewissen Maß an Sicherheit in einem Gesamtnetz erreicht werden. Dabei ist es auch möglich, mehrere logische Netze parallel oder geschachtelt zu betreiben. Eine Krypto-Box kann dann zu mehreren logischen Netzen gehören.

4.8 Einschränkungen und Voraussetzungen

Den obigen Ausführungen kann entnommen werden, dass die Standardisierung in vielen Bereichen noch nicht abgeschlossen ist, was zu einer Reihe von proprietären Lösungen geführt hat, die den Einsatz in einer heterogenen Umgebung praktisch unmöglich machen.

Die heute schon vorhandenen Lösungen stellen hohe Anforderungen an die Qualifikation des Netzbetreuungspersonals. Dasselbe ist auch von den in der Standardisierung befindlichen Ansätzen zu erwarten. Hinzu kommt, dass beim Betrieb von VLANs ein hoher administrativer Aufwand entsteht.

Die heutigen Hochschulnetze sind nicht flächendeckend für die dedizierte Anbindung von Endgeräten ausgelegt. Die Anbindung von nur einem Endgerät an einen Port einer Netzkomponente ist derzeit nur in Ausnahmefällen möglich.

4.9 Weitere Sicherheitsaspekte

Ein wichtiger Sicherheitsaspekt liegt bereits in der Natur der VLANs. Der Einsatz von VLAN-Techniken sorgt dafür, dass alle Daten, die für den internen Verkehr vorgesehen sind, innerhalb eines virtuellen Netzes bleiben. Schon alleine durch die Trennung des Datenverkehrs kann ein gewisses Maß an Abhörsicherheit in LANs erreicht werden. Die Daten können nur dann von nicht zu dem VLAN gehörenden Netzbenutzern empfangen werden, wenn sich mehrere virtuelle Netze auf einem physischen Netzsegment überlappen.

Daneben gibt es Bestrebungen, Firewall-Funktionalität in den Switches zu implementieren. So bietet z.B. die Firma Xylan eine switch-basierte Firewall an, bei der die Firewall-Technologie in die Routing-Funktionalität zwischen den VLANs integriert wird. Die Basis bildet die Software FireWall I von CheckPoint. Integrierte Firewall-Lösungen bieten außerdem eine höhere Flexibilität als physisch-basierte Firewalls.

Es sollte jedoch nicht übersehen werden, dass es nicht primäres Ziel der VLANs ist, Security-Mechanismen ins LAN zu integrieren.

4.10 Ausblick

Den virtuellen Netzen wird mit großer Wahrscheinlichkeit die Zukunft gehören, aber leider noch nicht die Gegenwart. Wichtig ist, dass man die aktuellen und die kommenden Entwicklungen genau beobachtet und sein Netz nach Möglichkeit so konzipiert, dass man sich hinsichtlich des Einsatzes und der Nutzung virtueller Netze möglichst viele Optionen offenhält. Dafür ist aber eine Weiterentwicklung der ab 1990 im Rahmen des NIP installierten Netzinfrastrukturen in den Hochschulen dringend erforderlich. Nach derzeitigem Stand basieren die vorhandenen Netzinfrastrukturen bei den Etagen- und Gebäudenetzen

noch vielfach auf Koaxialverkabelungen (10Base2 und 10Base5). Eine Weiterführung des Netzinvestitionsprogramms mit dem Ziel, eine sternförmige Verkabelung für dedizierte Anbindungen zu schaffen, ist dringend erforderlich. Eine strukturierte Verkabelung steht auch im Einklang mit den existierenden Planungshilfen und Planungsrichtlinien.

4.11 Empfehlungen zur Netzstruktur und zur Virtualisierung der Netze

- Die verschiedenen Server der Verwaltung bzw. Klinik sind möglichst in einem eigenen, von den Clients separierten, besonders gesicherten Subnetz zu konzentrieren und zu betreiben.
- Eine Kopplung von lokalen Netzen (LANs) über öffentliche oder auch private Netze sollte mit Hilfe logischer Kanäle (Tunnel) erfolgen. Mit zunehmender Verbreitung des IP Next Generation Protocol (IPng, IPv6) sollten die mit diesem Protokoll bereitgestellten Sicherheitsoptionen des Authentication Headers sowie des Encapsulating Security Payload Headers (ESP) konsequent für die Bildung und Absicherung solcher Tunnel eingesetzt werden.
- Für eine darüber hinaus besonders gesicherte Verbindung von Teilnetzen bzw. die gesicherte Anbindung einzelner PCs an ein Teilnetz über die grundsätzlich unsicheren Netzverbindungen des Hochschulnetzes oder des deutschen Wissenschaftsnetzes ist der dedizierte Einsatz von Krypto-Boxen vorzusehen, die den gesamten Datenverkehr zwischen den Teilnetzen bzw. zwischen dem Teilnetz und dem darin zu integrierenden PC verschlüsseln. Dabei ist Verfahren und Produkten der Vorrang zu geben, die eine nach heutigen Erkenntnissen ausreichende Kryptierungssicherheit bieten (anerkanntes Kryptierungsverfahren, hinreichend große Schlüssellänge) und darüber hinaus möglichst ein Sicherheitszertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) besitzen.
- Da die Standardisierung bei Techniken und Protokollen für virtuelle Netze (VLAN-Techniken) in vielen Bereichen noch nicht abgeschlossen ist, muss ihr Einsatz derzeit auf überschaubare und homogene Netzumgebungen beschränkt bleiben, in denen die spezifischen Anforderungen und Gegebenheiten (z.B. shared medium) berücksichtigt werden können.
- Um überhaupt die Voraussetzungen für den Einsatz von Switches und den Aufbau von virtuellen Netzen (VLANs) zu schaffen, muss der Ausbau einer strukturierten Verkabelung in den Hochschulen mit Nachdruck vorangetrieben werden. Da die Hochschulen mit der Finanzierung dieses Ausbaus der Netzinfrastruktur überfordert sein dürften, ist eine Weiterführung des Netzinvestitionsprogramms (NIP) dringend erforderlich.

4.12 Literatur

/Digital/ *„enVISN — das Architekturkonzept von Digital Equipment GmbH“*

/Eppele/ Eppele, K.:
„Virtuelle Netze“
`http://www.conware.de/Artikel`

/Fore/ *„LAN Emulation, Virtual LANs, and ATM Internetworks“*
`http://www.fore.com/atm-edu/whitep/lane.html`

/KryptG/ KryptoKom:
„KryptoGuard LAN und KryptoGuard PC: Innovatives Sicherheitssystem zum Schutz von modernen Kommunikationssystemen“

/KryptP/ KryptoKom:
„Unsere Produkte in der Übersicht“
`http://www.kryptokom.de/`

/PaFr/ Passmore, D. / Freeman, J.:
„The Virtual LAN Technology Report“
`http://www.3com.com/nsc/200374.html`

/RFC1483/ RFC 1483:
„Multiprotocol Encapsulation over ATM Adaptation Layer 5“
`http://sunsite.auc.dk/RFC/rfc/rfc1483.html`

/RFC1577/ RFC 1577:
„Classical IP and ARP over ATM“
`http://sunsite.auc.dk/RFC/rfc/rfc1577.html`

/Xylan/ Xylan:
„The Switching Book“
`http://www.xylan.com/sb/`

Kapitel 5

Netzabsicherung durch Firewalls

Es gibt bestimmte Punkte im Netz, an denen sinnvollerweise Maßnahmen zur Verbesserung der Sicherheit ansetzen sollten. Dies sind insbesondere die Übergänge zwischen (Teil-)Netzen mit unterschiedlichen Sicherheitsanforderungen (intern vs. extern; sicherer vs. unsicher). Durch geeignete Mechanismen können die Angriffsmöglichkeiten auf das Netz mit dem höheren Sicherheitsbedarf eingeschränkt werden. Das Konzept, welches sich dahinter verbirgt, ist unter dem Namen **Firewall** bekannt. Zu beachten ist dabei, dass die gewünschte Schutzwirkung nur dann gewährleistet ist, wenn jeglicher Datenverkehr zwischen den beteiligten Netzen über die Firewall geleitet wird.

5.1 Definition der Begriffe *Firewall, Gateway* und *Bastion*

Der Begriff Firewall wird nach /Ellermann94/ wie folgt definiert:

„Eine **Firewall** ist eine Schwelle zwischen zwei Netzen, die überwunden werden muss, um Systeme im jeweils anderen Netz zu erreichen. Es wird dafür gesorgt, dass jede Kommunikation zwischen den beiden Netzen über die Firewall geführt werden muss. Auf der Firewall sorgen Zugriffskontrolle und Auditing dafür, dass das Prinzip der geringsten Berechtigung durchgesetzt wird und potentielle Angriffe schnellstmöglich erkannt werden."

Das Prinzip der geringsten Berechtigung bedeutet hierbei, dass für jede nutzende Person bzw. Anwendung festgestellt wird, welche Berechtigungen für die Erfüllung der Aufgabe mindestens erforderlich sind. Genau diese Berechtigungen werden eingerichtet. Alle anderen Berechtigungen sind gesperrt (bzw. sind zu sperren). Darüber hinaus wird nach der Maxime verfahren „Es ist alles verboten, was nicht explizit zugelassen ist!".

5.1.1 Firewall-Architekturen

Eine Firewall kann in die Kommunikation auf verschiedenen Protokollschichten eingreifen. Für die einzelnen Protokollschichten, auf denen die Zugriffskontrolle und das Auditing angewendet werden, gibt es verschiedene Ausprägungen bzw. Architekturen von Firewalls.

In Abhängigkeit von der gewählten Architektur bzw. dem gewählten Ansatzpunkt besteht eine Firewall aus einer einzigen Komponente oder verbindet mehrere unterschiedliche Komponenten zu einem Gesamtsystem. Im Folgenden werden zunächst die beiden Komponenten **Packet-Screen** und **Application-Gateway** vorgestellt und anschließend Kombinationslösungen behandelt.

5.1.2 Packet-Screen

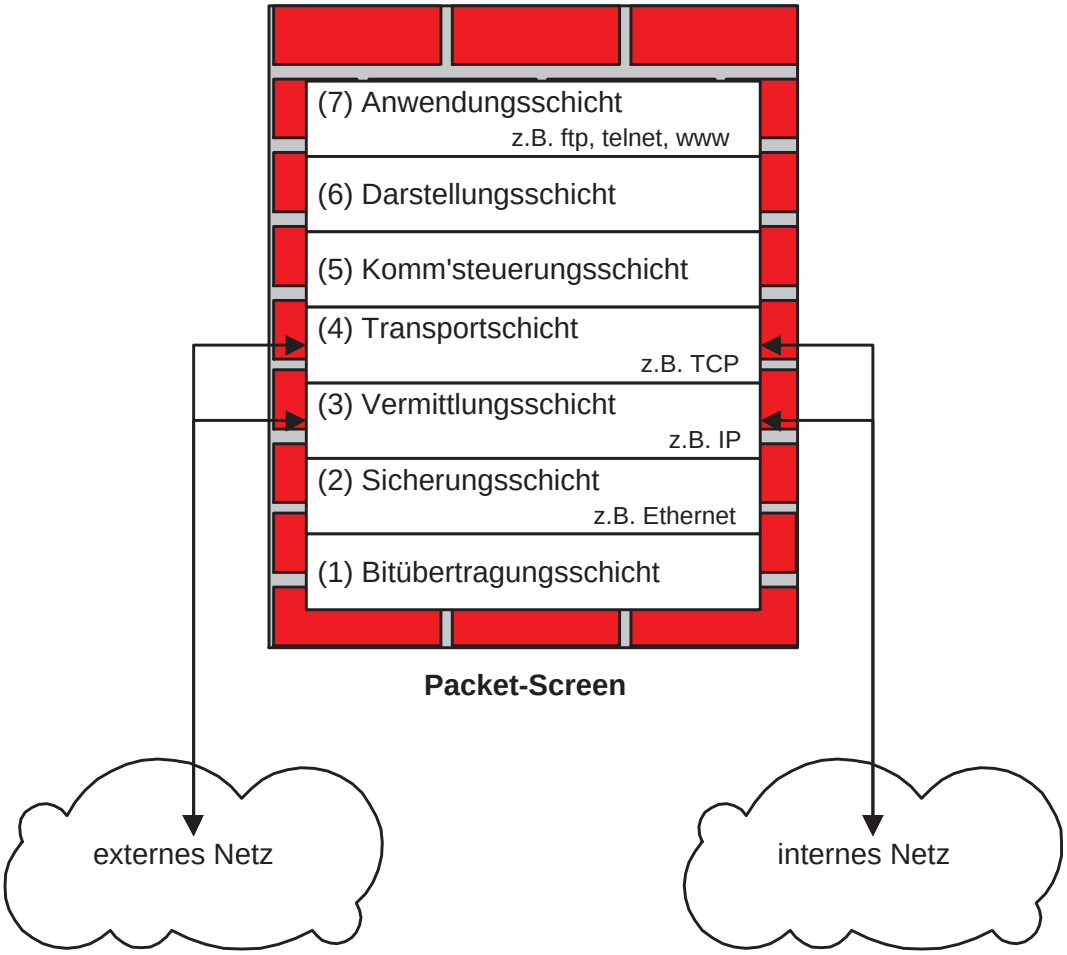


Abbildung 5.1: Darstellung einer Packet-Screen als Firewall

Eine **Packet-Screen**, auch unter der Bezeichnung *Screening-Router* bekannt, ist die einfachste Art einer Firewall. Sie arbeitet auf der Netzschicht (z.B. IP) bzw. auf der Transportschicht (z.B. TCP bzw. UDP). Dabei werden die in einem Datenpaket enthaltenen Informationen über Quelle und Ziel der Kommunikationsbeziehung (Adressen) sowie über den ausgewählten Kommunikationsdienst (Port) ausgewertet und für die Definition von Filtern benutzt. Bei der Definition der Filter können auch sog. Adressmasken benutzt werden, um mehrere Rechner bzw. ganze Netze in eine Regel zusammenzufassen. Bei TCP-basierten

Diensten kann das erste Paket, welches den Verbindungsaufbau initiiert, festgestellt werden. Als weitere Information kann die Lage der Quelle des Pakets (innen oder außen) ausgewertet werden.

Packet-Screens unterscheiden sich zum Teil im Hinblick auf die unterstützten Protokolle. Manche unterstützen nur das IP-Protokoll, welches auch die Grundlage des sog. Internet bildet. Die Wirkungsweise der Packet-Screen soll am Beispiel des IP-Protokolls vorgestellt werden.

Ein IP-Paket enthält folgende Adress- und Dienst-Informationen:

- IP-Quellenadresse z.B. 10.10.10.10
- IP-Zieladresse z.B. 192.168.0.5
- IP-Protokoll z.B. 6 (TCP) oder 1 (ICMP)
- Quellen-Port z.B. 7002 (unknown)
- Ziel-Port z.B. 25 (SMTP)
- ICMP-Nachrichtentyp z.B. 8 (Echo Reply)

Die Auswahl der Dienste erfolgt (u.a. beim IP-Protokoll-Stack für TCP bzw. UDP) über sogenannte Portnummern. Dabei sind einige dieser Portnummern bestimmten Diensten (Servern) zugeordnet; so bezeichnet z.B. Port 25 bei TCP den Transportdienst für Electronic Mail SMTP (Simple Mail Transfer Protocol). Diese Portnummern werden auch als „well-known ports“ bezeichnet. Demgegenüber erhalten die diese Dienste nutzenden Clients vom Betriebssystem meistens freie Portnummern zugewiesen, die im Allgemeinen aus dem Bereich >1024 stammen; diese Portnummern werden auch als „unknown ports“ bezeichnet. Allerdings ist nur bei Mehrbenutzersystemen (zumindest bei den meisten, wie z.B. UNIX) gewährleistet, dass ausschließlich Prozesse, die von *root* gestartet werden, diese „well-known ports“ (<1023) belegen können. Einzelplatzsysteme, die z.B. mit MS-DOS betrieben werden, können diese Unterscheidung nicht garantieren.

Aufgrund der großen Zahl an möglichen Diensten hat sich auch eine Methode etabliert, bei der Portnummern für Dienste dynamisch vergeben werden. Diese Dienste basieren auf dem Remote Procedure Call (RPC) und nutzen zur Verwaltung der Portnummern den Portmapper, der auf Port 111 residiert. Der Dienst ist auch unter dem Namen *rpcbind* bekannt. Hierzu registrieren sich die Dienste beim Start mit ihrer 4-Byte langen Funktions- sowie der Versionsnummer und geben die Portnummer mit, bei der sie auf Aufträge warten. Der Portmapper verwaltet nun die Tabelle der Dienste und gibt die Portinformation an anfragende Clients zurück. Neben dieser Aufgabe unterstützen einige Portmapper-Implementierungen auch eine Proxy-Funktionalität, bei der Anfragen vom Portmapper direkt an den gewünschten Dienst weitergegeben werden. Hierbei tritt zusätzlich das Problem auf, dass der Dienst annimmt, dass die Anfrage vom lokalen Rechner kommt.

RPC-basierte Standarddienste sind z.B. der Informationsdienst Yellow Pages (YP, NIS), der *mountd* zum Export von Dateisystemen, der *nfsd* zum Zugriff auf Dateien aus exportierten Dateisystemen und die Dienste *rusers* und *rstat*.

Bei der dynamischen Vergabe von Portnummern treten Schwierigkeiten bei der Filterdefinition auf, wenn die Packet-Screen keine Zusatzfunktionen für solche Dienste anbietet.

Es ist jedoch auch möglich, RPC-basierte Dienste an feste Portnummern zu binden (z.B. den *nfsd* auf Port 2049). Dies erlaubt wieder die Definition von passenden Filtern und ist als Maßnahme im Sicherheitskonzept für eigene bzw. eigenbeauftragte Programmentwicklungen für das eigene Netz festzulegen.

Einige Dienste vertrauen bei der Authentifizierung des Zugriffs auf die Angabe der Quellenadresse. Dies sind u.a. die sog. R-Dienste (*rlogin, rsh, rcp*). Eine besondere Sicherung der Quellenadresse existiert im IP-Protokoll nicht, die Quellenadresse ist also nicht vertrauenswürdig. Die Liste der erlaubten Adressen bzw. Nutzernamen ist auf dem Zielrechner in der Datei *.rhosts* im Home-Verzeichnis des Zielnutzers gespeichert. Sind diese Dienste nach außen verfügbar und gelingt es einem Angreifer, die Absenderadresse zu fälschen bzw. eine falsche Absenderadresse vorzugaukeln, kann ein unerlaubter Zugriff zum Zielsystem möglich sein. Diese Angriffe sind unter dem Namen **IP-Spoofing** bekannt. Sie werden zur Öffnung anderer Zugänge zum Zielsystem genutzt. Ein Schutz gegen IP-Spoofing von außen nach innen bzw. von innen nach außen kann durch die Prüfung des Adressbereichs am inneren bzw. äußeren Interface der Packet-Screen erreicht werden.

Eine Firewall hat bei der Absicherung des Netzübergangs auch die Aufgabe, internen Verkehr nicht nach außen dringen zu lassen. Hierbei spielen die Routingverfahren bzw. Mechanismen zur Änderung der Routingeinträge auf der Packet-Screen eine Rolle.

Router (die Packet-Screen ist meistens auch ein Router) entscheiden i. Allg. nur anhand der Zieladresse, an welche nächste Station ein Datenpaket weitergeleitet wird. Die Router besitzen dafür Routingtabellen, die über verschiedene Routingprotokolle dynamisch bzw. durch direkte Konfiguration der Wege statisch aufgebaut werden. Diese Routingtabellen werden bei entsprechender Konfiguration zwischen den Routern periodisch ausgetauscht. Um die Packet-Screen vor der Verwendung bzw. Weitergabe falscher Routingeinträge in das lokale Netz zu schützen, sollte kein dynamisches Routingprotokoll verwendet werden.

Darüber hinaus sind im IP-Protokollstack weitere Möglichkeiten vorgesehen, die Wegewahl zu beeinflussen. Zum einen können Router mit dem Nachrichtentyp *ICMP-Redirect* sendenden Stationen mitteilen, dass es bessere Wege als über sie selbst gibt, das Ziel zu erreichen (z.B. bei Vorhandensein mehrerer Router in einem Subnetz). In einem ICMP-Redirect-Paket steht nämlich die Adresse des Gerätes, über das das Ziel besser erreicht wird. Zum anderen kann einem IP-Paket die Option Source-Routing beigefügt werden, womit für dieses Paket anstatt der Routingtabellen der (im Paket selbst) vorgezeichnete Weg genutzt wird. Diese Option sollte ausgeschaltet sein. Erfolgreiche Angriffe auf die Wegewahl von Netzkomponenten ermöglichen dem Angreifer (möglicherweise unerkannt) ein Ablauschen von Verkehr über das Netz und bringen ihn dabei evtl. in den Besitz wertvoller Adress- oder Authentifizierungsinformationen bzw. vertraulicher Daten.

Die Filterregeln der Packet-Screen können je nach verwendetem Router statisch oder dynamisch, d.h. nach bestimmten Regeln während der Laufzeit selbstmodifizierend, sein. Über dynamische Filterregeln können z.B. variable Öffnungszeiten realisiert werden. Weiterhin können damit Dienste zugelassen werden, bei denen während des Datenaustausches der bzw. die zu nutzenden weiteren Ports vereinbart werden. Dies ist z.B. beim Dienst FTP der Fall, wobei die Verbindung vom Server mit dem Quellenport 20 und dem im vorherigen Paket (über die FTP-Kommandoverbindung) vereinbarten Zielport aufgebaut wird. Dynamische Filter bergen natürlich zusätzliche Gefahren für das Versagen der Filterregeln.

Bei den Filterregeln werden meistens Erlaubnis- (permit) und Verbotsregeln (deny) auftreten. Dann ist die Reihenfolge der Abarbeitung entscheidend für die Wirksamkeit.

Die erreichbare Performance der Packet-Screen wird außer durch den Umfang an vorgegebenen Filterregeln durch die Art und Weise beeinflusst, in der diese Filterregeln abgearbeitet werden. Hierbei existieren zwei unterschiedliche Vorgehensweisen:

- Die Filterregeln werden jedesmal der Reihe nach **interpretiert**.
- Die Filterregeln werden einmal **übersetzt** und anschließend direkt ausgeführt.

Die konkrete Ausprägung der Filterregeln bestimmt sich aus den Festlegungen der Sicherheitspolitik. Grundsätzlich sollte sie jedoch an der Maxime orientiert sein, dass **alles verboten ist, das nicht im Einzelnen explizit zugelassen ist.**

5.1.3 Application-Gateway

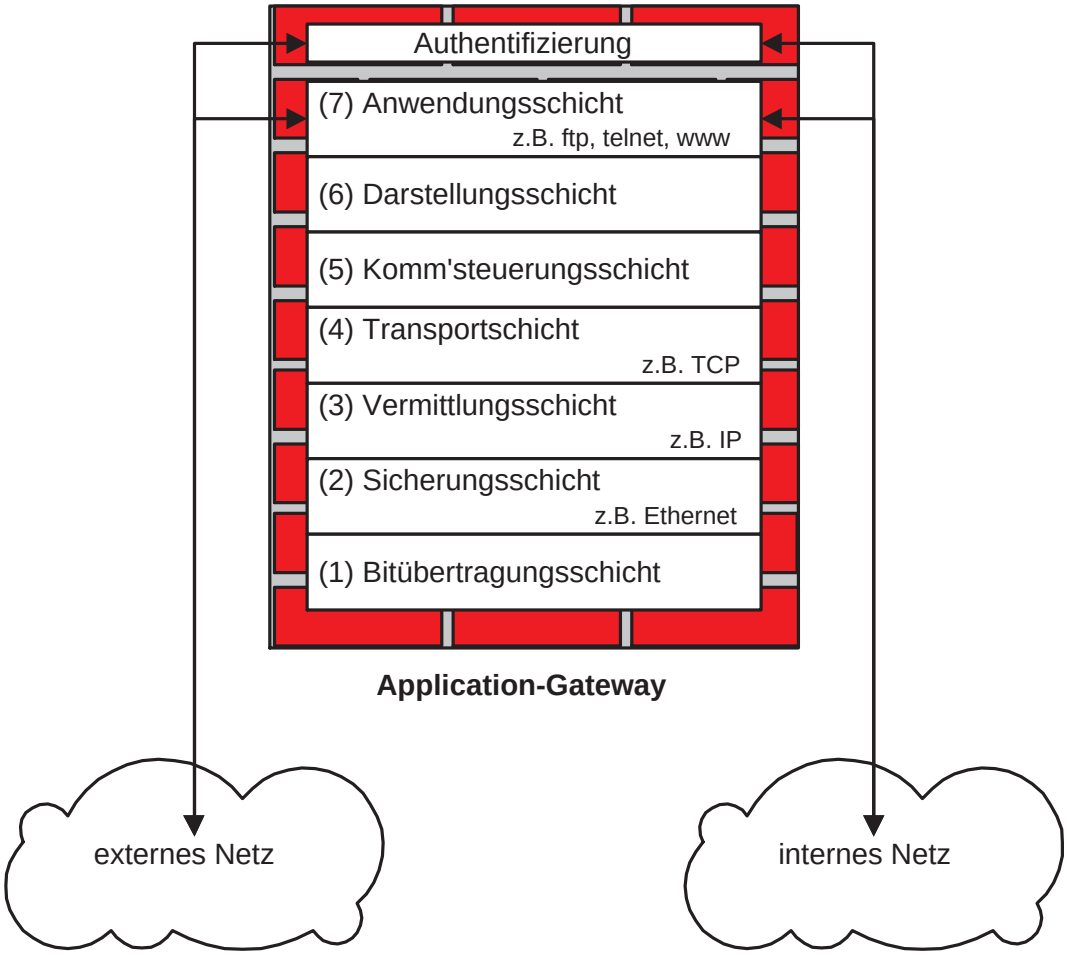


Abbildung 5.2: Darstellung eines Application-Gateway als Firewall

Bei einem **Application-Gateway** als alleiniger Firewall-Komponente handelt es sich um einen Rechner, der mit zwei getrennten Netz-Interfaces ausgestattet (dual-homed) als

Übergang zwischen die Netze geschaltet wird. Zur Überwindung des Gateways werden die Dienste auf der Anwendungsschicht abgearbeitet. Hierbei kann eine zusätzliche Authentifizierung bzw. anwendungsprotokollabhängige Filterung vorgenommen werden. Bei der Authentifizierung für die Überwindung der Firewall sollten strengere Mechanismen als normal üblich genutzt werden. Hierzu zählen u.a. Challenge-Response-Verfahren, Einmal- und zeitabhängige Passwörter. Diese Authentifizierungsmechanismen lassen sich selbst wieder mit unterschiedlichen Hilfsmitteln und Verfahren realisieren.

Der Übergang über das Application-Gateway erfolgt entweder über Proxy-Dienste oder alternativ über Benutzerberechtigungen auf der Firewall, wobei die Nutzung von Proxies eindeutig vorzuziehen ist. Unter einem Proxy-Dienst versteht man einen Dienst (nicht nur auf der Firewall), der als Vermittler Anforderungen von Clients entgegennimmt und (nach einer Prüfung) gegenüber dem eigentlichen Server wiederum als Client auftritt. Die Antworten des Servers werden dann entgegengenommen und an den anfragenden Client weitergegeben.

Welche Art Proxy eingesetzt wird bzw. werden kann, ist wiederum vom Dienst sowie von den Möglichkeiten auf der Clientseite abhängig. In einigen Fällen wird es zum Beispiel notwendig sein, die Clientsoftware zu modifizieren, um den Proxy-Einsatz überhaupt erst zu ermöglichen.

Bei Diensten, wie z.B. Electronic Mail oder NetNews, die nach dem Store-and-Forward-Mechanismus funktionieren, kann die Firewall die Nachrichten zwischenspeichern oder auch nur durchreichen. Werden die Nachrichten zwischengespeichert, so können anschließend Prüfmechanismen, wie z.B. eine Virenprüfung durchgeführt werden. Auf keinen Fall ist es sinnvoll, die interne Verteilung für solche Dienste auf der Firewall zu leisten. Ein erfolgreicher Einbruch auf der Firewall ermöglicht sofort den Zugriff auf interne vertrauliche bzw. sensitive Daten. Die internen Mail- und News-Server sollten sich im internen Netz befinden.

Für die gängigen Dienste wie z.B. *telnet, ftp, http* (WWW) bieten viele Hersteller von Application-Gateways Proxies an. Für andere, weniger verbreitete Dienste oder Dienste mit komplexerem Kommunikationsverhalten, wie z.B. *archie* oder *talk* sind keine bzw. kaum Proxies verfügbar.

Durch die alleinige Verbindung zwischen internem und externem Netz durch das Application-Gateway wird jeweils die interne Struktur des anderen Netzteils verborgen. Somit können im internen Netz auch Adressen genutzt werden, die im privaten Adressbereich nach RFC1918 liegen. Selbst die Verwendung von Adressen, die an andere Organisationen vergeben sind, ist möglich aber nicht unbedingt sinnvoll. Daraus folgt, dass es sinnvoll und notwendig ist, nach innen wie nach außen den Namensdienst mit unterschiedlichem Inhalt zu führen. Nach außen hin wird nur das Application-Gateway mit den angebotenen Diensten bzw. Aliasnamen bekanntgemacht.

Die anwendungsprotokollabhängige Filterung zeichnet sich gegenüber der Filterung auf der Netzschicht u.a. dadurch aus, dass einzelne Dienste in ihrem Funktionsumfang eingeschränkt werden können. So kann z.B. das Dienstangebot Filetransfer derart reduziert werden, dass nur der Transfer von Daten in das interne Netz erlaubt ist.

Implementierungen von Application-Gateways sind auf dem kommerziellen Markt von verschiedenen Herstellern erhältlich.

5.1.4 Packet-Screen mit Application-Gateway als Bastion

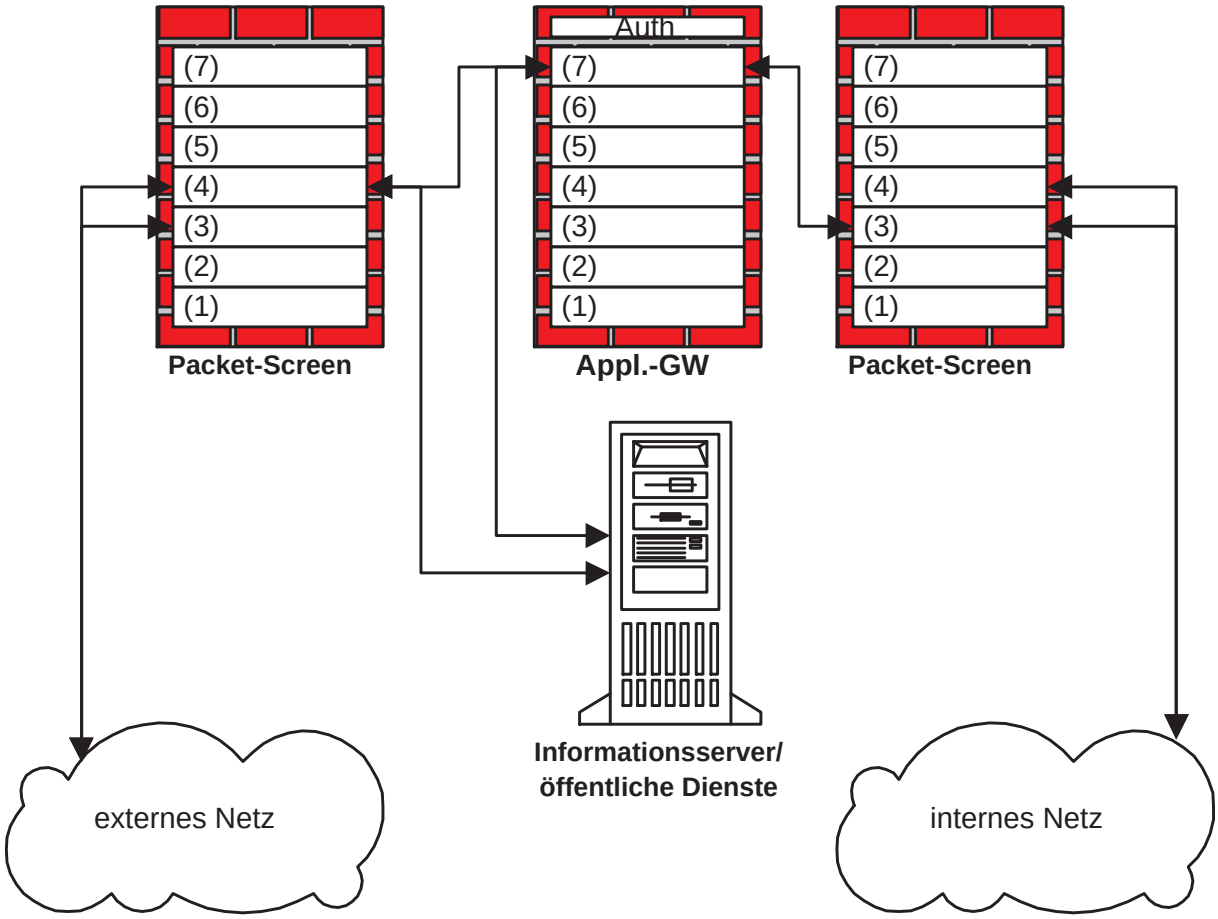


Abbildung 5.3: Darstellung der Kombinationslösung mit (teil-)geschütztem Informationsserver

Es existieren mehrere Kombinationslösungen von Packet-Screens mit Application-Gateways. In diesem Bericht wird die Kombination aus zwei Packet-Screens und einem dazwischenliegenden Application-Gateway, genannt Bastion, betrachtet. Die eine Packet-Screen wirkt gegenüber dem externen Netz, die andere gegenüber dem internen. Die dazwischenliegende Bastion kann auch aus mehreren über ein Netzsegment miteinander verbundenen Rechnern bestehen. In diesem Abschnitt werden die Unterschiede dieser Anordnung gegenüber dem Einsatz der Einzelkomponenten aufgezeigt.

Die beiden Packet-Screens schränken den Zugriff auf die Bastion ein und schützen sie somit vor (einigen) Angriffen. Weiterhin lassen die Packet-Screens keine direkte Verbindung zwischen dem externen und internen Netz zu.

Wie die Einzelkomponente Application-Gateway kann auch diese Bastion mit zwei Netz-Interfaces bestückt werden, so dass selbst bei kompromittierter Packet-Screen (innen wie außen) keine Dienste auf der Netzschicht die Firewall passieren können. Die Bastion kann als einziger Rechner mit beiden Netzen (intern und extern) kommunizieren. Da für die Bastion zwischen der Packet-Screen am externen Netz und der auch gegen Innentäter einsetzbaren Packet-Screen am internen Netz ein eigenes Subnetz geführt wird, können auf diesem (teilweise) abgesicherten, halbexternen Netz mehrere Server für den Zugriff von extern — wie z.B. Informationsserver (FTP, WWW) und ein Domain Name Server — eingesetzt werden. Diese Server können über die Packet-Screens geschützt werden, wenn nur die Dienste zugelassen werden, die diese Server anbieten sollen.

5.2 Bewertung der Firewall-Architekturen

5.2.1 Packet-Screen

Vorteile

- einfache Installation
- Transparenz für die Nutzer
- i. Allg. gute Performance

Nachteile

- weiterhin viele Rechner bedroht
- je nach Konfigurationsmöglichkeiten nicht alle gewünschten (notwendigen) Dienste durchführbar (ohne große Einbußen in der erreichbaren Sicherheit)
- keine benutzerbasierte Zugriffskontrolle
- ohne zusätzliche Hard- und Software keine genaue Übersicht über die Nutzung des Übergangs
- kein zentrales Audit aller genutzten Dienste (mit Parametern)

Abwehrbare Bedrohungen (Beispiele)

- Unsichere Dienste können an der Packet-Screen abgestellt werden, d.h. Angriffe auf nicht angebotene Dienste werden abgefangen.
- Bestimmte Ziele (intern) können vom externen Datenverkehr ausgeschlossen werden.
- IP-Spoofing ist abwehrbar, wenn Pakete mit interner Adresse von außen bzw. mit externer Adresse von innen kommen.

Weiterhin existierende Bedrohungen (Beispiele)

- Eine Entscheidung über die Zulassung ist nur anhand der Portnummer möglich, d.h. unerwünschte bzw. unerlaubte Dienste können auf erlaubten Ports angeboten werden.

- Interne Ziele können bei Nutzung von erlaubten Verbindungen zu anderen (internen) Systemen im internen Netz über einen Umweg weiterhin erreichbar sein.
- Es ist keine Einschränkung der Dienste z.B. für Datenexport möglich.

5.2.2 Application-Gateway

Vorteile

- benutzerabhängige Zugriffskontrolle möglich
- gutes Audit (alle Dienste zwischen den Netzen)
- die interne (Netz-)Struktur wird verborgen

Nachteile

- Die Performance stellt bei größeren Netzen einen Engpass dar.
- Es ist nicht erweiterbar, da Direktanschluss an das externe Netz.
- Es ist kein eigener Diensteserver außerhalb des geschützten Netzes möglich.

Realisierung durch Benutzerberechtigungen auf der Firewall

zusätzliche Vorteile:

- einfache Installation (Standardnutzereintragung)
- zusätzliche Dienste anbietbar (z.B. talk)

zusätzliche Nachteile:

- umständliche Bedienung:
  1. Login auf dem Application-Gateway notwendig
  2. eigentlicher Verbindungsaufbau erst nach erfolgreichem Login
  3. Daten zum Export bzw. Import müssen auf der Firewall zwischengelagert werden.
- umständliche Administration
- Sicherheit schwer zu gewährleisten

Realisierung mit Proxies

zusätzliche Vorteile:

- einfache Bedienung
- Transparenz
- hohe Sicherheit
- sehr gute Konfigurationsmöglichkeiten

zusätzliche Nachteile:

- evtl. geänderte Clientprogramme erforderlich
- hoher Administrationsaufwand bei Wandel von Diensten: neue Dienste bzw. neue Features der Dienste erfordern neue Proxy-Programme

Abwehrbare Bedrohungen (Beispiele)

- Unsichere Dienste können am Application-Gateway abgestellt werden, d.h. Angriffe auf nicht angebotene Dienste werden abgefangen.
- Ein ungewünschter Datentransport z.B. Datenimport via Filetransfer kann unterbunden werden.

Weiterhin existierende Bedrohungen (Beispiele)

- Fehler in der Dienstespezifikation
- Ausnutzung von Insiderwissen (z.B. Authentifizierungsinformation für den Übergang)

5.2.3 Packet-Screen mit Bastion

Vorteile

- wie beim Application-Gateway
- zusätzlich ein oder mehrere (Info)-Server außerhalb des geschützten Netzes im teilgeschützten Bereich möglich
- Bastion von innen und außen durch Packet-Screen schützbar
- mehrfache Absicherung mit unterschiedlichen Filtertechnologien

Nachteile

- Performance durch Application-Gateway bestimmt
- kostenaufwendiger
- aufwendigere Konfiguration gegenüber dem Betrieb einer einzelnen Komponente

Abwehrbare Bedrohungen (Beispiele)

- wie bei Packet-Screen und Application-Gateway

Weiterhin existierende Bedrohungen (Beispiele)

- Fehler in der Dienstespezifikation
- Ausnutzung von Insiderwissen (z.B. Authentifizierungsinformation für den Übergang)

Zusammenfassend lässt sich also feststellen, dass die Kombination von Packet-Screen und Bastion bei einem angemessenen Sicherheitskonzept die beste (erzielbare) Sicherheit ergibt. Natürlich ist klar, dass auch durch eine solche Firewall nur das dahinterliegende

Sicherheitskonzept durchgesetzt werden kann. Lücken in diesem Konzept bewirken dann auch (meistens) Schwächen in der Wirksamkeit der Firewall.

5.3 Grenzen des Firewallkonzepts

Firewalls dienen der Abschottung von Netzen am Netzübergang. Somit kann insbesondere die Insiderproblematik, also Angriffe aus dem eigenen Netz, nicht gelöst werden. Weiter existieren natürlich Gefahren bzw. Angriffsmöglichkeiten, die in den weiterhin „bewusst“ erlaubten Diensten liegen. Gefahren bzgl. bestimmter Dienste können nur durch Verbot bzw. Einschränkung der Dienste gemindert bzw. ausgeschlossen werden. Auch kann die Firewall keine Vorkehrungen gegen fehlendes Sicherheitsbewusstsein bzw. Fehler der nutzenden Personen treffen. Solche Probleme können z.B. allein schon durch die falsche Adressierung eines elektronischen Briefes entstehen.

5.4 Konfiguration und Betrieb einer Firewall

Eine Firewall enthält sensible Daten bzw. ist aufgrund ihrer Sammelfunktion als Angriffsziel interessant. Neben dem Schutz der Firewall vor möglichen Angriffen aus dem Netz ist daher die Aufstellung an einem abgesicherten Standort (Zugang, Zugriff) selbstverständlich.

Die Firewall sollte derart konfiguriert bzw. konfigurierbar sein, dass der Ausfall einer Komponente (höchstens) bewirkt, dass kein Datenverkehr mehr möglich ist. Keinesfalls darf der Ausfall einer Firewall-Komponente das Außerkraftsetzen der Firewall-Funktionalität bewirken.

Die Konfiguration einer Firewall muss sich quasi aus dem Sicherheitskonzept ableiten lassen. Hierbei steht immer die Entscheidung an, nach welchen Kriterien die Zugriffskontrolle durchgeführt wird.

Die beiden gegensätzlichen Ansätze sind:

- Prinzipiell ist **alles verboten**. Nur gewünschte Kommunikationsbeziehungen und Dienste werden erlaubt.
- Prinzipiell ist **alles erlaubt**. Nur unerwünschte Kommunikationsbeziehungen und nicht gewünschte bzw. verwundbare Dienste werden verboten.

Dem ersten Ansatz ist dabei wegen der geringeren Gefahr, unbeabsichtigt Sicherheitslöcher aufzureißen, grundsätzlich der Vorzug zu geben.

Zur Konfiguration gehört die Einstellung der Alarmierungs- bzw. Auditmechanismen. Auch hierzu sollten Vorgaben im Sicherheitskonzept enthalten sein. Insbesondere muss ein Verfahren definiert sein, wie im Betrieb die anfallenden Alarmmeldungen bzw. Auditinformationen rechtzeitig und kontinuierlich auszuwerten sind. Hierbei ist es auch möglich, aus

den Auditinformationen Hinweise zu finden, wie die Sicherheitspolitik sinnvoll modifiziert werden kann.

Eine weitere permanente Tätigkeit, die normalerweise automatisiert durchgeführt werden kann, ist die Prüfung der Integrität der Firewall-Konfiguration. Es ist jedoch neben dem Automatismus (z.B. über die Bildung von Prüfsummen, die durch das Werkzeug *tripwire* durchgeführt werden kann) eine unregelmäßige manuelle Prüfung vorzusehen.

Der Einsatz einer Firewall hat auch Auswirkungen auf Dienste, die intern wie extern bereitgestellt werden. Die notwendige und sinnvolle Konfiguration der Dienstinfrastruktur muss deshalb gegebenenfalls modifiziert werden, wie im Folgenden am Beispiel Electronic Mail dargestellt wird. Der Dienst bzw. die beteiligten Server und der (interne wie externe) Namensdienst sind so zu konfigurieren, dass sämtliche Post von internen Clients an den internen Mailrelay versandt wird. Dieser sorgt für die Zustellung bzw. Verteilung im internen Bereich. Sämtliche Post, die für externe Nutzer bestimmt ist, wird zur Firewall bzw. zur Komponente Application-Gateway weitergereicht, die wiederum die Verteilung im externen Netz vornimmt. Für die hereinkommende Post sieht der Weg folgendermaßen aus: Die Post wird vom Application-Gateway der Firewall entgegengenommen und anschließend (nach Prüfung) an den internen Mailrelay weitergegeben. Dieser sorgt wie im internen Fall für die Zustellung bzw. Verteilung.

Solche bzw. ähnliche Konfigurationsüberlegungen sind für die einzelnen anzubietenden Dienste durchzuführen und sollten im Sicherheitskonzept festgehalten sein.

Beim Einsatz einer Firewall muss klar sein, dass im Falle eines Falles auch die Abschaltung der Firewall bzw. die Trennung des Netzübergangs notwendig werden kann. Das Personal, welches die Firewall betreibt, muss demnach entsprechende Rechte besitzen und auch die Zeit haben, die anfallenden Daten auszuwerten und die Konfiguration bei vorheriger Änderung des Sicherheitskonzepts bzw. zur Behebung eines Konfigurationsfehlers unverzüglich anzupassen. Eine restriktive Anwendung des Sicherheitskonzepts muss u.U. ohne vorherige Änderung der Sicherheitspolitik möglich sein.

5.5 Empfehlungen zur Netzabsicherung durch Firewalls

- An Übergängen zwischen (Teil-)Netzen mit unterschiedlichen Sicherheitsanforderungen sollte eine Firewall eingesetzt werden, um die Angriffsmöglichkeiten auf das Netz mit dem höheren Sicherheitsbedarf einzuschränken. Allerdings hängt die Wirksamkeit dieser Maßnahme essentiell davon ab, dass jegliche Kommunikation zwischen den beiden Netzen ausschließlich über die Firewall geführt wird.
- Insbesondere zur Absicherung des Subnetzes der Verwaltungs- bzw. Klinik-Server ist eine Firewall grundsätzlich vorzusehen.
- Trotz eines höheren Kosten-, Konfigurations- und Administrierungsaufwands ist einer aus Packet-Screens und einem Application-Gateway (Bastion) im Screened Subnet bestehenden Firewall-Lösung (siehe 5.1.4) der Vorzug zu geben. Wenn es die

zu erreichende Sicherheitsstufe erfordert bzw. die finanziellen Rahmenbedingungen ermöglichen, sollte man dabei auf ein durch das BSI zertifiziertes Firewall-System (siehe 12.3) zurückgreifen.

- Die permanente Überwachung und Fortschreibung der Konfiguration des Firewall-Systems ist erforderlich.
- Die Firewall sollte nach dem Prinzip konfiguriert sein, dass grundsätzlich aller Datenverkehr verboten ist und nur gewünschte Kommunikationsbeziehungen und Dienste explizit freigegeben werden. Dabei darf der Ausfall einer Firewall-Komponente keinesfalls die Wirksamkeit der Firewall-Funktionen außer Kraft setzen, sondern allenfalls dazu führen, dass kein Datenverkehr mehr möglich ist.
- Da eine Evaluierung verschiedener Firewall-Systeme im Rahmen der Kommissionsarbeit nicht möglich war, wird die Durchführung eines Pilotprojekts unter Einbeziehung der Ansätze des Projekts BASILIKA und der Untersuchungen der Arbeitsgruppe nordrhein-westfälischer Hochschulverwaltungen /NRW96/ empfohlen. Zur Erzielung von Synergieeffekten ist eine einheitliche Lösung anzustreben.

5.6 Literatur

/BSI95/ Bundesamt für Sicherheit in der Informationstechnik:
„Internet-Firewalls: Anbindung von Sicherheitsbereichen an das Internet“,
November 1995

/BSI96/ Bundesamt für Sicherheit in der Informationstechnik:
„Sicherheitsanforderungen an Internet-Firewalls“,
Januar 1996

/Chapman95/ Chapman, D.B. / Zwicky, E.D.:
„Building Internet Firewalls“,
O’Reilly, 1995

/Cheswick96/ Cheswick, W.R. / Bellovin, St.M.:
„Firewalls und Sicherheit im Internet“,
Addison-Wesley, Bonn 1996

/DFN-CERT/ WWW-Server des DFN-CERT
`http://www.cert.dfn.de/`

/Ellermann94/ Ellermann, U.:
Firewalls, Klassifikation und Bewertung
in: *„Sicherheit in vernetzten Systemen, Workshop des Projekts CERT im DFN“,*
März 1994, Hamburg

/Gaissmaier95/ Gaissmaier, K.:
„Implementierung eines Firewalls unter Verwendung frei verfügbarer Software“,
Ulm, März 1995
`http://www.uni-ulm.de/~gaissmai/`

/LANline97/ Meuser, P.:
„Firewall-Testserie im LANline-Lab (1)–(7)“,
LANline 1997/98

/NRW96/ Hochschulverwaltungen NRW:
„Bericht der Arbeitsgruppe Firewalls und Netzsicherheit der NRW-Hochschulverwaltungen“,
August 1996

/Pohlmann97/ Pohlmann, N.:
„Firewall-Systeme, Sicherheit für Internet und Intranet“
International Thompson Publishing, 1997

Kapitel 6

Verschlüsselung vertraulicher und sensibler Daten

6.1 Übersicht

Verschlüsselungsverfahren werden als Beitrag zur Gewährleistung der Vertraulichkeit, Authentizität, Integrität und Verbindlichkeit von Daten eingesetzt. Hierbei werden u.a. (logisch) private Kommunikationswege zwischen Kommunikationspartnern realisiert und dabei die Informationen vor unbefugtem Zugriff und Verfälschung geschützt. In diesem Kapitel werden die Grundlagen der Verschlüsselung und deren Anwendungsmöglichkeiten vorgestellt. Im Einzelnen werden

- die unterschiedlichen Verschlüsselungsverfahren und deren Einsatzmöglichkeiten vorgestellt,
- die Methoden erläutert, die zur Behandlung der dafür erforderlichen Schlüssel notwendig sind,
- Möglichkeiten und Rahmenbedingungen für die Nutzung der Verschlüsselung zur Erstellung einer digitalen Signatur bzw. Unterschrift dargelegt und
- die Problematik des sog. Verschlüsselungsverbots und des „key recovery“ behandelt.

6.2 Einsatzszenarien

Verschlüsselungsverfahren sind beim täglichen Umgang mit EDV-Systemen vielfach im Einsatz, auch ohne dass dies die nutzenden Personen bemerken. Die hierzu verwendeten Verschlüsselungsverfahren werden sowohl bei der lokalen Datenspeicherung als auch bei der Datenübertragung eingesetzt, wobei insbesondere dort verschiedenste Ansatzpunkte für den Einsatz dieser Maßnahmen existieren. Sind diese für den Nutzer nicht sichtbar bzw. erkennbar, spricht man von „transparenten“ Verfahren.

Bereits beim lokalen Einsatz gibt es für Verschlüsselungsverfahren ein breites Anwendungsspektrum:

- verschlüsselt gespeicherte Passwörter dienen der Prüfung für die Zugangsberechtigung zum System (Authentifizierung),
- Verschlüsselung des kompletten Inhalts lokaler Festplatten (z.B. bei Laptops) und Disketten sowie einzelner Dateien bzw. bestimmter Daten in Dateien dient der Gewährleistung der Vertraulichkeit,
- Speicherung verschlüsselter Prüfsummen für einzelne Dateien ermöglicht es, die Integrität der gespeicherten Daten bzw. Programme zu prüfen.

Bei der Übertragung von Daten kommt das Zusammenspiel verschiedener Partner (Menschen/Dienste/Rechner) hinzu. Auch hierbei gibt es die verschiedensten Einsatzmöglichkeiten und entsprechende Produkte:

- Sicherung der Authentizität z.B. durch
  - Übertragung verschlüsselter Passwörter bzw. Daten (z.B. bei Novell NETWARE, bei Challenge-Response-Verfahren),
  - gegenseitige Authentifizierung von Client und Server (z.B. durch Kerberos);
- Sicherung der Vertraulichkeit z.B. durch
  - Verschlüsselung von Dialogverbindungen (z.B. Kerberos, Secure Shell (SSH)),
  - Tunnelung von X.11-Verkehr über verschlüsselte Kanäle (z.B. SSH),
  - Austausch von verschlüsselten Zahlungsinformationen beim Electronic Commerce (z.B. Secure Sockets Layer (SSL), Secure-HTTP (S-HTTP)),
  - verschlüsselte Übertragung von Dokumenten z.B. elektronischer Post (z.B. Pretty Good Privacy (PGP), Privacy Enhanced Mail (PEM));
- Sicherung der Integrität bzw. Verbindlichkeit z.B. durch
  - Übermittlung von Signaturen, d.h. verschlüsselter Prüfsummen für Dokumente bzw. Programme (Integrität (z.B. *tripwire*)),
  - Übermittlung von (nachweisbar von einem bestimmten Urheber erzeugten) Signaturen, d.h. verschlüsselter Prüfsummen für Dokumente (Integrität und Verbindlichkeit (z.B. PGP, PEM, . . .)).

6.3 Verschlüsselungsverfahren

Verschlüsselungsverfahren beruhen auf der mathematischen Eigenschaft, Daten (genannt Klartext) durch eine Transformation (mittels eines Schlüssels) so zu verändern, dass ohne Kenntnis des Verfahrens und des Schlüssels keine (besser gesagt, eine nur mit unverhältnismäßig hohem Einsatz von Rechenleistung und Rechenzeit durchführbare) Rekonstruktion des Klartexts möglich ist. Die verschlüsselten Daten werden „Chiffrat“ genannt. Mit einer weiteren Transformation (mittels des gleichen oder eines weiteren Schlüssels) werden die Originaldaten wiederhergestellt (entschlüsselt). Werden beide Transformationen mit dem

gleichen Schlüssel durchgeführt, so wird von **symmetrischer Verschlüsselung** gesprochen, anderenfalls von **asymmetrischer Verschlüsselung**. Für jede der beiden Klassen gibt es verschiedene Verfahren und Anwendungsgebiete.

Die einzelnen Verschlüsselungsverfahren unterscheiden sich durch den verwendeten Algorithmus sowie die genutzte Schlüssellänge.

Die „Stärke“ eines Verschlüsselungssystems hängt von mehreren Faktoren ab. Dies sind u.a.:

- Chiffriersicherheit,
- Schlüsselmanagement bzw. Verfahren zur Geheimhaltung der Schlüssel,
- Unterbindung verdeckter Kanäle,
- Fehlfunktions- bzw. Fehlbedienungssicherheit,
- Manipulationssicherheit.

Unter Chiffriersicherheit werden die mathematischen Eigenschaften verstanden, die es (beliebig) schwer machen, aus dem Wissen von Klartexten und dem dazugehörigen Chiffrat den bzw. die verwendeten Schlüssel zu erraten oder zu erzeugen. Bei asymmetrischen Verfahren soll auch aus der Kenntnis von Klartext, Chiffrat und einem der beiden zusammengehörigen Schlüssel der andere Schlüssel (beliebig) schwer herauszufinden sein.

Das Vorliegen eines verdeckten Kanals bedeutet, dass die Information für bestimmte (verdeckte) Adressaten leicht erkennbar ist. Dies kann z.B. dadurch geschehen, dass der Klartext mit einem anderen (dem verdeckten Empfänger bekannten) Schlüssel verschlüsselt zusätzlich abgelegt ist, der Schlüssel in einer dem verdeckten Adressaten bekannten Form im Chiffrat abgelegt ist oder der Empfänger ein anderes Verfahren kennt, mit dem der Klartext mit einem einfacheren Schlüssel (der nicht notwendigerweise bekannt sein muss) wiederhergestellt werden kann.

Unter den Begriff Schlüsselmanagement fallen die Verfahren zur Speicherung und Verteilung der Schlüssel. Auf diesen Aspekt wird in Abschnitt 6.4 weiter eingegangen.

Für das Brechen der Verschlüsselung („Kryptanalyse“) gibt es zwei prinzipiell verschiedene Wege:

1. Der für die Entschlüsselung notwendige Schlüssel wird unter Nutzung der bekannten mathematischen Eigenschaften des Verfahrens und bekannter Teile der verschlüsselten Information (z.B. Chiffrat und öffentlicher Schlüssel) berechnet. („Reverse Engineering“)
2. Der Schlüssel wird durch Ausprobieren aller möglichen Werte herausgefunden. („Brute-Force-Attack“)

Der Aufwand für beide Verfahren hängt wesentlich von der Länge des genutzten Schlüssels ab. Sie ist somit auch ein entscheidendes Kriterium für die Chiffriersicherheit.

Einige Hersteller von Verschlüsselungsverfahren bzw. -komponenten halten das genutzte Verfahren bzw. die Designkriterien (auch gegenüber dem autorisierten Nutzer) geheim. Dies hat zwei Implikationen:

1. Das Reverse Engineering kann nur eingeschränkt durchgeführt werden, da Informationen über das Verfahren (möglicherweise) nicht bekannt sind.
2. Die Chiffriersicherheit des Verfahrens kann (z.B. auf Veranlassung des Nutzers) nicht unabhängig geprüft werden.

6.3.1 Symmetrische Verschlüsselungsverfahren

Bei der symmetrischen Verschlüsselung wird ein geheimer Schlüssel verwendet. Je zwei Kommunikationspartner A und B, die verschlüsselte Nachrichten austauschen wollen, müssen denselben Schlüssel $K_{A,B}$ kennen. Man benötigt also eine sichere Methode, um Schlüssel zwischen den Kommunikationspartnern auszutauschen. Im Extremfall bedeutet dies das Überbringen durch einen Kurier, wenn im Netz selbst keine sichere Schlüsselverteilung möglich ist.

Heutzutage verwendete symmetrische Verschlüsselungsverfahren sind z.B. DES (Data Encryption Standard) und IDEA (International Data Encryption Algorithm).

DES benutzt eine Schlüssellänge von 56 Bit und verschlüsselt Blöcke zu je 64 Bit. Die Verschlüsselung kann in verschiedenen Modi (u.a. auch rückgekoppelt) benutzt werden. Bei der Rückkopplung wird das Chiffrat des vorherigen Durchlaufs in die Berechnung des neuen Schlüssels einbezogen. Dadurch wird bei der Verschlüsselung gleicher Blöcke nicht immer das gleiche Chiffrat erzeugt und somit die unbefugte Entschlüsselung weiter erschwert.

Der IDEA-Algorithmus verwendet Schlüssel mit einer Länge von 128 Bit.

Als Beispiel für ein schwaches symmetrisches Verschlüsselungsverfahren sei hier der ROT13-Algorithmus aufgeführt. Dieses Verfahren arbeitet auf Basis des Alphabets. Jeder Buchstabe wird durch seinen 13. Nachfolger ersetzt. Das Wort „HALLO“ wird zum Wort „UNYYB“ chiffriert und wieder zu „HALLO“ entschlüsselt.

Wird eine Information mehrfach mit dem gleichen symmetrischen Schlüssel chiffriert, ist es potentiellen Angreifern leichter, die Information zu entschlüsseln.

Die folgende Abbildung 6.1 stellt den Prozess der symmetrischen Verschlüsselung dar.

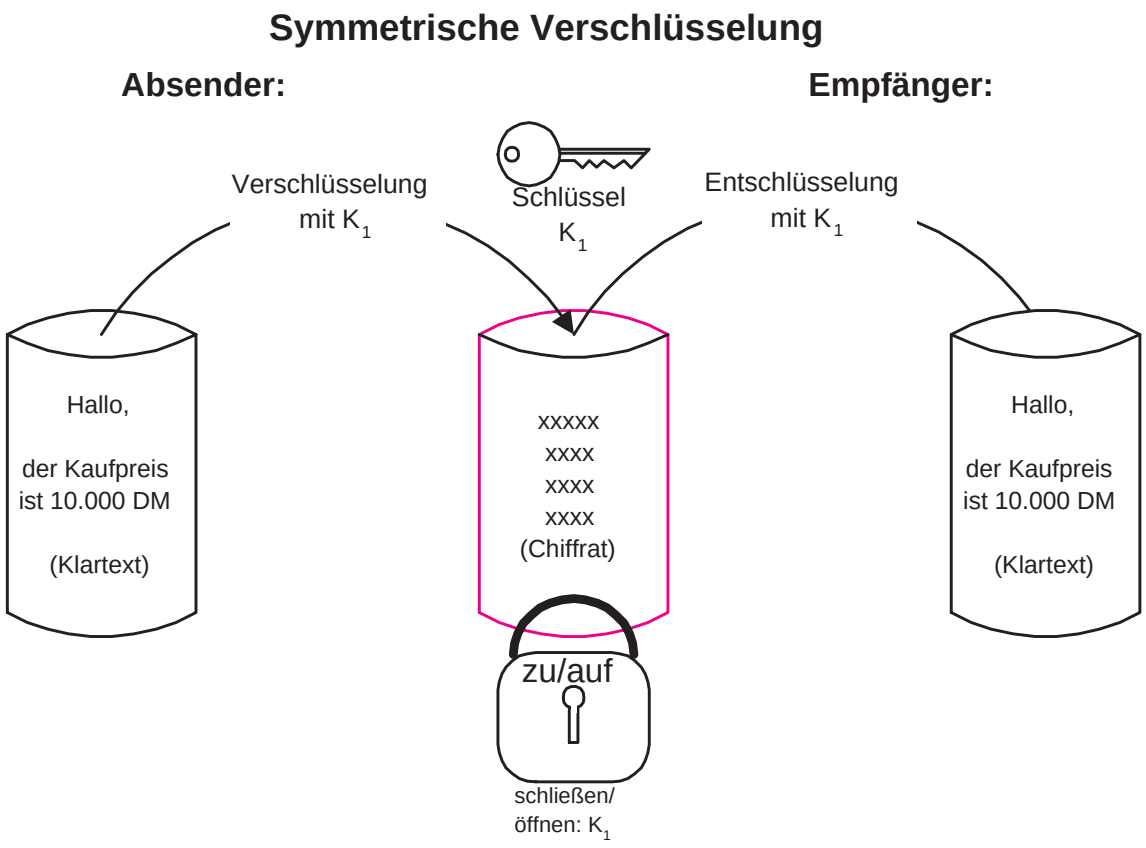


Abbildung 6.1: Symmetrische Verschlüsselung

6.3.2 Asymmetrische Verschlüsselungsverfahren

Asymmetrische Verfahren verwenden für die Ver- und Entschlüsselung unterschiedliche Schlüssel. Diese müssen folgenden Kriterien entsprechen:

- Der Entschlüsselungs-Schlüssel ist praktisch nicht aus dem Verschlüsselungs-Schlüssel ableitbar.
- Die Verschlüsselung kann nicht gebrochen werden, selbst wenn eine Nachricht gleichzeitig im Klartext und verschlüsselt vorliegt.

Unter den oben genannten Annahmen gibt es keinen Grund, den Verschlüsselungs-Schlüssel geheimzuhalten. Er wird „öffentlicher Schlüssel“ (Public Key) und der Entschlüsselungs-Schlüssel „geheimer Schlüssel“ (Private Key) genannt. Jeder Kommunikationsteilnehmer gibt seinen öffentlichen Schlüssel bekannt.

Der Informationsaustausch zwischen zwei Partnern A und B läuft dabei in den folgenden Schritten ab:

1. Absender A holt sich den öffentlichen Schlüssel K_B des Empfängers B.
2. Absender A verschlüsselt die zu übermittelnde Nachricht mit diesem Schlüssel.
3. Die verschlüsselte Nachricht wird dem Empfänger zugänglich gemacht.
4. Der Empfänger B benutzt seinen eigenen geheimen Schlüssel PK_B und entschlüsselt die Nachricht.

Da nur der Teilnehmer B den geheimen Schlüssel PK_B kennt, ist er der einzige, der diese mit dem öffentlichen Schlüssel K_B verschlüsselte Nachricht entschlüsseln kann. Der private Schlüssel PK_B ist weder aus dem öffentlichen Schlüssel K_B noch aus der verschlüsselten Nachricht bestimmbar.

Ausgehend von diesen prinzipiellen Überlegungen wurden verschiedene asymmetrische Verschlüsselungsverfahren, auch Public-Key-Verfahren genannt, vorgeschlagen. Vertreter dieser Klasse sind z.B. das Diffie-Hellman-Verfahren und das RSA-Verfahren (benannt nach seinen Erfindern Rivest, Shamir und Adleman).

Zur Zeit werden bei asymmetrischen Verschlüsselungsverfahren Schlüssellängen zwischen 512 und 1024 Bit verwendet. Nach heutigem Kenntnisstand wird jedoch die Verwendung von Schlüsseln mit einer Schlüssellänge von mindestens 2048 Bit empfohlen.

Im Gegensatz zu den symmetrischen Verfahren kann und muss ein Schlüssel (des Schlüsselpaares) öffentlich verbreitet werden. Die Problematik der Verteilung über einen vertrauenswürdigen Kanal stellt sich also nicht. Dafür stellt sich hier dennoch das Problem der Schlüsselvalidierung. Es gilt zu prüfen, ob der angebotene öffentliche Schlüssel einer Person / eines Dienstes auch tatsächlich zu dieser Person / diesem Dienst gehört. Zusätzlich ist es wichtig zu erfahren, ob dieser kompromittiert ist, d.h. die Geheimhaltung des diesem öffentlichen Schlüssel zugeordneten privaten Schlüssels nicht mehr sichergestellt ist.

Das Verfahren ist in der folgenden Abbildung 6.2 dargestellt.

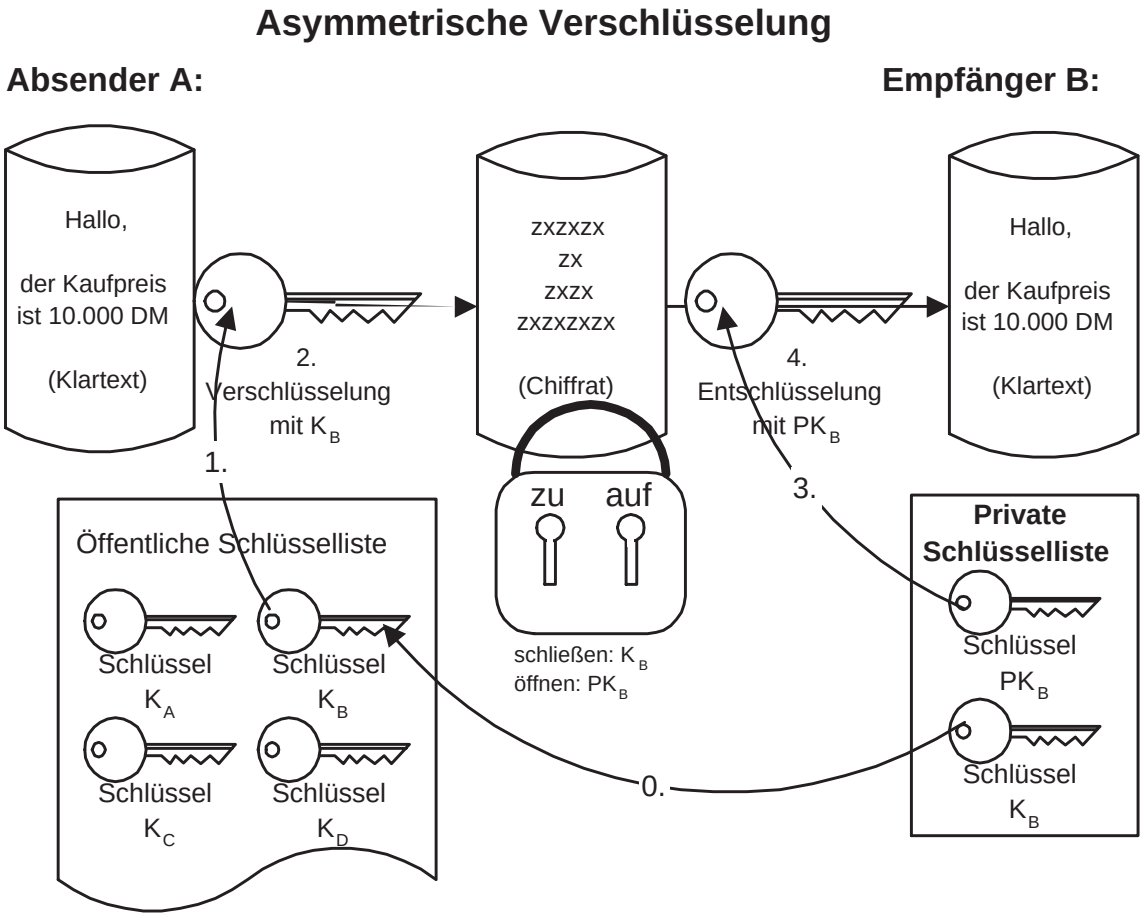


Abbildung 6.2: Asymmetrische Verschlüsselung

6.3.3 Hybridverfahren

Verfahren, die die Vorteile der symmetrischen und der asymmetrischen Verschlüsselungssysteme nutzen, heißen Hybridverfahren. Für die Verschlüsselung der eigentlichen Information wird ein symmetrisches Verschlüsselungsverfahren verwendet, wobei der genutzte Schlüssel nach einem Zufallsverfahren festgelegt wird. Dieser Schlüssel (Session Key) wird für jeweils genau einen Verschlüsselungsvorgang bzw. für ein begrenztes Zeitintervall gewählt. Er wird mit dem öffentlichen Schlüssel des Adressaten verschlüsselt und kann somit am Ziel durch den einzig dazu Berechtigten entschlüsselt und für die Entschlüsselung der eigentlichen Nachricht(en) verwendet werden. Die aufwendigere asymmetrische Verschlüsselung wird also nur für den im Vergleich zur Nachricht viel kürzeren temporären Schlüssel durchgeführt. Auf diese Art und Weise ist es auch möglich, dieselbe verschlüsselte Information mit geringem Mehraufwand für unterschiedliche Adressaten zu verschlüsseln.

Das Verfahren ist also durch die folgenden Schritte beschrieben, die auch in Abbildung 6.3 dargestellt sind:

Der Absender:

1. Wahl eines Zufallsschlüssels K_x.
2. Verschlüsseln des Zufallsschlüssels K_x mit dem öffentlichen Schlüssel des Empfängers K_B.
3. Verschlüsseln des zu übertragenden Dokuments mit dem Schlüssel K_x.

Der Empfänger:

4. Entschlüsseln des Zufallsschlüssels K_x mit dem privaten Schlüssel des Empfängers PK_B.
5. Entschlüsseln des übertragenen Dokuments mit dem Schlüssel K_x.

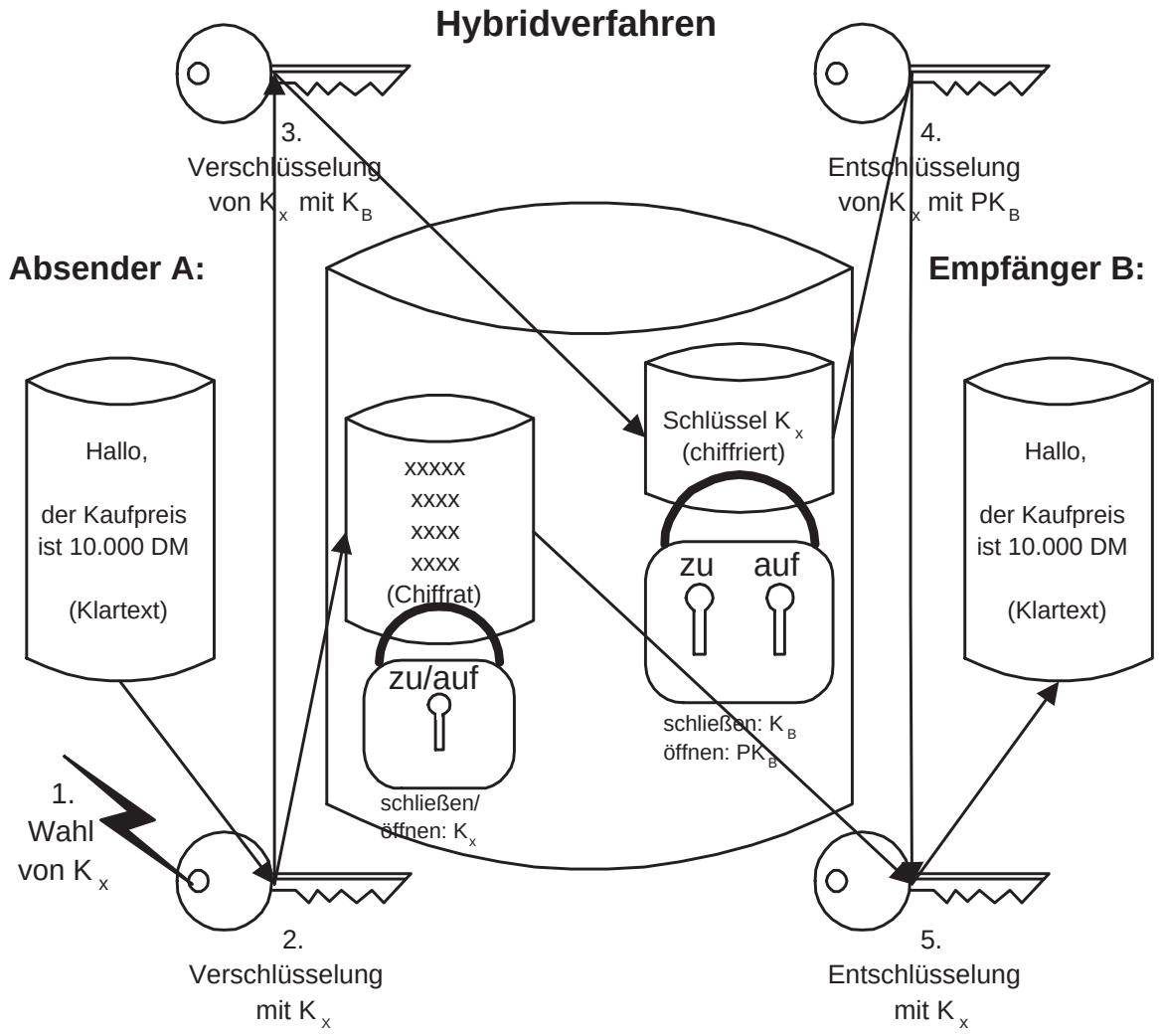


Abbildung 6.3: Hybridverfahren

6.3.4 Vergleich der Verfahren

Symmetrische Verfahren sind u.a. aufgrund der geringeren Schlüssellängen gegenüber asymmetrischen Verfahren performanter. Sowohl bei der Verschlüsselung lokaler Daten, bei der sich das Problem der sicheren Schlüsselübermittlung nicht stellt, als auch in den Fällen, in denen ein guter Durchsatz erreicht werden soll, bietet es sich daher an, symmetrische Verfahren zu nutzen. Hierbei ist die für dieses Verfahren verfügbare Schlüssellänge für den Schutz vor Entschlüsselung wichtig. Nach /Kauffels97/ reicht der Einsatz von 10 Mio $ aus, um einen 40 Bit-DES-Schlüssel in sieben Sekunden und einen 56-Bit Schlüssel in 13 Stunden zu entschlüsseln. Derzeit gelten Schlüssellängen für symmetrische Verfahren von 112 bzw. 128 Bit als angemessen.

Bei asymmetrischen Verfahren werden inzwischen üblicherweise Schlüssellängen von 1024 Bit verwendet. Ist dieser Schlüssel z.B. durch seinen Einsatz als Signaturschlüssel von größerer Bedeutung, so werden schon Mindestlängen von 2048 Bit empfohlen /DFN-PCA97/.

Aufgrund der Problematik des sicheren Schlüsselaustauschs bei symmetrischen Verfahren werden für die Verschlüsselung zwischen verschiedenen Kommunikationspartnern Hybridverfahren eingesetzt. Die genutzten Sitzungsschlüssel können auf sichere Weise automatisch gewechselt werden, es sei denn das asymmetrische Schlüsselpaar wurde kompromittiert oder entschlüsselt.

6.3.5 Signatur von Daten durch asymmetrische Verschlüsselung

Außer zur Verschlüsselung von Daten können asymmetrische Verschlüsselungsverfahren auch dazu genutzt werden, um die Integrität und den Urheber eines Dokuments zweifelsfrei nachzuweisen.

Bei der Verschlüsselung wird der öffentliche Schlüssel des Adressaten benutzt, um sicherzustellen, dass nur dieser (autorisiert) die Information entschlüsseln kann. Demgegenüber soll es durch die Verwendung einer digitalen Signatur prinzipiell jeder Person / jedem Dienst möglich sein, zu prüfen, ob die Information unverfälscht ist und ob der angegebene Autor auch tatsächlich stimmt. Aus diesem Grunde wird für die Erstellung der Signatur der private Schlüssel des Autors benutzt. Um eine Signatur zu erstellen und zu prüfen, ist es jedoch nicht erforderlich, das gesamte Dokument mit dem privaten Schlüssel zu verschlüsseln. Es reicht, wenn mit Hilfe eines Hash-Algorithmus wie beispielsweise SHA oder MD5 eine qualifizierte Prüfsumme, auch „Message-Digest“ genannt, ermittelt wird, die dann verschlüsselt abgelegt wird. Dieses Verfahren ist natürlich auch eine mögliche Schwachstelle, wenn es (mit wenig Aufwand) gelingt, für ein anderes Dokument die gleiche Prüfsumme zu erzeugen. Folgende Schritte sind also durchzuführen:

Zur Erstellung der Signatur:

1. Bildung der qualifizierten (kryptographischen) Prüfsumme aus dem zu signierenden Dokument.
2. Verschlüsselung dieser Prüfsumme mit dem privaten Schlüssel des Autors.

Zur Prüfung der Signatur:

3. Bildung der qualifizierten (kryptographischen) Prüfsumme aus dem signierten Dokument.
4. Entschlüsselung der übermittelten Prüfsumme mit dem öffentlichen Schlüssel des Autors.
5. Vergleich der beiden ermittelten Prüfsummen. Stimmen diese überein, so ist die Urheberschaft und Integrität des Dokuments nachgewiesen.

Für den zweifelsfreien Nachweis der Urheberschaft für ein Dokument sowie seiner Unversehrtheit kommt der Validierung des Schlüsselpaares sowie der Geheimhaltung des privaten Schlüssels besondere Bedeutung zu.

Das damit verbundene Problem der Rechtsverbindlichkeit digitaler Unterschriften sowie das Verfahren zur Validierung sind Gegenstand des 1997 verabschiedeten Signaturgesetzes bzw. der dazu ergänzend erlassenen Signaturverordnung.

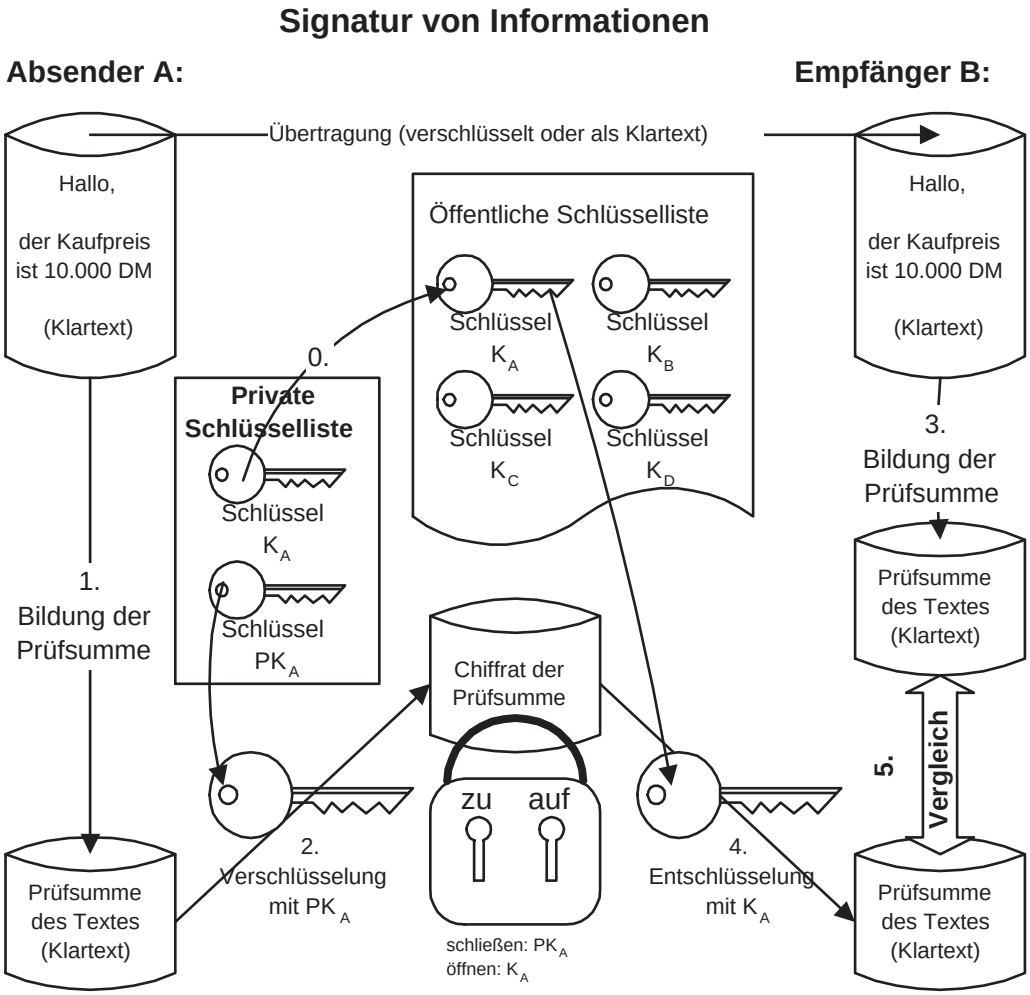


Abbildung 6.4: Signatur von Informationen

6.4 Schlüsselerzeugung, -verwaltung und -verteilung, Zertifizierungsinstanzen, Schlüsselmanagement

Für die sichere und einfache Durchführung von Verschlüsselung ist die Schlüsselerzeugung, -verwaltung und -verteilung von entscheidender Bedeutung. Hinzu kommt die evtl. notwendige Validierung der Gültigkeit eines Schlüssels sowie der Zuordnung zwischen Person/Dienst und dem angegebenen Schlüssel.

6.4.1 Schlüsselerzeugung

Vielfach wird bei der Schlüsselerzeugung eine Zufallszahl bzw. Zufallsbitfolge verwendet. Abhängig vom Zufallsverfahren kann die Chiffriersicherheit stark geschwächt werden, wenn z.B. nur eine geringe Anzahl unterschiedlicher Zufallszahlen und somit nur eine geringe Anzahl unterschiedlicher Schlüssel erzeugt werden kann.

Bei asymmetrischen Verfahren hängt der Aufwand, den fehlenden Teil des Schlüsselpaars zu rekonstruieren, davon ab, wie groß die relative (mathematische) Rekonstruierbarkeit der beiden Teile ist.

Bei der Schlüsselerzeugung ist sicherzustellen, dass der Schlüssel bzw. das Schlüsselpaar nicht bereits bei der Erzeugung kompromittiert, d.h. Unbefugten zugänglich wird.

6.4.2 Schlüsselverwaltung

Die Verwaltung eines erzeugten Schlüssels bzw. des geheimen Teils eines Schlüsselpaares ist entscheidend für die Gewährleistung der gewünschten Eigenschaften. Daraus folgt, dass an das Speichermedium sowie seine Umgebung hohe Anforderungen gestellt werden müssen.

Die Geheimhaltung des für die Entschlüsselung notwendigen Schlüssels kann z.B. dadurch erleichtert werden, dass für den Zugriff zusätzlich der Besitz einer Chipkarte notwendig ist, auf der (allein) der Schlüssel gespeichert ist. Die Speicherung eines geheim zu haltenden Schlüssels auf einem Mehrbenutzersystem dagegen stellt ein besonders hohes Risiko dar.

6.4.3 Schlüsselverteilung

Zur Verteilung der öffentlichen Schlüssel (mit der Zuordnung zu bestimmten Personen bzw. Diensten) können verschiedene Mechanismen genutzt werden:

- Verteilung via Electronic Mail,
- Angebot über die Informationsdienste WWW, Gopher, FTP,
- Verteilung über sog. Key-Server,
- Verteilung über Directory-Dienste, wie z.B. X.500.

Allein aus der Verfügbarkeit eines öffentlichen Schlüssels mit der Zuordnung zu einer bestimmten Person bzw. einem Dienst lässt sich nicht schließen, dass der gefundene Schlüssel auch tatsächlich für die bzw. von der genannten Person erzeugt wurde. Eine Schlüsselvalidierung sollte auf alle Fälle erfolgen.

Bei symmetrischen Verfahren muss der Schlüssel auf anderen vertrauenswürdigen Wegen verteilt werden, z.B. durch die Übermittlung per Boten oder per Einschreiben mit Rückschein. Bei der Wahl des Verteilweges ist jedoch immer zu prüfen, ob mögliche Angreifer auch auf diesen Weg Zugriff haben. So ist etwa bei der Übermittlung über Telefon oder Telefax nicht davon auszugehen, dass die Vertraulichkeit gewahrt ist.

6.4.4 Validierung des Schlüssels

Bei der Validierung eines (bekannten) Schlüssels werden die folgenden Eigenschaften geprüft:

- Ist die angegebene Zuordnung zwischen Schlüssel und Person/Dienst korrekt?
- Ist der Schlüssel bzw. das Schlüsselpaar noch gültig oder ist der Schlüssel kompromittiert und darf deshalb nicht mehr verwendet werden?

Die Notwendigkeit dieser Prüfung stellt sich vor allem bei der Verwendung öffentlich verfügbarer Schlüssel, sie ist jedoch auch bei der Verwendung symmetrischer Schlüssel sinnvoll. Dies gilt selbst dann, wenn der/die Schlüssel auf vertrauenswürdigen Wegen zugestellt wurden. (Auch ein Bote kann „falsche“ Schlüssel überbringen.)

Für die Validierung stehen je nach eingesetztem Verfahren verschiedene Wege zur Auswahl:

- Persönlicher Kontakt zum Eigentümer bzw. Aussteller des (öffentlichen) Schlüssels,
- Beglaubigung der Zuordnung durch einen vertrauenswürdigen Dritten,
- Aufbau eines „Vertrauenspfades“ zwischen Absender und Empfänger.

Der erste Weg setzt voraus, dass man den Empfänger bzw. Aussteller tatsächlich kennt.

Der zweite Weg wird u.a. dann eingeschlagen, wenn keine zentrale Instanz eingesetzt wird bzw. werden soll, die die Beglaubigung der Schlüssel übernimmt. Dies ist z.B. bei Pretty Good Privacy (PGP) vorgesehen.

Für den dritten Weg nutzt der Anfragende eine Reihe sich gegenseitig vertrauender Instanzen, um die Gültigkeit der Zuordnung zwischen Empfänger und Schlüssel (beim Empfänger bzw. dessen schlüsselausgebender Stelle) zu prüfen. Diese Vertrauensprüfung kann auch automatisch durchgeführt werden.

6.4.5 Zertifizierungsinstanzen und TrustCenter

Für den Aufbau eines Vertrauenspfades zwischen Absender und Empfänger ist eine Struktur erforderlich, auf der das verlässliche Vertrauen mit relativ geringem Verwaltungsaufwand herstellbar ist.

Dieser Vertrauenspfad lässt sich z. B. bilden, indem eine Kette von Instanzen zwischen Absender und Empfänger gefunden wird, die sich jeweils gegenseitig vertrauen.

Die Ordnung der Instanzen in einer Zertifizierungshierarchie bietet sich an, um den Aufwand zum Herstellen von möglichst vielen Vertrauenspfaden zu minimieren. In dieser Zertifizierungshierarchie werden von Zertifizierungsinstanzen bestimmte Regeln, die sog. Policies, aufgestellt, die erfüllt werden müssen, damit andere (Unter-)Instanzen zertifiziert werden können.

Ein Zertifikat ist die nachprüfbare Bestätigung einer Stelle, dass die Zuordnung einer Person bzw. einer Institution zu deren öffentlichem Schlüssel geprüft ist. Das Zertifikat selbst ist der mit dem privaten Schlüssel der zertifizierenden Instanz signierte öffentliche Schlüssel des Zertifizierten. Lässt sich also eine Institution zertifizieren, so tauscht sie mit der Zertifizierungsstelle das Zertifikat für den öffentlichen Schlüssel aus, der zu dem privaten Schlüssel gehört, mit dem diese Instanz Zertifikate ausstellt. Durch diesen Austausch ist es somit möglich, die Zertifikate der anderen Institution zu prüfen. Die Abbildung 6.5 auf der folgenden Seite stellt eine solche Zertifizierungshierarchie und beispielhaft die Prüfung eines öffentlichen Schlüssels dar.

Derzeit wird im deutschen Wissenschaftsbereich über ein BMBF-gefördertes Projekt (DFN-PCA) eine Zertifizierungshierachie aufgebaut. Die an der Universität Hamburg eingerichtete DFN-PCA (Policy Certification Authority) hat die Regularien festgelegt, die berücksichtigt werden müssen, damit Zertifizierungsinstanzen an den Hochschulen aufgebaut, betrieben und ihrerseits von der DFN-PCA zertifiziert werden können. Hierfür existieren zwei Policies /DFN-PCA97/, die den Aufgaben entsprechend unterschiedliche Anforderungen an untergeordnete Certification Authorities (CA) und Registration Authorities (RA) stellen. In diesen Policies werden u.a. folgende Punkte geregelt:

- Zuständigkeitsbereich der PCA,
- Sicherheit der PCA-Ausstattung,
- Sicherheitsanforderungen an CAs/RAs:
  - Anforderungen an die Rechnerausstattung und Verbindungen zu anderen Rechnern,
  - Anforderungen an die Benutzung der Schlüssel der CA,
- Sicherheitsanforderungen an Benutzer,
- Zertifizierungsregeln:
  - wie werden die Schlüssel erzeugt, gespeichert und vernichtet,
  - wie muss die Zuordnung zwischen Schlüsselinhaber und Schlüssel geprüft werden,
- Management von Zertifikaten,
- Widerruf von Zertifikaten.

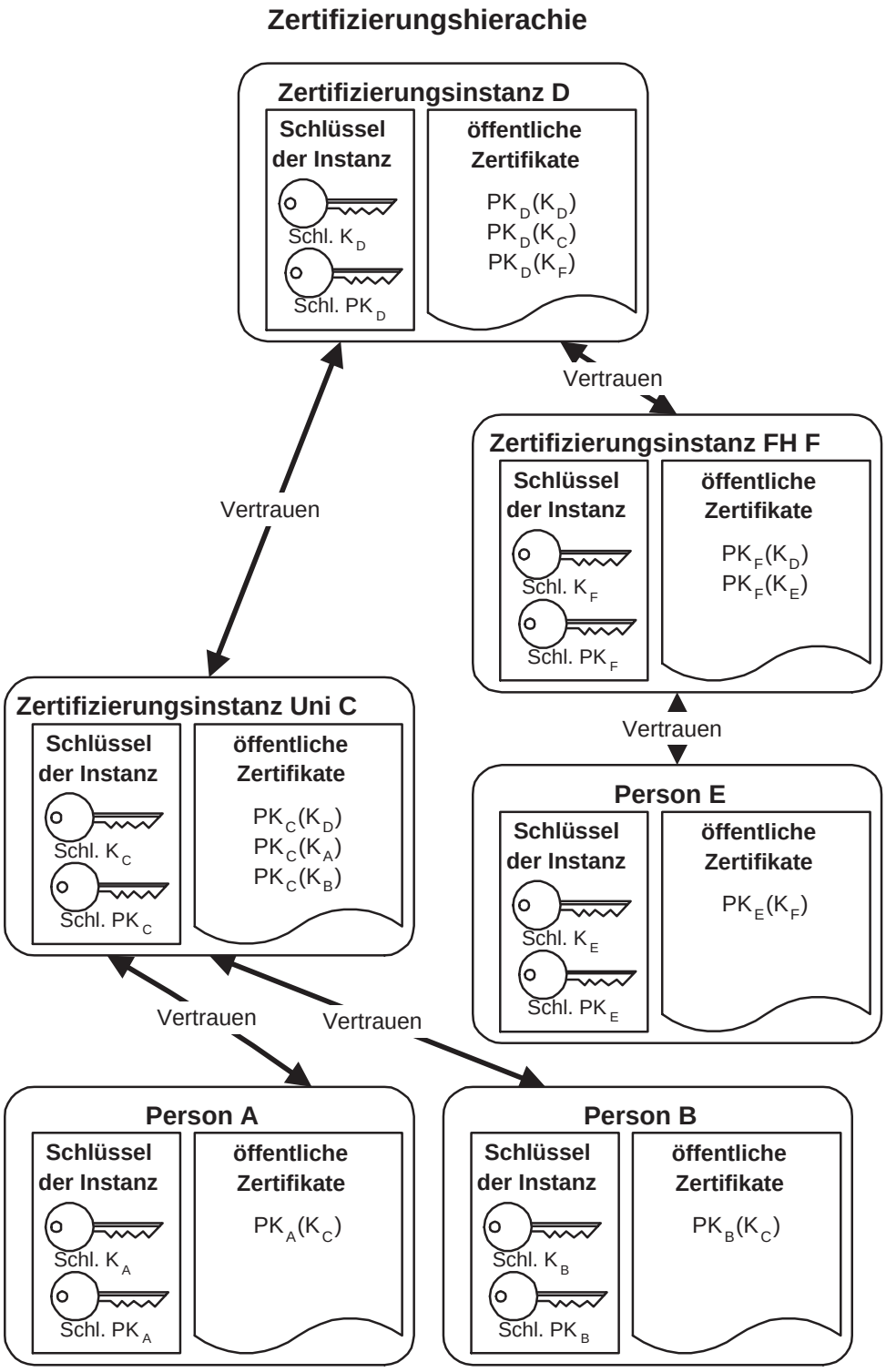


Abbildung 6.5: Zertifizierungshierarchie

Die Erzeugung von Schlüsselpaaren und die Verwaltung der eigenen (geheimen) Schlüssel spielen eine zentrale Rolle beim Betrieb der CA. Rechner, die u.a. dafür eingesetzt werden, bezeichnet man als **TrustCenter**. Ein TrustCenter erfüllt insgesamt folgende Aufgaben:

- Erzeugung von Schlüsselpaaren,
- sichere Übergabe an den Besitzer z.B. durch physische Ausstellung von Chipkarten,
- Ausgabe zertifizierter und beglaubigter Softwarekomponenten.

Das TrustCenter stellt als eine zentrale Komponente des Key-Management ein bevorzugtes Angriffsziel für Eindringlinge in geschützte Netze dar. Daraus folgt, wie es auch in den Policies der DFN-PCA geregelt ist, dass dieser bzw. diese Rechner vom Rechnernetz separiert zu betreiben ist (sind) und spezielle Mechanismen für den Zugriffsschutz und den Datenträgeraustausch vorgesehen werden müssen. Der Aufbau und Betrieb des TrustCenters ist daher kostspielig.

Aus dem isolierten Betrieb des TrustCenters folgt unmittelbar, dass es folgende Aufgaben nicht erfüllen kann:

- Die Verteilung oder Bereitstellung der beglaubigten öffentlichen Schlüssel,
- Online-Schlüsselbeglaubigung.

Aufgrund der zwischenzeitlich verabschiedeten gesetzlichen Regelungen und des absehbaren kommerziellen Einsatzes von Signaturverfahren für elektronischen Geschäftsverkehr werden durch einige Organisationen TrustCenter aufgebaut bzw. deren Aufbau vorbereitet. Dies soll dann als Dienstleistung für andere Unternehmen angeboten werden.

6.5 Verfahren zur Verschlüsselung lokaler Daten

Die Verschlüsselung lokaler Daten ergibt sich aus verschiedenen Gründen. Für die einzelnen Einsatzzwecke gibt es dann wiederum verschiedene Ansätze.

Bei den klassischen Arbeitsplatzrechnern (PCs) handelt es sich meistens um Rechner, deren Betriebssystem (z.B. MS-DOS) keine Zugangskontrolle enthält.

Zugangskontrollen zu diesen Rechnern sind jedoch aus folgenden Gründen wünschenswert:

- Einsatz lizenzrechtlich geschützter Software,
- Einsatz eigenentwickelter Software,
- Speicherung lokaler (vertraulicher) Daten insbesondere auf mobilen PCs,
- Schutz vor dem Einbringen von Viren oder trojanischen Pferden.

Hier setzen Produkte verschiedener Hersteller (z.B. Utimaco Safeware /Utimaco97/) an, die mit der Zugangskontrolle die Verschlüsselung kompletter Festplatten verbinden. Diese Produkte umfassen mit diesem Ansatzpunkt weitere Funktionalitäten:

- Benutzerabhängige Schreib- und Leserechte auf einzelne Dateien,
- Vergabe von Zugriffsrechten für Disketten und Schnittstellen,
- Verschlüsselung von Disketten zum Schutz vor unerlaubtem Export von Dateien,

- Dokumentation der Systemnutzung.

Je nach Performanceanforderungen werden solche Produkte sowohl softwarebasiert als auch hardwarebasiert bzw. -unterstützt angeboten.

Hardwarebasierte Verfahren beeinträchtigen die Leistungsfähigkeit des Hauptprozessors bei gleichzeitigen Plattenzugriffen nicht und sind somit performanter als Softwarelösungen.

Neben diesen hardwarenahen Mechanismen gibt es auch auf Anwendungsebene die Möglichkeit, Dateien zu verschlüsseln. Erste Programme aus dem Bereich der Standardprodukte mit derartigen Verschlüsselungsmöglichkeiten waren Textverarbeitungsprogramme. Dort war diese Funktion jedoch eher eine Nebensächlichkeit, so dass die eingesetzten Algorithmen größeren Kryptanalyse-Ansätzen nicht standhielten.

Einige weitere Programme, wie z.B. Pretty Good Privacy (PGP) oder (aus der UNIX-Welt) *crypt* bieten die Möglichkeit, lokale Dateien zu verschlüsseln. Diese Programme spielen ebenso bei der Verschlüsselung von Daten zur Übertragung eine Rolle. Werden die Daten nur lokal abgelegt und nicht mit anderen ausgetauscht, so entfällt die Notwendigkeit, auf vertrauenswürdigen Wegen Schlüssel auszutauschen. Der Einsatz rein symmetrischer Verfahren reicht deshalb zur Verschlüsselung lokaler Dateien im Allgemeinen aus.

6.6 Verfahren zur Verschlüsselung von Daten bei der Übertragung

Für die Verschlüsselung von Daten bei der Übertragung gibt es Ansätze auf den verschiedenen Schichten der Protokollhierarchie. Im Allgemeinen sind diese Verfahren jedoch nicht standardisiert, so dass auf beiden Seiten der Kommunikation Geräte, Programme bzw. Kommunikationsprotokolle des gleichen Herstellers eingesetzt werden müssen.

6.6.1 Verschlüsselung auf den netzorientierten Schichten

Bei den netzorientierten Schichten (Schicht 1 (Physische Schicht) bis Schicht 3 (Vermittlungsschicht)) hängt es von der logischen Entfernung der Kommunikationspartner ab, auf welcher Schicht Verschlüsselungsverfahren eingesetzt werden können. Soll z.B. ein lokales Netz durch ein fremdes Gebäude verlängert werden, so kann eine Verschlüsselung auf Schicht 2 gewählt werden. Soll jedoch ein Virtuelles Privates Netz (VPN) über andere Netze hinweg aufgebaut werden, so ist eine Verschlüsselung und Tunnelung auf Schicht 3 (z.B. IP) notwendig. Für die Verschlüsselung auf der Netzschicht (IP, IPX, X.25) stehen einige Produkte (z.B. von Network Systems, Cisco) zur Auswahl, die zusätzlich als Router fungieren. Andere Geräte (z.B. von KryptoKom) haben keine eigene Routingfunktionalität.

Die einzelnen Produkte unterscheiden sich u.a. durch die eingesetzten Verschlüsselungsverfahren und insbesondere auch durch die Schlüssellängen.

Wird die Verschlüsselung über einen separaten speziellen Verschlüsselungsbaustein durchgeführt, ist das Gerät meistens derart ausgelegt, dass der Durchsatz (die Chiffrierleistung) durch das genutzte Transportmedium (Ethernet, ISDN, ...) begrenzt ist. Wird hingegen die Verschlüsselung in Software über den Hauptprozessor realisiert, so wird die Chiffrierleistung eher durch die Leistungsfähigkeit des Prozessors begrenzt sein.

Neben der Verschlüsselungsfunktionalität an Netzübergängen bieten einige Hersteller auch Einsteckkarten für einzelne Geräte (i. Allg. PCs) an, so dass für die Einbindung von Einzelgeräten in ein VPN keine separaten (und teureren) Netzkomponenten eingesetzt werden müssen.

Der Aufbau eines Virtuellen Privaten Netzes (VPN) mittels Verschlüsselungskomponenten auf der Netzschicht bietet sich zur Kopplung verschiedener verteilter Standorte von Hochschulverwaltungen und -kliniken an. Entsprechende Pilotinstallationen sind an den Universitäten Eichstätt, Erlangen-Nürnberg und der TU München im Einsatz. Bei der Kommunikation wird vielfach ein regelmäßiger Schlüsselwechsel durchgeführt. Das Verfahren zum Austausch dieser neuen Schlüssel kann auch eine Schwäche des Systems darstellen.

Die Verwaltung und der gesicherte (automatische) Austausch der genutzten Schlüssel zwischen den einzelnen Geräten erfordert z.T. ein gemeinsames Managementsystem, auf dem auch die Betriebsmeldungen des Systems auflaufen. Ist eine Kopplung von Verschlüsselungsgeräten nicht nur innerhalb einer Einrichtung gewünscht, so sind neben den technischen auch entsprechende organisatorische Maßnahmen zu ergreifen, um den Betrieb auch dafür zu gewährleisten.

Abhängig vom vorhandenen Kommunikationsbedarf ist der Aufbau eines VPN über verschlüsselnde Netzkomponenten gegebenenfalls nicht der geeignete Weg, so z.B. wenn nur sporadisch elektronische Briefe vertraulichen Inhalts ausgetauscht werden. Soll andererseits der Verkehr zu einem Server im Rahmen rechtsverbindlicher Geschäfte zu beliebigen Beteiligten gesichert sein, ist der Aufbau eines VPN gar nicht möglich. Hier müssen Mechanismen auf höheren Protokollschichten genutzt werden.

6.6.2 Verschlüsselung auf den anwendungsorientierten Schichten

Für die Unterstützung verschiedener Anwendungen durch Verschlüsselungsmaßnahmen wurden in letzter Zeit auf unterschiedlichen Protokollschichten Verschlüsselungsprotokolle entworfen:

- auf der Vermittlungsschicht (3):
  - Authentication Header (teilweise auch in IPv4-Implementierungen realisiert),
  - Encapsulating Security Payload (ESP);
- auf der Kommunikationssteuerungsschicht (5):
  - Secure Sockets Layer (SSL) von Netscape und anderen Herstellern mit Schlüssellängen bis 128 Bit,
  - „Private communication technology“ von Microsoft;

- auf der Anwendungsschicht (7):
  - S-HTTP,
  - S/MIME,
  - Secure Shell (SSH);
- Anwendungen als Aufsatz für Datenaustauschprotokolle:
  - Pretty Good Privacy (PGP),
  - *crypt*.

Die Entscheidung, auf welchen Schichten Verschlüsselungsmechanismen eingesetzt werden sollen, hängt einerseits von der organisatorischen Zusammengehörigkeit der Kommunikationspartner und andererseits von den Anwendungen ab, aus denen heraus Daten verschlüsselt ausgetauscht werden sollen. Einige der oben genannten Ansätze beruhen auf Produkten, die in den USA hergestellt und von dort nach Deutschland exportiert werden müssen. Die Stärke des verwendeten Verschlüsselungsverfahrens ist dann (z.T.) aufgrund der Exportrestriktionen der USA für Kryptoprodukte stark eingeschränkt.

6.6.3 Steganographie

Unter Steganographie versteht man Verfahren, bei denen Informationen in einem Trägerdokument versteckt werden, wenn dabei die folgenden Eigenschaften erfüllt sind:

- Die versteckte Information ist nur mit dem Wissen, wo sie platziert ist oder nach welchem Algorithmus sie versteckt ist, aus dem Trägerdokument zu extrahieren.
- Der Trägerinformation ist (abhängig vom eingesetzten Verfahren) nicht bzw. nur sehr schwer anzumerken, dass darin weitere Informationen versteckt sind.
- Die versteckte Information bleibt auch bei Transformationen, wie z.B. Komprimierung, erhalten.

Die dritte Anforderung stellt sich erst mit dem automatisierten Einsatz von Steganographiemethoden auf Computern. Die Geschichte der Steganographie ist bereits sehr viel älter.

Steganographieverfahren sind symmetrischen Verschlüsselungsverfahren vergleichbar. Das Wissen, wie die versteckte Information aus dem Trägerdokument zu extrahieren ist, entspricht der Kenntnis des Schlüssels bei symmetrischen Verfahren.

Als Dokumente, in denen andere Informationen versteckt werden, eignen sich Bilder vorzüglich. Es ist inzwischen üblich, Farbbilder mit hoher Auflösung und großer Farbtiefe auszutauschen. Durch leichte Modifikation von Farbinformationen an bestimmten Stellen wird die zu versteckende Information im Dokument untergebracht. Diese Unterschiede sind auch ohne zusätzliche Verschleierungsmaßnahmen am Bild für das menschliche Auge nicht zu erkennen.

Auf diese Art und Weise kann (verschlüsselte) Information ausgetauscht werden, ohne dass dies von außen erkennbar ist.

Steganographie wird inzwischen auch genutzt, um Informationen über das Copyright digital verfügbarer Bilder in den Bildern selbst zu speichern.

6.6.4 Kryptoverfahren im Widerstreit der Interessen

Kryptographische Verfahren ermöglichen es bei Verwendung ausreichend langer Schlüssel sowie eines geeigneten Verfahrens, die unerlaubte Kenntnisnahme bzw. Verfälschung von Informationen (bei vertretbarem Aufwand für einen Angreifer) zu verhindern.

Sieht man diese Möglichkeiten aus der Sicht von Konkurrenten, so sind Kryptoverfahren entscheidende Hemmnisse in der Informationsgewinnung über den jeweils Anderen.

Aus diesem Grund unterliegen kryptographische Verfahren beim Export aus den USA der Genehmigungshoheit des Department of Defense (DoD). Weiterhin ist bekannt, dass nationale Nachrichtendienste ihre Möglichkeiten einsetzen, um der eigenen Wirtschaft Vorteile aus der verdeckten bzw. unerwünschten Informationsgewinnung zu verschaffen. Dies gelingt am besten, wenn die Verfahren, die die andere Seite einsetzt, mit vorhandenem Zusatzwissen leicht zu entschlüsseln sind und dennoch Außenstehende größte Anstrengungen unternehmen müssen, um evtl. an die Informationen heranzukommen.

So ist bei Produkten, die nicht durch eine offizielle Stelle des eigenen Landes (in Deutschland das BSI) bzw. in deren Auftrag tätige Stelle zertifiziert sind, nicht auszuschließen, dass darin Anderen bekannte verdeckte Kanäle enthalten sind.

Auch im Hochschulbereich ist davon auszugehen, dass für andere Länder bzw. fremde Organisationen interessante Daten vorhanden sind und ausgetauscht werden. Neben den Daten, die personenbezogen in den Kliniken und Verwaltungen anfallen, sind dies im Forschungsbereich beispielsweise Projektanträge oder Zwischenberichte an das Ministerium. Außerdem finden viele Projekte in Kooperation zwischen verschiedenen Forschungseinrichtungen statt, so dass dort Projektinformationen ausgetauscht werden.

Neben nachrichtendienstlichen Interessen gibt es weitere Vorstöße, eine unabhängige sichere Kryptographie zu behindern.

Die US-Regierung hat im Januar 1997 ein Programm gestartet, das amerikanischen Herstellern den Export von (immer noch nicht ausreichend starker) Verschlüsselungstechnologie erleichtert, wenn sich diese verpflichten, innerhalb von zwei Jahren sog. „key recovery“-Mechanismen zu implementieren, siehe auch /Kauffels97/. Diese Mechanismen sehen vor, dass bei „vertrauenswürdigen Stellen“ sog. Ersatzschlüssel hinterlegt werden, mit denen die Entschlüsselung der ausgetauschten Daten möglich ist. Neben der Frage, welche (Regierungs-)Stelle z.B. für multinationale Unternehmen vertrauenswürdig ist, stellt allein die Existenz von (gesammelten) Ersatzschlüsseln ein erhebliches Sicherheitsrisiko dar.

Ein weiterer Ansatz ist ein Verbot des Einsatzes von Verschlüsselungsverfahren außerhalb streng gesetzlich geregelter Bereiche. Wie im Abschnitt 6.6.3 über die Steganographie ausgeführt, existieren jedoch Verfahren, mit denen Informationen ausgetauscht werden können, ohne dass dies erkennbar ist. Die erwünschte Wirkung würde durch ein derartiges Verbot also nicht erreicht, während das Risiko für andere, auf vertrauliche Speicherung und

Übertragung von Daten angewiesene Organisationen allerdings beträchtlich erhöht würde. Die sog. „interessierten Kreise“, die eigentlich durch ein Verschlüsselungsverbot behindert werden sollten, besäßen jedoch weiterhin die Möglichkeit, ungestört Informationen auszutauschen.

Ohne Verschlüsselung jedoch sind einige der für den gesicherten Einsatz von verteilten bzw. öffentlich zugänglichen DV-Verfahren in den Hochschulen notwendigen Eigenschaften nicht zu gewährleisten.

Die Kommission erachtet deshalb ein Verschlüsselungsverbot oder den Einsatz von „key-recovery“-Mechanismen als nicht sinnvoll und kontraproduktiv.

6.7 Empfehlungen zur Verschlüsselung

- Sämtliche Arbeitsplatzrechner und Server in der Verwaltung und den Kliniken sollten das Arbeiten erst dann ermöglichen, wenn sich die nutzende Person authentifiziert hat. Das Gleiche gilt für das Ändern von Daten auf der lokalen Festplatte.

  Sofern diese Authentifizierung nicht vom Betriebssystem unterstützt wird, sollen entsprechende Softwareverfahren eingesetzt werden, wie sie z.B. von Utimaco Safeware verfügbar sind, die diese Funktionalität bieten.
- Werden Laptops eingesetzt, so sind wegen des höheren Diebstahlrisikos zusätzlich Verfahren zur lokalen Verschlüsselung der Festplatte vorzusehen.
- Die Verbindung verteilter Standorte von Verwaltungen und Kliniken sollte durch die Implementierung eines durch kryptographische Methoden gesicherten VPN erfolgen. Zur Interoperabilität zwischen den bayerischen Hochschulen ist es bei weiterhin positiv verlaufendem Pilotbetrieb zu empfehlen, Geräte der Fa. KryptoKom einzusetzen.
- Für den Austausch von Dateien mit möglicherweise vertraulichem oder sensitivem Inhalt sollte das Produkt PGP genutzt und von den Hochschulrechenzentren unterstützt werden. Bei der Erzeugung eigener Schlüssel ist u.a. darauf zu achten, dass der private Schlüssel sicher z.B. auf einer Chipkarte aufbewahrt und keiner anderen Person zugänglich wird. Insbesondere verbietet sich die Verwahrung auf Mehrbenutzersystemen, wo der unautorisierte Zugriff nicht ausgeschlossen ist. Generell empfiehlt sich bei asymmetrischen Verschlüsselungsverfahren eine Schlüssellänge von 2048 Bit.
- Ist eine sensitive Information auf dem Weg zum Empfänger nicht ausreichend gesichert bzw. ist eine Zuordnung zwischen Empfänger und zugehörigem Schlüssel nicht gewährleistet, so ist die Übertragung im Allgemeinen zu unterlassen.
- Werden interne Dokumente verschlüsselt abgelegt, so sollte sichergestellt werden, dass auch im Verhinderungsfall des Autors bzw. Schlüsselinhabers andere autorisierte Personen Zugriff zu diesen Daten haben. Eine Möglichkeit ist die versiegelte Ablage von Umschlägen mit den entsprechenden Passwörtern in separat zugangsgeschützten Einrichtungen (z.B. Tresor). Diese Umschläge sollten u.a. die Daten der Berechtigten, des Erstellers, das Datum sowie den Namen der Person, die im Falle des Siegelbruchs verständigt werden muss, enthalten.

6.8 Literatur

/Bauer94/ Bauer, F.L.:
„Kryptologie“,
2. Auflage, Springer Verlag Berlin, 1994

/Beutelspacher/ Beutelspacher, A.:
„Kryptologie“,
3. Auflage, Vieweg Verlag

/Beutelspacher95/ Beutelspacher, A. / Schwenk, J. / Wolfenstetter, K.-D.:
„Moderne Verfahren der Kryptographie“,
Vieweg Verlag, 1995

/DFN-CERT/ DFN-CERT:
„WWW-Server des DFN-CERT“,
`http://www.cert.dfn.de`

/DFN-PCA97/ Deutsches Forschungsnetz – DFN –:
„Die Policies der DFN-PCA
Zertifizierungsrichtlinien des Projekts PCA im DFN“,
DFN-Bericht Nr. 82, April 1997

/Garfinkel95/ Garfinkel, S.:
„PGP“,
O’Reilly, 1995

/Kauffels97/ Kauffels, F.:
„Key Recovery in der Diskussion“,
DATACOM 2/97

/KryptoKom/ Pohlmann, N.:
„KryptoGuard und Kryptowall“,
Produktinformationen

/Network Systems/ Network Systems:
Produktinformationen

/PGP/ Zimmermann, P.:
„Pretty good privacy“,
Dokumentation

/Ruhland93/ Ruhland, Ch.:
„Informationssicherheit in Datennetzen“,
Datacom Verlag, 1993

/Schneier95/ Schneier, B.:
„Applied Cryptography“,
1995

/SSH/ SSH Remote Login Program
`http://www.cs.hut.fi/ssh`

/Stallings94/ Stallings, W.:
„Network and Internetwork Security: Principles and Practice“,
Prentice-Hall, 1994

/Utimaco/ Utimaco Safeware AG:
Produktinformationen

Kapitel 7

Sichere Betriebssysteme und Basisdienste

7.1 Übersicht

Betriebssysteme spielen als zentrale Instanzen zur Verwaltung der Ressourcen von Rechnern auch eine wichtige Rolle in Bezug auf deren Sicherheit. Dieses Kapitel

- erläutert die mit der Sicherheit von Betriebssystemen zusammenhängenden Konzepte,
- gibt eine systematische Übersicht über Sicherheitsmechanismen im Betriebssystem und
- stellt konkrete Beispiele dazu vor.

7.2 Sicherheitsziele

Eine begriffliche Klärung der mit der Sicherheit von Betriebssystemen zusammenhängenden Konzepte erleichtert es, Maßnahmen zur Verbesserung ihrer Sicherheit zu beurteilen. Wir stellen daher zunächst diese Konzepte vor.

Es ist üblich, in einem EDV-System *Objekte* und *Subjekte* zu unterscheiden. Als Objekte bezeichnen wir passive Informationen oder Systemressourcen. Beispiele für Objekte sind Dateien, Arbeitsspeicher, CPU-Leistung, Programme. Subjekte dagegen sind aktive Instanzen, die den Systemzustand beeinflussen können. Beispiele für Subjekte sind Prozesse, Benutzer, Geräte. Je nach dem Zusammenhang kann ein Objekt in anderem Kontext auch die Rolle eines Subjekts übernehmen. So ist ein aktiver Benutzer zunächst ein Subjekt. Für einen Prozess, der aktive Benutzer sucht, hat dieser Benutzer Objektcharakter.

Sicherheit (security)

Sicherheit ist die Fähigkeit eines Systems, für seine Objekte *Vertraulichkeit (confidentiality)* und *Integrität (integrity)* zu garantieren.

- *Vertraulichkeit (confidentiality)*

  Vertrauliche Objekte sind gegen Missbrauch geschützt. Konkret bedeutet dies z.B. den Schutz vor unerlaubtem Zugang zu Informationen oder unerlaubter Nutzung von Systemressourcen.
- *Integrität (integrity)*

  Die Integrität von Objekten garantiert ihren Schutz gegen unautorisierte Veränderungen.

Weitere Ziele, die ebenfalls in Zusammenhang mit der Sicherheit eines Systems stehen, sind:

- *Verfügbarkeit (availability)*

  Diese bezeichnet die Wahrscheinlichkeit, dass ein System zu einem bestimmten Zeitpunkt betriebsbereit ist und Leistungen erbringen kann.
- *Betriebssicherheit (reliability)*

  Diese bezeichnet die Wahrscheinlichkeit, dass ein System über einen bestimmten Zeitraum hinweg ununterbrochen zur Verfügung steht.
- *Ausfallsicherheit (safety)*

  Damit ist die Tatsache gemeint, dass ein Fehler keine katastrophalen Folgen haben kann, sondern nur zu einer abgestuften Leistungsminderung führt.

Sicherheitspolitik

Die Sicherheit eines Systems ist keine absolute Größe, sondern kann immer nur in mehr oder weniger hohem Umfang erreicht werden. Die Aufgabe der Sicherheitspolitik ist es daher, aufgrund einer Bedrohungsanalyse und der erforderlichen Sicherheitsstufe Regeln für die Sicherheit von Objekten aufzustellen und Maßnahmen zum Erreichen dieser Sicherheit zu bestimmen. Die folgenden Faktoren sind dabei abzuwägen (siehe auch Kapitel 1 „Leitlinien für die Entwicklung und Umsetzung eines IT-Sicherheitskonzepts“):

- *die Art und Höhe des möglichen Schadens*

  Dieser hängt in erster Linie vom Einsatzfeld eines Systems ab. Für elektronischen Zahlungsverkehr, die Steuerung einer Produktionsanlage, ein Patienten-Verwaltungssystem oder die Studenten- und Prüfungsverwaltung einer Hochschule ergeben sich ganz unterschiedliche Schadensszenarien.
- *die möglichen Bedrohungen der Sicherheit*

  Das Bedrohungsszenario hat neben unterschiedlichen Formen aktiver Bedrohung durch Außenstehende auch unabsichtliche Handlungen, z.B. Bedienungsfehler, sowie Fehler in Hard- und Software zu berücksichtigen.

- *die Kosten von Maßnahmen zum Erreichen einer bestimmten Sicherheitsstufe*

  Außer direkten finanziellen Aufwendungen fallen darunter auch indirekte Kosten, z.B. verminderte Systemleistung, kompliziertere Systembedienung, erhöhte Systemkomplexität usw.

Als Ergebnis solcher Abwägungen legt die Sicherheitspolitik zunächst fest, welche Objekte welchen Subjekten zugänglich sein sollen und welche Operationen die Subjekte mit den Objekten durchführen dürfen. Daraus ergeben sich dann die zur Umsetzung dieser Festlegungen erforderlichen Maßnahmen.

Bedrohung der Systemsicherheit

Gefahren für die Sicherheit eines Systems ergeben sich einerseits aus absichtlichen Handlungen, andererseits aber auch aus nicht beabsichtigten Ereignissen und Handlungen von Subjekten. In jedem Fall sind beide Aspekte der Sicherheit betroffen:

- *Confidentiality:* Die Vertraulichkeit von Objekten kann verletzt werden.
- *Integrity:* Objekte können verändert oder sogar vernichtet werden.

Unbeabsichtigte Verletzungen der Sicherheit eines Systems ergeben sich einerseits aus Fehlfunktionen von Hard- und Softwarekomponenten, aus unbekannten Systemeigenschaften, aber auch durch Handlungen von Personen. Einige typische Beispiele verdeutlichen die Bandbreite solcher Risiken:

- Ein Benutzer verschickt per E-Mail eine Datei mit vertraulichem Inhalt. Durch einen Adressierungsfehler landen diese Informationen bei Adressaten, die keine Kenntnis von diesen Informationen erhalten sollen.
- Statt des UNIX-Kommandos `rm a*` schreibt ein Benutzer `rm *` und löscht damit unbeabsichtigt alle Dateien im aktuellen Verzeichnis. Durch das Zusammentreffen weiterer Faktoren (keine aktuelle Sicherung, aktuelles Verzeichnis ist ein wichtiges Systemverzeichnis, Benutzer arbeitet gerade als Superuser) kann diese Aktion katastrophale Auswirkungen haben.
- Bei der Umstellung der Telefontarife am 1.1.1996 wurde die Software erst kurz nach Mitternacht gestartet. Sie bekam damit den Wechsel von Silvester auf Neujahr nicht mit und berechnete den Telefonkunden den Werktagstarif. Der unmittelbare materielle Schaden dürfte dabei gegenüber dem Image-Verlust für das Unternehmen noch am wenigsten ins Gewicht gefallen sein.

Angriffe auf die Systemsicherheit sind Aktionen, die zum Ziel haben, die Vertraulichkeit oder die Integrität von Objekten zu verletzen. Sie zielen nicht immer direkt auf die Objekte, deren Sicherheit sie verletzen wollen. Oft erhält ein Angreifer auch Informationen über ein Objekt durch Schlussfolgerungen aus anderen Daten, z.B. aus Zugriffsstatistiken, geschickt formulierten Datenbankabfragen usw.

Man unterscheidet bei Angriffen auf die Systemsicherheit aktive und passive Angriffe:

- *Passive Angriffe* beschränken sich auf die Beobachtung eines Systems, z.B. seines Netzverkehrs oder seiner CPU-Auslastung, und schließen daraus auf die gefährdeten Objekte. Sie sind schwer zu erkennen und oft gibt es kaum Gegenmaßnahmen.

- *Aktive Angriffe* greifen in das System ein und verändern seine Objekte oder sein Verhalten. Insofern sind sie auch leichter zu entdecken.

Einige Beispiele verdeutlichen das Gefahrenpotential solcher Angriffe:

- Durch die Auswertung der Logfiles in einem WWW-Server lassen sich detaillierte Informationen über das Verhalten eines Benutzers ableiten, z.B. welche Seiten er in einem bestimmten Zeitraum abgerufen hat.
- Durch Abhören des Netzverkehrs lassen sich Passwörter und andere Informationen sammeln, die dann den Zugang zu vertraulichen Daten ermöglichen.
- Eine Textdatei enthält ein Makro, das im System des Benutzers Dateien löscht, sobald er die Textdatei zum Lesen öffnet.
- DoS-Angriffe (DoS = Denial of Service) zielen darauf ab, das angegriffene System einfach lahmzulegen. Ein Rechner kann z.B. gezielt mit Anfragen bombardiert werden, etwa *ping*-Requests, so dass er nur noch eingeschränkt oder gar nicht mehr seine eigentlichen Aufgaben erledigen kann.

Grundsätzlich lassen sich Sicherheitsrisiken dadurch minimieren, dass man die Komplexität eines Systems so gering wie möglich hält und nur unbedingt benötigte Funktionen installiert.

7.3 Sicherheitsmechanismen in Betriebssystemen

Die Sicherheitsmechanismen eines Betriebssystems sollen seine Objekte vor der Verletzung ihrer Vertraulichkeit und ihrer Integrität in dem Umfang schützen, wie es die Sicherheitspolitik vorgibt. Man unterscheidet drei Arten von Sicherheitsmechanismen:

- Vorbeugende Sicherheitsmaßnahmen,
- Überwachungsmaßnahmen (Auditing),
- Recovery-Maßnahmen.

Vorbeugende Maßnahmen haben zum Ziel, Verletzungen der Sicherheit zu verhindern oder zumindest so zu erschweren, dass ein Angriff sich nicht lohnt.

Überwachungsmechanismen sollen die Verletzung der Sicherheit von Objekten feststellen. Da Angriffe oft nicht beim ersten Versuch erfolgreich sind, kann eine Überwachung kritischer Aktivitäten auch vorbeugend wirken: Ein Angriff kann entdeckt werden, bevor er sein Ziel erreicht hat.

Recovery-Maßnahmen greifen in dem Fall, dass ein Angriff auf die Sicherheit des Systems erfolgreich war, indem sie den Zustand vor dem Angriff wiederherstellen. Eine einfache Möglichkeit ist eine Sicherung des gesamten Systems auf Band. Dabei ist es aber wesentlich, im Schadensfall den Zeitpunkt des Angriffs zu erkennen, damit beim Backup eine integre Systemversion restauriert werden kann.

Multiuser-/Multitaskingbetriebssysteme verwenden Hardwareunterstützung für unterschiedlich privilegierte Prozessor-Modi und ermöglichen damit eine Trennung von Prozessen. Nur dadurch können die typischen Merkmale klassischer Betriebssysteme realisiert werden, wie z.B.:

- Die Nutzung der privilegierten Befehle des Prozessors ist nur im Systemmodus möglich.
- Prozess-zu-Prozess-Kommunikation ist nur unter Betriebssystem-Kontrolle möglich.
- Der Adressraum fremder Prozesse kann nicht verletzt werden.
- Die Zuteilung von Prozessorleistung wird vom Betriebssystem kontrolliert.
- Hardwarezugriffe (z.B. auf Massenspeicher oder das Netz) sind nur über das Betriebssystem möglich.

Wirksame Sicherheitsfunktionen setzen auch die Einhaltung organisatorischer Rahmenbedingungen voraus. So muss der direkte Zugriff auf die Rechnerhardware für Unbefugte verhindert werden, z.B. dadurch dass der Rechner in einem abgeschlossenen Raum steht. Rechner, die direkt am Arbeitsplatz stehen, sollten mindestens ein physisch abschließbares Gehäuse haben, das auch die Schnittstellen nach außen schützt, sie dürfen nicht über externe Medien bootbar sein und müssen einen Bootschutz haben (z. B. Power-On-Password).

Im Folgenden stellen wir Sicherheitsmechanismen vor, die in heutigen Betriebssystemen üblich sind.

7.3.1 Authentifizierungsverfahren

Als Authentifizierung bezeichnen wir die Feststellung der Identität von Subjekten. Eine eindeutige Identifizierbarkeit der Subjekte ist Voraussetzung für viele weitere Mechanismen in einem Betriebssystem. Einige Beispiele verdeutlichen das:

- Eine benutzerbezogene Abrechnung von Leistungen ist nur sinnvoll, wenn die Identität aller Benutzer eindeutig feststeht.
- Zugriffsrechte auf Objekte vergibt der Eigentümer dieser Objekte. Dessen Identität muss daher außer Zweifel stehen.
- Ein Benutzer, der sich auf einem System einloggt, vererbt seine Rechte an seine Prozesse. Diese besitzen dann die gleichen Privilegien wie der Benutzer selbst.

Einer sicheren und robusten Authentifizierung kommt daher in jedem Betriebssystem eine besondere Bedeutung zu. Je sicherer die gewählte Methode ist, desto aufwendiger ist sie.

Es gibt prinzipiell zwei Arten der Authentifizierung: die *einfache* und die *strenge Authentifizierung*. Während sich bei der einfachen Authentifizierung lediglich der Sender gegenüber dem Empfänger ausweist, kann der Sender bei der strengen Authentifizierung auch die Identität des Empfängers überprüfen, wobei zusätzlich die ausgetauschten Authentifizierungsdaten bei der Übertragung verschlüsselt werden.

Einfache Authentifizierung

Bei der einfachen Authentifizierung werden traditionell Passwörter benutzt, etwa beim Login-Vorgang auf einem Rechner. Das Subjekt gibt dabei eine Information preis, die nur es selbst besitzt, nämlich das Passwort. Die Sicherheit des Systems hängt hier wesentlich von der Geheimhaltung und der Qualität der Passwörter ab.

Durch Preisgabe, Erraten oder Ausspähen von Passwörtern sowie durch Entschlüsseln der Passwortdatei können Angreifer diesen Sicherheitsmechanismus durchbrechen.

Mechanismen, die die Sicherheit dieser einfachen Authentifizierung verbessern, sind One-Time-Passwörter, SmartCards und biometrische Verfahren:

- One-Time-Passwörter sind nur ein einziges Mal gültig und bieten damit einen guten Schutz gegen Abhören des Netzverkehrs. Dazu wird z.B. aus der aktuellen Zeit und einem geheimen Schlüssel ein einmaliges Passwort gebildet. Dieses ändert sich regelmäßig (etwa einmal pro Minute) und wiederholt sich niemals. Die Gegenseite überprüft den Benutzer, indem sie mit einer Kopie des geheimen Schlüssels und der aktuellen Zeit das gleiche Passwort bestimmt und beide Passwörter vergleicht. Eine weitere Verbesserung des Verfahrens verlangt zusätzlich die Eingabe einer persönlichen Identifikationsnummer (PIN). Eine kommerzielle Software-Lösung zur Authentifizierung mit One-Time-Passwörtern ist S/Key (s. Abschnitt 7.6.5).
- Technisch lassen sich solche Verfahren mit SmartCards realisieren. Diese sind durch den auf ihnen enthaltenen Mikrochip in der Lage, eine einfache Autorisierung im Dialog mit dem Zielrechner durchzuführen. Der Hauptvorteil ist, dass der geheime Schlüssel in der Karte abgelegt werden kann und nicht auf dem Rechner des Benutzers gespeichert werden muss.
- Biometrische Verfahren überprüfen die Identität von Personen durch die Messung unverwechselbarer biologischer Parameter. In Frage kommen dafür z.B. Fingerabdrücke, eine Stimmenanalyse oder eine Unterschrift. Es sind dazu spezielle Geräte erforderlich, was den Einsatz dieser Verfahren beschränkt. Die natürlichen Veränderungen der Parameter, z.B. der Stimme oder der Unterschrift erzwingen eine gewisse Toleranz der Authentifizierungsverfahren, was man als ein Risiko ansehen kann. Eine kommerzielle Lösung für die Identifikation mit Hilfe von Fingerabdrücken ist Finger-ID (s. Abschnitt 7.6.6)

Bei allen einfachen Authentifizierungsverfahren wird nur die Identität eines Subjekts überprüft. Das Subjekt selbst hat aber keine Möglichkeit, die Identität der Gegenseite zu verifizieren.

Strenge Authentifizierung

Bei der strengen Authentifizierung wird im Gegensatz zur einfachen die Vertraulichkeit der übermittelten Information durch Verschlüsselung gesichert. Zusätzlich erhalten die beteiligten Subjekte die Möglichkeit, sich gegenseitig zu überprüfen. Die dabei eingesetzten Verfahren sind:

- *Symmetrische Verschlüsselung*

  Dabei wird von den Partnern derselbe geheime Schlüssel verwendet.

- *Asymmetrische Verschlüsselung*

  Der Sender benutzt dabei den öffentlich bekannten Schlüssel des Empfängers und dieser muss zur Entschlüsselung seinen eigenen, geheimen Schlüssel anwenden.

Für eine ausführliche Darstellung von Verschlüsselungsmethoden wird auf Kapitel 6 verwiesen.

Produkte für die Authentifizierung

- *RADIUS*

  RADIUS (Remote Authentication Dial-In User Service) ist ein System mit einer Authentifizierungsdatenbank, das eine einfache Authentifizierung auf der Basis von Login-Identifiern und Passwörtern durchführt. Es kann für jeden Benutzer individuell eingestellte Rechte enthalten, unterstützt Passwort-Alterung und gibt Benutzern die Möglichkeit, ihre Passwörter zu ändern (dies allerdings nur in der kostenpflichtigen Vollversion). Die Kommunikation zwischen den Clients und der RADIUS-Datenbank erfolgt dabei verschlüsselt mit einem RSA-Verfahren (RSA MD5). RADIUS wird häufig zusammen mit Remote-Access-Servern eingesetzt.

- *Kerberos*

  Kerberos wurde am MIT im Rahmen des Athena-Projekts für die strenge Authentifizierung und die verschlüsselte Kommunikation zwischen Partnern in einem unsicheren Netz entwickelt. Kerberos basiert auf einem zentralen Authentifizierungsserver, der für alle Clients (principals) ein individuelles, geheimes Passwort kennt. Will ein Client mit einem anderen Client kommunizieren, lässt er sich vom Authentifizierungsserver ein Ticket ausstellen, mit dem er sich ausweisen kann und das einen Session Key für die gesicherte Kommunikation zwischen den Clients enthält. Zu keiner Zeit werden dabei unverschlüsselte Informationen über das Netz ausgetauscht.

7.3.2 Zugriffskontrolle

Die Sicherheit der Objekte in einem System wird durch Zugriffskontrollmechanismen geregelt. Diese bestimmen, welche Subjekte auf ein Objekt zugreifen und welche Operationen sie darauf anwenden dürfen. Dabei unterscheidet man zwei Strategien, die oft auch gemischt im selben System eingesetzt werden:

- *Diskrete Zugriffskontrollen*

  Sie überlassen dem Eigentümer eines Objekts die Entscheidung darüber, welche Subjekte darauf zugreifen dürfen und welche Operationen damit erlaubt sind.

- *Globale Zugriffsmodelle*

  Diese geben organisatorische Richtlinien für den Zugriff auf Objekte vor, die auch für deren Eigentümer bindend sind. Sie sind sinnvoll in Systemen, bei denen eine hohe Sicherheit garantiert werden soll.

Operationen, die beim Zugriff kontrolliert werden, sind z.B. das Lesen, Schreiben, Löschen und Aufrufen als Programm. Übliche Techniken zur Implementierung von Zugriffskontrollen sind:

- *Gruppen*

  Die Subjekte eines Systems werden in Gruppen eingeteilt. Der Zugriff auf ein Objekt hängt dann nur noch von der Gruppenzugehörigkeit des zugreifenden Subjekts ab.
- *Access-Listen*

  Diese sind einem Objekt zugeordnet und spezifizieren, welche Subjekte oder Subjekt-Gruppen auf dieses Objekt zugreifen dürfen und welche Operationen damit erlaubt sind.
- *Rechte-Listen*

  Diese sind den Subjekten zugeordnet und spezifizieren, auf welche Objekte sie zugreifen dürfen.
- *Zugriffspasswörter*

  Diese werden den Objekten zugeordnet. Ein Subjekt, das auf ein Objekt zugreifen will, muss dessen Passwort vorweisen.

Ein umfassendes Zugriffsrecht, wie es unter UNIX der Superuser *root* besitzt, stellt ein erhebliches Gefährdungspotential dar. Dieser Gefahr kann eine Aufsplittung der Superuser-Rechte entgegenwirken: Durch die Definition unterschiedlicher Rollen mit genau festgelegtem Berechtigungsprofil wird eine Beschränkung der Rechte auf den jeweils benötigten Umfang erreicht. Eine Implementierung dieses Modells ist z.B. der Capability-Access-Control-Mechanismus im UNIX-Derivat Secure DG/UX von Data General.

Eine ausführliche Darstellung der Zugriffskontrollmechanismen enthält Kapitel 8.

7.3.3 Separationsmechanismen

Systeme, in denen Objekte mit differenzierten Sicherheitsanforderungen und Subjekte mit unterschiedlichen Rechten existieren, benötigen Separationsmechanismen, mit denen die Beziehungen aller Subjekte und Objekte kontrolliert werden können. Wir unterscheiden dabei:

- *Physische Trennung*

  Die einfachste und sicherste Methode ist die physische Trennung von Systemen nach Sicherheitsaspekten. Entweder werden für kritische Anwendungen isolierte Rechner betrieben oder mehrere virtuelle Maschinen auf derselben Hardware.
- *Zeitliche Separation*

  Bevor sicherheitskritische Applikationen ins System eingespielt werden, werden alle anderen Aktivitäten gestoppt.

- *Kryptographische Separation*

  Subjekte und Objekte unterschiedlicher Sicherheitsstufen werden durch Verschlüsselung gegeneinander geschützt.

- *Logische Separation*

  Damit wird erreicht, dass Subjekte nur die Objekte in ihrer Umgebung vorfinden, auf die sie legalerweise Zugriff haben. Beispiele logischer Separation sind getrennte virtuelle Adressräume, hierarchische Abstufung von Privilegien für Prozesse sowie die Zugriffskontrolle durch Referenz-Monitore.

  Ein Referenzmonitor (Trusted Computing Base, TCB) ist eine Komponente des Betriebssystems, in der alle Zugriffskontrollen konzentriert sind. Sie ist relativ kompakt und somit lässt sie sich leichter vollständig analysieren. Andererseits bedeutet ein Versagen der TCB den vollständigen Verlust der Systemsicherheit.

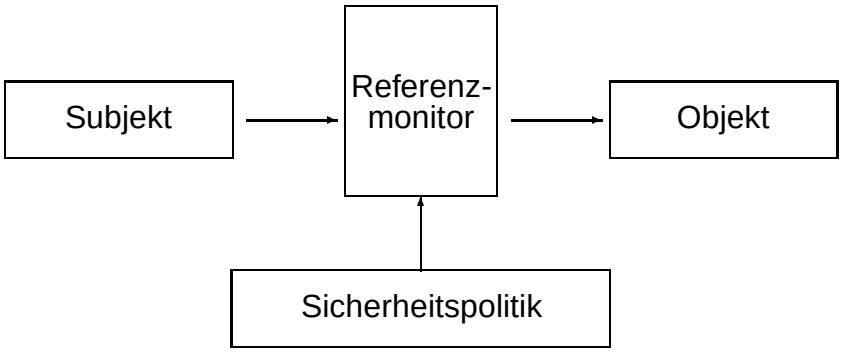


Abbildung 7.1: Referenzmonitor

Referenzmonitore werden nicht nur beim Zugriff auf Datenobjekte eingesetzt, sondern auch zur Kontrolle anderer Auftragsbeziehungen. Einer der ältesten Mechanismen dieser Art sind Supervisor Calls (SVC):

- Ein nichtprivilegierter Prozess verlangt vom System die Ausführung einer privilegierten Funktion.
- Der SVC entzieht als software-generierte Unterbrechung dem Auftraggeber die Kontrolle.
- Das Betriebssystem überprüft, ob der Auftrag berechtigt ist, führt ihn aus oder weist ihn ab.

7.4 Sicherheitsaspekte heutiger Betriebssysteme

In diesem Abschnitt betrachten wir die wesentlichen Sicherheitsaspekte für die Betriebssysteme WINDOWSNT und UNIX. Als zusammenfassende Wertung dieser Gegenüberstellung ist vorab festzuhalten,

- dass beide Systeme potentielle Sicherheitslücken besitzen, die erfahrene Administratoren erfordern,
- dass die Schwachstellen bei UNIX besser bekannt sind, weil das System schon über einen längeren Zeitraum im Einsatz ist, eine größere Verbreitung hat und der Source Code bekannt ist,
- dass eine permanente Verfolgung der von Computing Emergency Response Teams (CERTs) und anderen Organisationen verbreiteten Berichte über neu bekannt gewordene Sicherheitslücken für beide Betriebssysteme unabdingbar ist.

7.4.1 Windows NT

Das Betriebssystem WINDOWSNT hat eine Zertifizierung (siehe Kapitel 12) der Klasse C2 gemäß den „Trusted Computer System Evaluation Criteria“ des amerikanischen Verteidigungsministeriums erhalten in Bezug auf die Bereiche

- *diskrete Zugriffskontrolle*

  Der Eigentümer kann Zugriffe auf seine Objekte kontrollieren.
- *Identifikation und Authentifizierung*

  Benutzer weisen durch Account-Namen und Passwort ihre Identität nach. Das System kann damit die Aktivitäten der Benutzer verfolgen.
- *Object Reuse*

  Die Daten eines Prozesses im Arbeitsspeicher sind anderen Prozessen nicht zugänglich. Ebenso sind die Informationen einer Datei nach Löschen nicht mehr zugänglich.
- *Auditing*

  Kritische Aktionen können protokolliert werden und bei Bedarf können Alarme ausgelöst werden.

Die Zertifizierung gilt nur für Stand-alone-Konfigurationen. Für einen Einsatz von WINDOWSNT als Netzbetriebssystem gilt sie nicht (siehe Kapitel 12.2.4).

Positive Aspekte der Sicherheit von WINDOWSNT sind die folgenden:

- Die Mechanismen sind im Betriebssystem integriert. Damit kommt es durch Versionswechsel beim Betriebssystem nicht zu Inkompatibilitäten zwischen diesem und aufgesetzten Mechanismen.
- Es gibt abgestufte Rechte für den Zugriff (Read, Write, Execute, Delete, Change Permissions, Take Ownership).
- Auf Betriebssystem-Aktionen können abgestufte Rechte vergeben werden (z.B. Debugging erlaubt).
- Durch Access-Listen werden Sicherheits-Attribute direkt an die Objekte gebunden.
- Detailliertes Auditing
- Die graphische Benutzerschnittstelle kann auf die Funktionen reduziert werden, die der Benutzer auch verwenden darf.

- Ab der Version 4.0 verfügt WINDOWSNT über das Point-to-Point-Tunneling-Protokoll. Damit lassen sich gesicherte Verbindungen zwischen einem Client und einem Server über öffentliche Netze realisieren.

Allerdings hat WINDOWSNT auch Schwachpunkte, z.B. die folgenden:

- Die Struktur des NTFS-Dateisystems ist zwar nicht offengelegt, die Daten können aber trotzdem gelesen werden, z.B. mit einer DOS-Boot-Diskette und dem Shareware-Tool NTFSDOS.EXE.
- Mit der unter WINDOWSNT erstellten Emergency Repair Disk kann man das System booten und unter Umgehung der Sicherheitsmechanismen von NTFS auf die Dateien zugreifen.
- WINDOWSNT besitzt selbst keine Verschlüsselungsmechanismen für die Speicherung von Daten oder den Datenaustausch.
- Die Anzahl von Fehlversuchen beim Login lässt sich nicht beschränken.
- CD-ROMs und MO-Disks verfügen nicht über die Sicherheitsmechanismen des NTFS, so dass sich darüber unkontrolliert Daten in ein System einschleusen lassen. Insbesondere kann man von einer CD aus eine Installation durchführen und damit alle Sicherheitseinstellungen ausschalten.
- Die seriellen Schnittstellen sind ungesichert, so dass darüber Informationen eingeschleust werden können.
- Es lässt sich nicht erzwingen, dass bestimmte Daten nur mit bestimmten Programmen bearbeitet werden dürfen, z.B. Buchhaltungs-Daten nur mit der Anwendung FIBU, wie das unter VMS mit *Rights Identifiers* möglich ist.

7.4.2 Unix

Wie bei den meisten anderen Betriebssystemen standen beim Design von UNIX Sicherheitsaspekte nicht im Vordergrund. Die wichtigsten im System integrierten Schutzmechanismen sind

- *Passwort-Schutz*

  Passwörter werden im System gespeichert, wobei zunächst das Benutzerpasswort um eine Zufallszahl ergänzt und dann nach dem DES-Standard verschlüsselt wird. Zusätzlich werden die Passwortdateien durch Zugriffsbeschränkungen geschützt.

- *Zugriffsschutz*

  UNIX bietet eine diskrete Zugriffskontrolle auf Objekte mit abgestuften Rechten (*read, write, execute*) für die Benutzergruppen *user*, *group*, *other*.

- *Auditing*

  Die Möglichkeiten zum Erstellen von Protokolldateien sind unter UNIX sehr umfangreich und flexibel einstellbar. Weitere Auditingfunktionen melden einem Benutzer beim Login den Zeitpunkt des letzten Login unter seiner Kennung oder geben Auskunft über die aktiven Benutzer im System (*who*-Kommando).

Gleichzeitig enthält UNIX aber Mechanismen, die diesen Schutz außer Kraft setzen können, wenn sie von unerfahrenen oder nachlässigen Administratoren bzw. Benutzern verwendet werden, z.B.

- *Sonderfunktionen beim Zugriffsschutz*

  Im UNIX-Dateisystem können Benutzer erlauben, dass für den Zugriff auf ihre Objekte die Rechte des Eigentümers statt der fremder Subjekte maßgebend sind. Damit können gefährliche Rechtebeziehungen entstehen, die sich kaum überblicken lassen.
- *Network File System (NFS)*

  NFS erlaubt transparenten Zugriff auf verteilte Ressourcen in einem Netz, u.U. auch schreibenden Zugriff auf die Dateien fremder Benutzer. Wenn dadurch die *.rhost*-Datei eines anderen Benutzers verändert wird, ist ein *rlogin* mit dessen Kennung ohne Authentifizierung möglich. Dieser Mechanismus war z.B. die Ursache für die schnelle Ausbreitung des „Internet Worm“.
- *uucp und E-Mail*

  UNIX to UNIX Copy (uucp) ist ein UNIX-Mechanismus zum Austausch von Dateien zwischen UNIX-Systemen, u.a. von E-Mail. Durch Nachlässigkeit bei der Konfiguration von uucp können jedoch leicht ernsthafte Gefährdungen der Systemsicherheit entstehen, z.B. wenn fremden Maschinen der lesende Zugriff auf das eigene Filesystem nicht beschränkt wird, wenn keine Passwort-Authentifizierung von ihnen verlangt wird, oder wenn mit UNIX to UNIX Execute (uux) remote execution erlaubt wird.
- *FTP und TFTP*

  Mit den Protokollen FTP (File Transfer Protocol) und TFTP (Trivial File Transfer Protocol) können Dateitransporte zwischen Systemen durchgeführt werden. Im Fall von TFTP und anonymous FTP geschieht dies sogar, ohne dass die fremden Benutzer sich ausweisen müssen. Bei nachlässiger Konfiguration kann dabei das ganze Dateisystem für diese sichtbar und kopierbar sein.

Über solche unzureichende Zugriffskontrollen hinaus ist aber oft auch der praktisch nicht vorhandene Schutz vor unkontrolliertem Ressourcen-Verbrauch einzelner Prozesse problematisch.

7.5 Sicherheitsaspekte bei Standard-Anwendungen

An zwei typischen Beispielen, nämlich ORACLE und SAP R/3 werden nun Sicherheitsaspekte von Standard-Applikationen vorgestellt.

7.5.1 Oracle

Die Sicherheit ihrer in Datenbanken gespeicherten Informationen ist heute für viele Organisationen lebenswichtig. Der Schutz dieser Informationen vor Missbrauch, Verlust usw. hat

einen entsprechend hohen Stellenwert. Wichtige Aspekte der Datenbank-Sicherheit sind z.B.

- Der Zugang zu den Dateien einer Datenbank muss kontrolliert werden. Dies kann über die Zugriffskontrollmechanismen der Betriebssysteme und die zusätzliche Authentifizierung beim Datenbank-Prozess erreicht werden.
- Falls Daten beim Zugriff über ungesicherte Netze transportiert werden, müssen sie verschlüsselt übertragen werden.

ORACLE bietet mit der *Advanced Networking Option* ein umfangreiches Paket von Funktionalitäten an, die über die normale Client/Server-Funktionalität hinaus einen gesicherten Zugriff der Clients auf den Datenbank-Server ermöglichen.

Die wichtigsten Komponenten der Advanced Networking Option sind

- *Enterprise Directory Service Integration*

  Mit SQL*Net sind unternehmensweite Directory Services mit ORACLE-Namen möglich. *Native Naming Adapter* ermöglichen aber auch eine transparente Einbettung von ORACLE in bestehende Directory Services anderer Hersteller. Im Einzelnen werden unterstützt:
  - Sun NIS / Yellow Pages,
  - Novell Directory Services (NDS),
  - Banyan StreetTalk,
  - OSF DCE Cell Directory Services (CDS).
- *Network Encryption Services*

  Diese sichern die Vertraulichkeit und Integrität der über unterschiedlichste Netze übertragenen Daten. Für die Verschlüsselung werden die RSA-Techniken RC4 und DES eingesetzt, für die jedoch Exportbeschränkungen der USA gelten. Die Verschlüsselung kann vom Server, vom Client oder von beiden verlangt werden. Zur Sicherung der Datenintegrität wird das RSA-Verfahren MD5 eingesetzt. Verletzungen der Datenintegrität werden protokolliert und die betroffene Operation sofort abgebrochen. Außerdem wird Fortezza, der NSA-Standard für Hardware-Verschlüsselung, unterstützt, der auf PC-Einschubkarten basiert.
- *Single-Signon Services*

  Benutzer müssen sich nur einmal pro Sitzung mit ihrem Passwort einloggen. Danach sind Zugriffe auf alle Kerberos- oder SESAME-basierten Dienste möglich, ohne dass eine erneute Passwort-Eingabe verlangt wird.
- *Authentifizierungsverfahren*

  Zusätzlich zur Authentifizierung mit Passwörtern werden weitere Verfahren unterstützt:
  - *Token Authentication* verwendet eine Kombination von Chipkarte und PIN-Nummer,
  - *Biometric Authentication* wertet Fingerabdrücke aus.

7.5.2 SAP R/3

Die Anwendungen und Datenbestände des Systems R/3 sind bei vielen Unternehmen und Organisationen die Basis des gesamten Geschäftsablaufs. Daraus ergeben sich hohe Anforderungen an die Sicherheit und Zuverlässigkeit. Um diese zu erfüllen, werden R/3-eigene Sicherheitsmaßnahmen aber auch Funktionalitäten der darunter liegenden Systemsoftware genutzt, z.B. des Betriebssystems und des Datenbanksystems. Im Einzelnen sind dies:

Maßnahmen auf der Anwendungsebene

- *Sicherung der Datenintegrität*

  Dazu gehören die Prüfung ausgelieferter Datenträger auf Virenbefall, eine Änderungs- und Versionskontrolle, sowie Sperrmechanismen für die Synchronisation gleichzeitiger Zugriffe auf einen Datenbestand.
- *Authentifizierung*

  Die Authentifizierung von Benutzern erfolgt über Passwörter. Dabei können auch im Netz schon bestehende Authentifizierungsverfahren verwendet werden.
- *Zugriffsberechtigungen*

  Rechte zur Durchführung von Operationen auf Objekten werden in den R/3-Benutzerstammsätzen hinterlegt. Zur Vereinfachung der Rechteverwaltung gibt es Berechtigungsprofile, die auch mehreren Benutzern zugeordnet werden können.
- *Protokollierung*

  R/3 verfügt über eine umfangreiche Protokollierung aller Vorgänge im System.

Maßnahmen auf der Netzebene

SAP bietet für die Netzebene keine eigenen Sicherungsmechanismen an, sondern empfiehlt Produkte anderer Hersteller, die teilweise speziell auf R/3 zugeschnitten sind.

- *Firewalls*

  SAP empfiehlt, die Applikations- und Datenbank-Server in einem gesicherten Subnetz zu betreiben. Für die Kommunikation über dieses Subnetz hinaus wird eine Firewall mit einem „SAProuter“ verlangt. Der SAProuter ist ein Proxy-Server, über den die Kommunikation zwischen zwei durch die Firewall getrennten Netzen gelenkt wird.
- *Authentifizierung*

  Für die Authentifizierung von Benutzern wird von SAP Kerberos empfohlen.
- *Verschlüsselung mit* SECUDE

  Das Produkt SECUDE der GMD dient zur Verschlüsselung des Datenverkehrs zwischen einem R/3-Client und dem R/3-Server. Zu Beginn einer Sitzung authentifiziert sich ein Client über eine PIN (personal identification number). Dabei wird ein Public-Key-Verfahren (RSA) eingesetzt, so dass auch die PIN nur verschlüsselt übertragen

wird. Im Verlauf der Authentifizierung wird dann ein Sitzungsschlüssel für die symmetrische Verschlüsselung des Datenverkehrs mit dem DES-Verfahren vergeben.

Maßnahmen auf der Datenbankebene

Dafür stehen keine SAP-eigenen Funktionen zur Verfügung, d.h. es müssen die Schutzmechanismen des Datenbanksystems eingesetzt werden (ORACLE, INFORMIX, ADABAS).

Maßnahmen auf der Betriebssystemebene

In diesem Bereich werden die für das jeweilige Betriebssystem geltenden Sicherheitsmaßnahmen empfohlen (s. Abschnitt 7.4).

7.6 Sichere Kommunikationsprotokolle und Basisdienste

Der Austausch von Objekten zwischen Subjekten innerhalb eines isolierten Rechners stellt bereits ein Sicherheitsrisiko dar. Der Transport von Objekten über Kommunikationsnetze erweitert das Szenario von Bedrohungen aber wesentlich, wenn diese Kommunikationsnetze selbst keine Garantie für die Sicherheit der transportierten Objekte übernehmen können.

Angreifer können Objekte während des Transports verändern, ihre Reihenfolge vertauschen, duplizieren, löschen oder durch andere ersetzen. Die Verschlüsselung von Objekten beim Transport bietet nur einen begrenzten Schutz, weil bereits die Tatsache, dass Objekte überhaupt transportiert werden, eine für Angreifer wertvolle Information darstellen kann.

Im Folgenden betrachten wir Mechanismen, welche die Sicherheit bei der Kommunikation erhöhen.

7.6.1 Schutzmaßnahmen auf der Netzschicht: IPv6

Das zur Zeit noch eingesetzte IP-Protokoll besitzt unterhalb der Applikationsschicht keine Mechanismen zur Sicherung von Integrität und Vertraulichkeit sowie zur Authentifizierung. Das in /RFC1752/ festgeschriebene *IP Next Generation Protocol (IPng, IPv6)* besitzt zwei integrierte Sicherheitsoptionen, die je nach Bedarf einzeln oder zusammen verwendet werden können.

- *Authentication Header*

  Der Authentication Header sichert die Integrität der Kommunikation und dient zur Authentifizierung der Kommunikationspartner. Er ist prinzipiell unabhängig von bestimmten algorithmischen Methoden, es wird jedoch das RSA-Verfahren MD5 als Standard vorgeschlagen, um die weltweite Interoperabilität zu gewährleisten. Damit können zur Zeit noch mögliche Angriffe ausgeschlossen werden, die auf der Behauptung falscher Host-Identität beruhen, z.B. IP-Spoofing. Der Mechanismus beinhaltet

keine Verschlüsselung und unterliegt daher auch keinen Export-Beschränkungen seitens der USA.

- *Encapsulating Security Payload Header (ESP)*

  Mit diesem Mechanismus kann die Integrität und Vertraulichkeit der Kommunikation erreicht werden. Der ESP kann entweder Segmente auf der Transportschicht (transport-mode ESP) oder ganze IP-Pakete (tunnel-mode ESP) verschlüsseln.

  Mit dem transport-mode ESP-Mechanismus werden nur die Daten verschlüsselt, die in den IP-Paketen transportiert werden. Normalerweise sind dies TCP- oder UDP-Segmente auf der Transportschicht. Das Verfahren bietet somit Vertraulichkeit für beliebige Anwendungen, ohne spezielle Maßnahmen auf der Applikationsschicht zu erfordern. Es verhindert aber nicht die Analyse des Datenverkehrs, weil Absender- und Empfängeradressen unverschlüsselt übertragen werden.

  Das tunnel-mode ESP-Verfahren verschlüsselt ganze IP-Pakete, um auch eine Analyse des Datenverkehrs unmöglich zu machen. Dabei wird der ESP-Header dem IP-Paket vorangestellt; seine hinteren Felder und das gesamte IP-Paket werden verschlüsselt. Dieser Block wird mit einem neuen IP-Header ausgestattet, der nur die für das Routing notwendigen Informationen enthält. Der Mechanismus eignet sich somit zur Realisierung Virtueller Privater Netze. Um Interoperabilität zu garantieren, müssen alle Implementierungen das Verfahren DES-CBC (Data Encryption Standard-Cipher Block Chaining) unterstützen.

7.6.2 S-HTTP

Das Secure HTTP-Protokoll (S-HTTP) ist eine Erweiterung des HTTP-Protokolls auf der Applikationsschicht. Es ermöglicht im WorldWideWeb eine gesicherte Kommunikation zwischen einem HTTP-Server und einem HTTP-Client, wobei eine Palette unterschiedlicher Sicherungsmechanismen angeboten wird, z.B.:

- digitale Unterschriften,
- einseitige oder gegenseitige Authentifizierung,
- kryptographische Verfahren, u.a. symmetrische Verschlüsselung, Public Keys und Kerberos-Tickets.

Die Verwendung von Secure HTTP erfordert eine Erweiterung der Syntax von HTML-Dokumenten. Falls einer der beiden Partner das S-HTTP-Protokoll nicht beherrscht, können sie trotzdem miteinander kommunizieren. Dabei entfallen allerdings die Sicherheitsmechanismen, u.U. sogar ohne dass die beteiligten Partner dies bemerken.

Das S-HTTP-Protokoll wurde ursprünglich von EIT und RSA gemeinsam entwickelt. Ein kommerziell verfügbares Toolkit enthält Funktionen, mit denen S-HTTP in WWW-Server und -Clients integriert werden kann.

7.6.3 SSL – SSLeay, Apache-SSL

Das Protokoll SSL (Secure Sockets Layer) wurde von der Netscape Communications Corporation und Verisign (RSA) für eine gesicherte Kommunikation zwischen WWW-Browsern und -Servern entwickelt. Es hat den Status eines IETF-Entwurfs und ist in vielen WWW-Servern und den wichtigsten WWW-Browsern integriert, z.B. dem Netscape Navigator und dem Microsoft Internet Explorer. Der Hauptzweck ist die gesicherte Übertragung von Kreditkarten-Informationen bei kommerziellen Transaktionen.

Ziele des SSL-Protokolls sind:

- Eine gesicherte Kommunikation zwischen je zwei Partnern,
- Interoperabilität zwischen SSL-fähigen Programmen unterschiedlicher Hersteller,
- Erweiterbarkeit, wenn künftig bessere Verschlüsselungsmethoden gefunden bzw. erlaubt werden.

Wesentliche Merkmale des SSL-Protokolls sind:

- Die Partner können sich optional gegenseitig authentifizieren. Dazu wird ein asymmetrisches Verfahren mit öffentlichen Schlüsseln verwendet.
- Für den eigentlichen Datenaustausch wird eine symmetrische Verschlüsselung mit einem geheimen Schlüssel verwendet.
- Das Protokoll setzt unmittelbar auf der TCP-Transportschicht auf und ist damit für höhere Schichten transparent.

Die Kommunikation zwischen WWW-Browser und -Server beginnt mit einem Handshake-Protokoll, mit dem auf gesicherte Datenübertragung umgeschaltet wird. Beim Netscape-Browser wird dabei das links unten im Fenster dargestellte, gebrochene Schlüsselsymbol ungebrochen dargestellt und am oberen Rand der Seite erscheint eine blaue Linie.

Server-Betreiber, die eine SSL-gesicherte Übertragung anbieten wollen, müssen sich bei einer Certification Authority (z.B. Verisign) registrieren lassen. Diese überprüft den Betreiber und teilt ihm ein Zertifikat zu. Bei der Installation des SSL-Moduls auf dem Server wird das Zertifikat verwendet und es werden ein öffentlicher und ein privater Schlüssel für das Handshake-Protokoll generiert. Die sitzungsspezifischen geheimen Schlüssel für den Datenaustausch mit Clients werden dynamisch erzeugt.

SSLeay, Apache-SSL

Außer der kommerziellen Implementierung des SSL-Protokolls durch Netscape und Verisign gibt es eine frei verfügbare Implementierung von E.A.Young: SSLeay. Diese Version steht auch für die Integration in kommerzielle Produkte frei zur Verfügung. Ein WWW-Server auf der Basis von SSLeay ist Apache-SSL. Zertifikate für Apache-SSL gibt es nicht direkt von Verisign aber von anderen Certification Authorities.

7.6.4 SSH – F-Secure

SSH (Secure Shell) ist ein Protokoll und eine Referenz-Implementierung mit einem Server-Modul und Client-Modulen, die gesicherte Ersatzfunktionen für *rlogin*, *rcp* und *rsh* bieten. Im Gegensatz zu *rlogin* und *rsh* nutzt SSH jedoch das RSA-Verfahren für die Authentifizierung. Der Zugriff wird nur dem Rechner gewährt, der im Besitz des geheimen RSA-Schlüssels ist. Zusätzlich werden neben RSA-Keys für Rechner auch Schlüssel für Benutzer unterstützt. Nach einer erfolgreichen Authentifizierung werden alle Daten für die Übertragung verschlüsselt, ein Abhören ist somit ebenfalls nicht möglich.

F-Secure ist eine auf dem SSH-Protokoll basierende kommerzielle Produktfamilie. Sie nutzt das SSH-Protokoll sowohl für die gegenseitige Authentifizierung der Kommunikationspartner, wie auch zur Sicherung der Vertraulichkeit und Integrität der ausgetauschten Informationen.

Die Komponenten der F-Secure-Familie sind F-Secure-Server und F-Secure-Clients für die wichtigsten UNIX-Plattformen. Proxy-Server und F-Secure-Clients sind außerdem auch für WINDOWS- und Macintosh-PCs verfügbar.

Das Zusammenspiel der Komponenten verdeutlicht die folgende Skizze.

Der F-Secure-Server stellt dabei zusammen mit dem F-Secure-Client gesicherte Funktionen zur Verfügung für login-Verbindungen, File-Transfer, X11- und andere TCP/IP-Verbindungen über unsichere Netze. Dabei werden eine strenge Authentifizierung der Partner und ein verschlüsselter Datenaustausch verwendet.

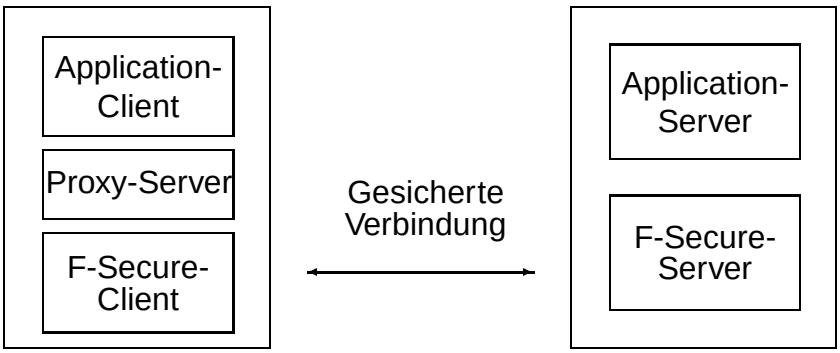


Abbildung 7.2: F-Secure

Das dabei eingesetzte TCP/IP-Port-Forwarding verwendet auf der Client-Maschine einen Proxy-Server, der die Kommunikation zwischen dem Application-Client und dem Server abfängt und über die gesicherte Verbindung umlenkt. Damit ist der Mechanismus für die Applikation transparent, bis auf die Tatsache, dass sie statt für den entfernten Applikationsserver auf den lokalen Proxy-Server hin konfiguriert wird. Die bisher unterstützten Dienste sind *rsh*, *rlogin*, *rcp*, *rdist*, *X11* sowie *telnet*.

7.6.5 S/Key

S/Key ist eine auf One-Time-Passwörtern aufbauende Software-Lösung für die Authentifizierung. Das Verfahren läuft dabei folgendermaßen ab:

- Im Rahmen der S/Key-Authentifizierung präsentiert der Server dem Client einen Challenge-String, der einen Login-Zähler, einen Basisstring (seed) und das zu verwendende Hash-Verfahren enthält. Der Zählerwert wird bei jedem Login-Vorgang um 1 herabgesetzt.
- Zusammen mit dem geheimen Passwort des Benutzers wird dann von der Client-Software die Hash-Funktion so oft iteriert, wie der aktuelle Zählerwert angibt. Der dabei entstehende Key wird zum Host übertragen, der die Hashfunktion noch einmal darauf anwendet und prüft, ob das Ergebnis mit dem Key der vorhergehenden Sitzung übereinstimmt. Ist dies der Fall, dann ist die Authentifizierung erfolgreich. Der aktuelle Key wird im Host gespeichert und beim nächsten Login zum Vergleich herangezogen.
- Bei der erstmaligen Verwendung oder vor Ablauf des Zählers muss ein neues geheimes Passwort generiert werden. Dieses wird dann solange unverändert benutzt, bis der Zähler abgelaufen ist, um daraus in jeder Sitzung neue Keys zu erzeugen. Das geheime Passwort selbst wird weder im Client-Rechner gespeichert noch über das Netz übertragen.

Verfügbarkeit von S/Key-Implementierungen:

- kommerzielle Implementierung von Bellcore (auch für Hochschulen kostenpflichtig): für die Serverplattformen AIX, HP-UX, SunOS, SOLARIS, IRIX, WINDOWSNT und für die gleichen Clientplattformen und zusätzlich für WINDOWS- und Macintosh-Clients;
- Freeware-Implementierungen: für die verschiedenen UNIX-Plattformen, nicht für WINDOWS.

7.6.6 Finger-ID

Ein Beispiel für biometrische Verfahren ist Finger-ID, eine Entwicklung des Fraunhofer-Instituts für Produktionsanlagen und Konstruktionstechnik (IPK) in Berlin. Dieses Verfahren basiert auf Methoden der Mustererkennung und der mathematischen Morphologie. Ein Fingerabdruck wird dabei durch einen Satz von Merkmalen beschrieben und gespeichert. Bei der Authentifizierung von Personen werden die Merkmale ihres Fingerabrucks mit den gespeicherten Merkmalen verglichen.

7.7 Empfehlungen zu sicheren Betriebssystemen und Basisdiensten

- **Notwendige Schutzlevel**

  Sicherheitsziele können nur schrittweise erreicht werden. Es sollten daher die folgenden Prioritäten beachtet werden:

  1. Priorität: Sicherung von Vertraulichkeit und Integrität gespeicherter Daten auf Servern unter den Bedingungen des lokalen Betriebs.
  2. Priorität: Server sind nach außen zu schützen, gegen unberechtigten Zugang und Denial-of-Service-Angriffe.
  3. Priorität: Applikationen sind gegen unberechtigte Benutzung zu sichern.
  4. Priorität: Die Integrität übertragener Daten ist zu gewährleisten.
  5. Priorität: Die Vertraulichkeit übertragener Daten ist zu wahren.

- **Absicherung der Unix/NT-Server unter den Bedingungen des lokalen Betriebs**

  Für berechtigte Benutzer sind die in den Betriebssystemen vorhandenen Schutzmechanismen zur Authentifizierung sowie zur Sicherung von Vertraulichkeit und Integrität der gespeicherten Daten konsequent anzuwenden. Vom DFN-CERT empfohlene Sicherheitspatches sind umgehend zu übernehmen.

- **Absicherung der Unix/NT-Server nach außen**

  Die Server sind konzentriert aufzustellen und in gesicherten Subnetzen zu betreiben. Alle nicht unbedingt nötigen Dienste sind von den Servern zu entfernen. Als aktive Maßnahmen gegen Angriffe kommen in erster Linie infrage:

  - Zulassen von Verbindungen ausschließlich von wohldefinierten Rechnern aus (TCP-Wrapper),
  - Paketfilter mit Auswertung der Logfiles,
  - Einsatz voll ausgebauter Firewall-Systeme.

- **Novell-Server:**

  Die Gefährdung ist wesentlich geringer, weil Angriffe praktisch nur vom lokalen Netz aus möglich sind und das NETWARE Core-Protokoll nicht offengelegt ist. Ein weiterer Vorteil ist, dass Novell-Passwörter von den Novell-Clients verschlüsselt werden.

- **Authentifizierungsverfahren**

  Normaler Passwortschutz ist erfahrungsgemäß praktisch wirkungslos, gerade bei unerfahrenen Benutzern. Daher sollte im Verwaltungsbereich eine wirkungsvollere Authentifizierungsmethode eingesetzt werden, z.B.

  - SSH (siehe 7.6.4)
  - S/Key (siehe 7.6.5)

- **E-Mail**

  Für den Versand vertraulicher Informationen per E-Mail ist PGP ein sicheres Verfahren. Die Handhabung muss für die Anwender aber künftig noch vereinfacht werden.

- **Sicherung von HTTP-Anwendungen**

  Für gesichert zu betreibende Intranet-Anwendungen ist Apache-SSL eine kostenlose und trotzdem mit umfangreichen Sicherungsfunktionen ausgestattete WWW-Server-Software. Zudem werden kommerzielle SSL-fähige HTTP-Server mit einer Schlüssellänge von 128 Bit für die verwendeten symmetrischen Schlüssel angeboten.

- **Telnet und darauf aufgesetzte Applikationen**

  Unter dem Aspekt des Hijacking von Telnet-Verbindungen sollte eine Absicherung mit SSH erfolgen.

- **Grenzen der Sicherungsmöglichkeiten bei Betriebssystemen**

  Außer den bei ORACLE und SAP R/3 aufgeführten herstellerspezifischen Maßnahmen, die alle teuer sind, sind keine mit geringem Aufwand umsetzbaren Techniken zur Sicherung von Client/Server-Applikationen bekannt. Wenn ein brauchbares Authentifizierungsverfahren implementiert ist, sollte das zunächst ausreichen. Dabei wird natürlich keine Vertraulichkeit und Integrität erreicht.

  Es ist daher zu prüfen, ob Client/Server-Applikationen durch die Implementierung von SSH-Tunnels gesichert oder durch den Einsatz von Krypto-Routern virtuelle private Kanäle realisiert werden können (Siehe dazu Kapitel 4: „Virtualisierung der Netze“ und Kapitel 6: „Verschlüsselung vertraulicher oder sensibler Daten“).

7.8 Literatur

/Aalto/ Aalto, T.:
„IPv6 Authentication Header and Encapsulating Security Payload“,
`http://www.tcm.hut.fi/Opinnot/Tik-110.551/1996/ahesp.html#sources`

/Anderson/ Anderson, M. (Bellcore Corporation):
„S/KEY One-time Password Authentification System“
Release 3.0
`http://www.bellcore.com/BC.dynjava?SKEYRelease3WPBeneralWhitePaper`

/Bacic/ Bacic, E.M.:
„UNIX *Security“,*
`http://www.alw.nih.gov/Security/FIRST/papers/unix/unixsec.ps`

/DARPA/ DARPA/NSA/DISA Joint Technology Office:
„Research Challenges in Operating System Security“,
`http://www.ito.arpa.mil/Proceedings/OS_Security/challenges/challenges.html`

/DFNSSH96/ DFN-CERT:
„SSH (Secure Shell)“,
Informationsbulletin DIB-96:01, Sept. 1996

/ECC/ ECC Engineering Computer Consultants Inc.
`http://www.engcc.com/info/secure.html#Solutions`

/FIRST/ FIRST Security Papers (Literaturverzeichnis)
`http://www.alw.nih.gov/Security/first-papers.html`

/FrKaKo/ Freier, A.O. / Karlton, Ph. / Kocher, P.C.:
„The SSL Protocol, version 3.0“,
Internet Draft, März 1996

/Gigler95/ Gigler, R.:
„Sicherheit in Rechnernetzen“,
Diplomarbeit, FH Regensburg, 1995

/MayRo/ Mayerhofer, J. / Rotter, Chr.:
„Installation, Test und Bewertung von Internet-Sicherheitsmechanismen“,
FH Regensburg 1997
http://homepages.fh-regensburg.de/~maj39316/da/Diplomarbeit/index.html

/Netscape/ Netscape Corporation:
„Securing Communications on the Intranet and over the Internet“,
http://home.netscape.com/newsref/ref/128bit.html#SSL

/NIST94/ National Institute of Standards and Technology:
„An Introduction to Computer Security: The NIST Handbook“,
Juni 1994

/NISTEG/ National Institute of Standards and Technology:
„Executive Guide to the Protection of Information Resources“

/NISTFC/ National Institute of Standards and Technology:
„Federal Criteria for Information Technology Security“, Vol. 1 + 2

/NISTUG/ National Institute of Standards and Technology:
„User's Guide to the Protection of Information Resources“

/ReSchi96/ Rescorla, E. / Schiffmann, A.:
„The Secure Hypertext Transfer Protocol“,
Internet Draft, Januar 1996

/ReSchi96a/ Rescorla, E. / Schiffmann, A.:
„Secure Extension for HTML“,
Internet Draft, Mai 1996

/RFC1752/ RFC 1752:
„The Recommendation for the IP Next Generation Protocol“,

/Ritchie/ Ritchie, D.M.:
„On the Security of UNIX*“,*
http://www.alw.nih.gov/Security/first-papers.html#Unix

/RRZN96/ Regionales Rechenzentrum Niedersachsen:
„Lokale Netze mit Novell Netware 4.1 — Eine Einführung“,
Hannover, März 1996

/UtiNT96/ Utimaco Safeware AG:
„Das WINDOWSNT *Betriebssystem“,*
LOG on 3/1996

/Weck91/ Weck, G.:
„Zugriffskontrolle: Häufig sind die Systeme falsch eingestellt“,
Computerwoche 5/1991

Kapitel 8

Zugangs- und Zugriffskontrollen bei DV-Anwendungen im Klinik-/Verwaltungsbereich

8.1 Problemstellung

Zugang und Zugriff zu Rechnersystemen finden auf folgenden Ebenen statt:

- physischer Zugang zum Rechner oder den Endgeräten oder der Netzverbindung zwischen beiden,
- DV-technischer Zugang zum Rechnersystem,
- Zugriff zu den Ressourcen des Rechnersystems.

Während der physische Zugang zum Rechner in der Regel vergleichsweise einfach zu kontrollieren ist, ist der logische Zugang zum Rechner und seinen Ressourcen über das Netz von irgendeinem Endgerät aus in offenen Netzen nur schwer zu kontrollieren. Die Zugangs- und Zugriffskontrollsysteme in Rechnersystemen wirken nur lokal, d.h. der Rechner oder die Applikation kann immer nur aufgrund der eintreffenden Nachrichten zulassen oder sperren. Das Betriebssystem und/oder die Applikation haben i. Allg. keine Möglichkeit, die Unversehrtheit der eintreffenden Nachricht selbst zu kontrollieren, es sei denn, sie selbst oder ein vorgelagertes vertrauenswürdiges System gewährleisten durch spezielle Techniken die Unversehrtheit aller Nachrichten (siehe Private Virtual Channel in Kapitel 4). Die nachfolgende Beschreibung beschränkt sich auf Techniken, die dem Betriebssystem und/oder der Applikation zur Verfügung stehen, um aufgrund der eingetroffenen (unversehrten) Nachricht Zugang und Zugriff zuzulassen oder zu verweigern.

Der Zugang zu DV-Systemen oder Anwendungen ist zu kontrollieren, weil

- Missbrauch verhindert und/oder
- der Urheber einer Transaktion zweifelsfrei festgestellt werden muss.

Dabei wird Urheber in zweifachem Sinn verstanden:

– als Person, die Rechte an Informationen besitzt,
– aber auch als Verursacher von Transaktionen und Veränderungen an Informationen.

Der Feststellung der Urheberschaft dient das **Authentifizierungsverfahren.**

Authentifizierung in offenen Netzen ist aber nicht nur einseitig vom Nutzer gegenüber dem Server sondern auch umgekehrt notwendig, d.h. auch der Server muss sich gegenüber dem Nutzer zweifelsfrei authentifizieren, damit der Nutzer sicher sein kann, seine Informationen nur dem Server anzuvertrauen, dem er sie geben will.

Wenn ein Nutzer Zugang erhalten hat, so ist diese Identifikation alleine noch nicht ausreichend. Denn ein Informationssystem verwaltet in der Regel multiple Informationen, die nicht immer allen Zugangsberechtigten in gleicher Weise zugänglich sein sollen. Es ist also eine nutzerspezifische Begrenzung des Zugriffs auf die Systemressourcen, Daten, Transaktionen, Systemverwaltungsinformationen und Ein-/Ausgabemedien zusätzlich notwendig (Need-to-Know-Prinzip, Least-Privilege-Prinzip). Zugriffsbegrenzung wird mit sog. **Nutzerprofilen** erreicht.

Die Verwaltung von Zugangs- und Zugriffskontrollen kann manuell und administratorgesteuert oder teilautomatisiert durch Selbstbedienung durch den Nutzer realisiert werden. Nutzerprofile und Authentifizierungsmechanismen und -daten sind besonders vor Zugriffen durch den allgemeinen Nutzer zu schützen. Bei hohen Sicherheitsanforderungen werden solche Daten sogar auf spezielle Server ausgelagert, auf die der allgemeine Nutzer keine Zugangsberechtigung hat. Diese speziellen Ressourcen eines DV-Systems werden u.U. auch nicht einmal den System- und Applikationsadministratoren zugänglich gemacht. Das heißt im Extremfall, dass alle sicherheitsrelevanten Komponenten völlig von den anderen Systemkomponenten (Betriebssystem und Applikationen) separiert werden.

Wesentlicher Bestandteil der Sicherheit eines Zugangs- und Zugriffskontrollsystems ist die laufende Dokumentation aller Zugangs- und Zugriffsaktivitäten (Auditing bzw. Protokollierung), wer wann was ausgelöst und geändert oder zu aktivieren versucht hat. In gewissen Fällen ist diese Dokumentation auch aus rechtlichen, datenschutzrechtlichen und innerbetrieblichen Gründen notwendig. Dies kann z.B. auch schon deshalb erforderlich sein, um das Recht des Urhebers festzuhalten oder den Verursacher zu dokumentieren.

Die Auswertung der Audit-Dokumentation wird immer einem Spezialisten mit besonderen Rechten vorbehalten bleiben. Man wird in Systemen mit hoher Sicherheit den Personenkreis, der Nutzungsrechte verwaltet, strikt vom Personenkreis trennen, der die Dokumentation auswerten darf. Unter Umständen wird die Nutzungsdokumentation verschlüsselt gespeichert, notfalls auf einem separaten DV-System (Audit-Server), um das genannte Ziel zu erreichen. Damit soll verhindert werden, dass Innentäter, wie z.B. Systemadministratoren, unkontrolliert Audit-Daten fälschen oder Personenprofile erstellen können.

Die vorgenannten Aspekte zeigen, dass bei angestrebter hoher Sicherheit eines DV-Systems die Bereiche

- Betreuung des Betriebssystems bzw. der Applikationen,

- Betreuung der Zugriffsrechte bzw. Nutzerprofile zu den Applikationen,
- Zugriffs- und Zugangskontrollen inkl. zweiseitiger Authentifizierung und
- Auditing

personell und technisch strikt getrennt werden sollten.

Die Zugriffskontrolle kann auf drei Ebenen erfolgen, die unterschiedliche Granularität an Sicherheit bieten können:

- Betriebssystem- und Netzebene,
- Applikationsebene / Datenbankebene,
- separate Zugangs- und Zugriffskontrollsysteme.

Dabei sollte Single-Signon ermöglicht werden, d.h. der Benutzer authentifiziert sich gegenüber dem System und allen Applikationen nur einmal.

Die Zugriffsrechte bzw. Nutzerprofile der Applikationen sollten von der Art der Authentifizierung, vom Ausgangspunkt und eventuell vom Zeitpunkt des Zugriffs abhängig gemacht werden können. Beispielsweise sind die Zugriffsrechte der gleichen Person für einen Fernzugriff vom heimischen Arbeitsplatz aus im Vergleich zum dienstlichen Zugriff vom Arbeitsplatz in der Klinik/Verwaltung aus u.U. einzuschränken.

8.2 Systeme und Mechanismen zur Zugangs- und Zugriffskontrolle

Auf Betriebssystem- und Applikationsebene werden diverse Objekte verwaltet. Beispiele von Objekten sind:

- Dateien
- Programme
- Medien (Bänder, Disketten etc.)
- Endgeräte
- Netzschnittstellen
- TCP/IP-Ports
- Datentabellen
- Datensätze
- Datenfelder
- Datenfeldgruppen
- Objektklassen
- Objekte im Sinne der OO-Programmierung
- Mailboxen
- etc.

Diverse Subjekte greifen auf die Objekte mit eventuell zeitlich unterschiedlich eingeschränkten Privilegien und Rechten zu. Die Rechte werden in Nutzerprofilen hinterlegt, die bei Applikationen bis auf Datenfelder und Teilmengen von Datensätzen heruntergebrochen werden können.

Subjekte	Privilegien und Rechte
• Benutzer	• lesen
• Dialog-Prozesse	• schreiben
• Batch jobs	• ausführen
• Remote-Login-Prozesse	• löschen
• RPC-Anfragen	
• UDP-Datagramme	

Diese Zugriffe sind zu verwalten und zu schützen. Dies ist allerdings nur möglich, wenn die Zugriffswege sicher über die Zugriffskontrolleinrichtungen des Betriebssystems oder der Applikation geführt werden. Dies ist bei Zugriffen über RPC, UDP und NFS z.B. nicht generell der Fall. Solche Zugriffswege dürfen deshalb nur innerhalb geschützter Netzinseln, die zum gleichen Betreiber gehören, benutzt werden.

Verwaltung heißt hier, Zugriffsrechte zu vergeben und ihre Vergabe zu dokumentieren. Diese Dokumentation ist zu unterscheiden von der Dokumentation über die Einhaltung der Zugriffsrechte. Diese Feststellung, wer wann in welcher Art auf welches Objekt zugegriffen hat, ist Gegenstand der oben genannten Audit-Dokumentation bzw. Protokollierung.

8.2.1 Mechanismen für die Benutzeridentifikation und Authentifizierung

Die Verbindung zu einer Applikation muss immer nutzerspezifisch sein und den Urheber des Zugriffs eindeutig nachweisen. Es ist nicht ausreichend, wenn die Sicherheitsmechanismen nur endgerätespezifisch funktionieren. Die Identifikation des Endnutzers muss andererseits möglichst einfach sein, um hohe Akzeptanz zu erreichen. Die Nutzeridentifikation kann über permanente, semipermanente und einmalige (token) Passwörter oder PIN (personal identification number) oder mit Hilfe von Medien wie Wallets (tragbare Hardware mit eingebautem elektronischen Schlüssel für Challenge-Response-Authentifizierung), Chipkarten etc. erfolgen. Gefahren bei den Medien liegen im Verlust des Mediums und der missbräuchlichen Nutzung durch Unberechtigte. Man braucht beim Medieneinsatz also wiederum einen Authentifizierungsmechanismus gegenüber dem Identifikationsmedium selbst (z.B. durch PIN).

Bei **Passworttechniken** liegt die Gefahr in der Auswahl leicht zu erratender Passwörter bzw. in der Hinterlegung der schriftlich aufgezeichneten Passwörter am Endgerät. Die heute gängigen Zugangskontrollen der Betriebssysteme und Applikationen unterstützen ausschließlich Passworttechniken, die z.T. dadurch etwas sicherer gemacht sind, dass ein regelmäßiger Passwortwechsel und die Verwendung nichttrivialer Passwörter erzwungen werden kann. Meistens werden diese Techniken aber abgeschaltet bzw. nicht genutzt, weil sich niemand, insbesondere jene nicht, die zu verschiedenen Systemen Zugriff haben

müssen, die sich laufend ändernden und kryptischen Passwörter merken kann. Wenn sie aber auf Merkzetteln hinterlegt werden, ist alle Sicherheit wiederum gefährdet. Deshalb ist die Sicherheit der heute gebräuchlichen Techniken nur in einem geschlossenen Nutzerumfeld, das zudem räumlich abgesichert ist, einigermaßen als sicher einzustufen, nicht aber in einem offenen Umfeld wie z.B. dem Internet, in dem die üblicherweise im Klartext übertragenen Passwörter sehr leicht abgehört werden können.

In einem offenen Umfeld beinhaltet ein Authentifizierungsvorgang die wechselseitige Versicherung, dass am Endgerät ein bestimmter Nutzer anwesend ist und dass dieser Nutzer mit dem von ihm ausgewählten Server auch tatsächlich verbunden ist. Ferner muss streng genommen jedem Authentifizierungsvorgang die wechselseitige Verifikation der im Endgerät und im Zugangsserver geladenen und vertrauenswürdigen Software vorausgehen. Diese Art von Authentifizierung wird in der Regel durch asymmetrische Verschlüsselungsverfahren mit wechselseitigem Austausch von Zertifikaten über die geladene Software (AuthentiCode-Verfahren) erreicht.

Außer bei WINDOWSNT V4.0 ist derzeit diese Art von Authentifizierung auf keinem Betriebssystem und keiner Applikation standardmäßig verfügbar. Bei WINDOWSNT V4.0 ist diese Authentifizierung auch nur gegenüber dem Endgerät realisiert aber nicht gegenüber dem Endnutzer. Auf UNIX-Ebene lässt sich dieselbe Qualität an Authentifizierung durch den zusätzlichen Einsatz sog. Secure-Shell-Techniken (z.B. SSH) erreichen.

Bei einer Integration der Authentifizierung und der Zugangskontrolle zu Anwendungen, die aus Gründen der Akzeptanzerhöhung beim Endnutzer angestrebt werden sollte, müssen die Schlüssel für das asymmetrische Verschlüsselungsverfahren endnutzerspezifisch sein. D.h. es genügt nicht, endgerätespezifische Schlüssel zu verwenden, da mit diesen nur das Endgerät und nicht der Nutzer identifiziert werden kann. Darüber hinaus sollte man keine (endgerätespezifischen) Schlüssel auf einem offen zugänglichen Endgerät speichern. Dies gilt unabhängig davon, wie sicher angeblich Schlüssel auf einem Endgerät hinterlegt werden können.

Benutzerspezifische Zugangsschlüssel können Passwörter, Einmalpasswörter, zugangsdynamisch erzeugte Zugangsschlüssel aus Wallets (Challenge-Response-Verfahren), benutzerspezifische Schlüssel in einer Speicherkarte (oder Magnetkarte) oder besonders schützbare Schlüssel in einer Prozessorchipkarte sein. In einer universitären Umgebung, die weltweiten Zugang ermöglichen will, müssen alle genannten Verfahren gemischt einsetzbar sein. Mit den genannten Verfahren können in Abhängigkeit von den Sicherheitsverfahren, mit denen das Verwaltungs-/Klinikrechnernetz abgesichert wurde, unterschiedliche Sicherheitsstufen erreicht werden. Passwörter und Einmalpasswörter sind wenig sicher, weil sich kein Benutzer applikationsspezifische Passwörter merkt, wenn er auf mehr als eine Applikation Zugriff hat. Dieses Problem kann wesentlich entschärft werden, wenn mit einer Homogenisierungsschicht (Single-Signon) für alle Applikationen nur noch ein Passwort erforderlich ist, wodurch die Gefahr wesentlich verringert wird, dass das Passwort irgendwo für Nichtautorisierte lesbar hinterlegt wird.

Die höchste Stufe der Sicherheit ermöglichen **Prozessorchipkarten.** Geheime und öffentliche Schlüssel für asymmetrische Verschlüsselungsverfahren zur Authentifizierung können

sicher auf Prozessorchipkarten hinterlegt werden. Eine Authentifizierung des Inhabers einer Chipkarte gegenüber der Chipkarte, dass er auch tatsächlich deren Besitzer ist, erfolgt über einen sogenannten PIN-Schutzmechanismus. Auf die Sicherheitsmaßnahmen bei Prozessorchipkarten wird an dieser Stelle nicht gesondert eingegangen.

Bei allen externen Identifizierungstechniken besteht immer die Gefahr des Verlusts. Es muss also eine Instanz geben, die sog. Verlust-/Sperrlisten (black oder white list; revocation lists) der gültigen Chipkarten führt. Der Kartenbesitzer muss jederzeit die Möglichkeit haben, in Selbstbedienung seine eigene Karte zu sperren.

Ferner ist eine Entscheidung zwischen zwei Varianten der Zugangs- und Identitätsüberwachung in einer laufenden Sitzung zu unterscheiden:

- permanente Überwachung durch periodisches Lesen des Identifizierungsmediums während der Sitzung (permanente Reauthentifizierung) und
- einmalige Authentifizierung bei Sitzungbeginn und Reauthentifizierung nur nach einstellbarem Timeout.

Die beiden Strategien sind in unterschiedlichen Anwendungsszenarien in Abhängigkeit von der Nutzerfluktuation am Endgerät einzusetzen.

Sicherer Zugang bei **hohen Sicherheitsanforderungen** setzt nicht nur eine wirksame Zugangsregelung auf oder vor dem Applikationsserver voraus, sondern muss den gesamten Weg vom *Nutzer bis zum Applikationsserver* umfassen. Andernfalls könnte durch diverse Internet-Dienste und Viren der Authentifizierungsmechanismus kompromittiert werden.

Wie bereits in Kapitel 4 erläutert, ist ein sog. Private-Virtual-Channel erforderlich, der mindestens folgende Eigenschaften gewährleistet:

- Datenunversehrtheit bei Übermittlung und Datenspeicherung (data integrity),
- Zweiseitige Authentifizierung der Partner (authentication),
- Nichtanfechtbarkeit einer Transaktion (non-repudiation),
- Kontrolle des eingesetzten Authentifizierungsmediums gegen Missbrauch, Verlust und Vergesslichkeit,
- Zeitkontrolle über offen gelassene Sitzungen, insbesondere bei multifunktionaler Nutzung von Endgeräten,
- Zugangsregelung zu Teilen einer Anwendung; zentrales Konzept für die Zugangskontrolle für alle Applikationen eines Unternehmens oder seiner Bereiche (zentraler Berechtigungsserver oder Hierarchie von Berechtigungsservern und Single-Signon).

Diese hier dargestellten Eigenschaften sind auf Betriebssystem-, Applikations- oder auf einer separaten Ebene erzielbar.

8.2.2 Zugriffskontrolle

Der Zugriff auf Objekte wird durch das Betriebssystem, die Applikationen und durch separate Berechtigungsserver kontrolliert. Die Rolle des Betriebssystems bei der Zugriffskontrolle wurde bereits in Abschnitt 7.3.2 diskutiert.

Applikationsebene

Die auf der Betriebssystemebene verwalteten Objekte sind in der Regel zu grob. Applikationen brauchen wesentlich feinere Objektverwaltung auf Datenfeld- und Transaktionsebene. Deshalb werden auch in Datenbankschnittstellen (z.B. SQL) und in sog. Transaktionsmonitoren (z.B. Tuxedo, CICS, UTM) oder in den Applikationsgeneratoren (siehe Abschnitt 8.3.1) entsprechende Funktionen vorgehalten. Auf dieser Ebene können sog. anwendungsspezifische Nutzungsprofile, d.h. Zugriffs- und Bearbeitungsberechtigungen bis auf Datenfeldebene definiert werden, die dann Benutzern nach individueller Zugangsgewährung zeitlich befristet zugestanden werden.

Separate Berechtigungsserver

Falls es zum Einsatz eines separaten Berechtigungsservers kommt, ist eine Schnittstelle zwischen ihm und der Applikation erforderlich, da die Nutzungsprofile selbst zwar in der Applikation, z.B. auf SQL-Ebene, definiert sind, die Zugangskontrolle und die zeitlich begrenzte Zuordnung eines Nutzungsprofils zu einem konkreten und authentifizierten Nutzer jedoch außerhalb der Applikation erfolgt. Der Einsatz eines separaten Berechtigungsservers ist nur möglich, wenn die real verfügbaren Applikationen eine Schnittstelle zu ihm bereitstellen. Das Ziel ist wünschenswert, aber es ist zu fragen, ob und wann ein solcher Weg verfügbar sein wird.

Das externe Zugangsberechtigungsprüfsystem (z.B. ein Authentifizierungsproxy in einer Firewall) nutzt im Zusammenspiel mit dem Berechtigungsserver die Zuordnung,

- welcher (authentifizierte) Nutzer
- welche (kostenpflichtige) Transaktion
- mit welchem Nutzerprofil
- zu welcher Zeit und
- mit welchen Timeout-Konditionen

ausführen darf. Ferner wird hier eine globale Sperrlistenverwaltung (revocation list) mitgeführt.

Der zweifellos erhöhte Aufwand, der mit der Trennung verbunden ist, wird aber durch die Vereinfachung der laufenden Pflege wieder wettgemacht, wenn der Zugang zu einer heterogenen DV-Landschaft erzielt werden soll. Für die Öffnung einer einzigen Applikation zum Internet lohnt sich der Aufwand nicht. Ebenso lohnt sich der Aufwand nicht, wenn nur wenige Nutzer zu verwalten sind.

Die Zusammenfassung der Zugangs- und Zugriffskontrollfunktionen in einem separierten System lohnt sich dagegen und ist zwingend, wenn Tausende von (sporadischen) Nut-

zern Zugang zu einer heterogenen DV-Landschaft mit einem breiten Applikationsspektrum haben sollen.

8.2.3 Rechteverwaltung

Die in den vorstehenden Abschnitten beschriebenen Zugangs- und Zugriffskontrolltechniken erfordern eine einfache und übersichtliche Möglichkeit der Pflege. Ist der Aufwand groß, wird nur ungenügend genau verwaltet und es werden zu große Berechtigungsspielräume eingeräumt. Deshalb kommt der graphisch unterstützten Pflege der Berechtigungsprofile und der Zugriffsrechte große Bedeutung zu.

Ferner kann es wichtig sein, die Zugangsrechte und die Zugriffsrechte getrennt durch unterschiedliche Personengruppen verwalten zu lassen. In diesem Fall wären zu unterscheiden:

- Personen, die die Nutzerprofile, d.h. Rechte des Zugriffs auf Datengruppen und Ressourcen pro Nutzergruppe, z.B. Studenten, Dozenten, Gasthörer etc. festlegen;
- Personen, die festlegen, welche Authentifizierungsverfahren pro Nutzergruppe unterstützt und mindestens verlangt werden;
- Personen, die festlegen, welche Transaktionen in Abhängigkeit von der vom Nutzer gewählten Authentifizierungstechnik und Tageszeit und Endgerätetyp (d.h. Clientsoftware und Standort) zugelassen werden, d.h. bei Authentifizierung mit Passwort von einem offen zugänglichen Client werden weniger Rechte gewährt als bei Authentifizierung mit Prozessorchipkarte von einem Client, der in einem abgeschlossenen Raum steht;
- Personen, die die Zuordnung des individuellen Nutzers zu Nutzerprofilen in Abhängigkeit von Tageszeit und Applikation festlegen.

Bei einem sehr hohen Bestand an potentiellen Nutzern kann eine manuelle Pflege kaum mehr sinnvoll und mit endlichem Aufwand betrieben werden. Dann sind Automatismen vorzusehen, d.h. Nutzer einer Nutzergruppe erhalten die gleichen Rechte. Davon abweichende Wünsche sind per Selbstbedienung über das Netz an den Berechtigungsserver zu melden und die Sonderwünsche werden dort durch Spezialisten (siehe Abschnitt 8.3) bearbeitet, die aber keinen Zugriff auf die Definition der Nutzerprofile oder pro Transaktion geforderten Authentifizierungstechniken haben.

Die Bedeutung dieser Fragestellung wird daraus ersichtlich, dass immer mehr spezielle Lösungen auf den Markt kommen, mit denen von zentraler Stelle aus diverse Systeme gesteuert werden können (z.B. NDS von Novell, Directory Server unter WINDOWSNT 5.0, Directory-Server von UNISYS, mit LDAP und X.509-Schnittstellen). Diese Systeme bieten in der Regel die Möglichkeit einer HTML-Programmierschnittstelle, um Selbstbedienfunktionen zu ermöglichen (siehe 8.3.1).

8.3 Lösungsmöglichkeiten für Zugriffskontrollen zu unterschiedlichen Anwendungen

8.3.1 Systemvorschläge für Zugangs- und Zugriffskontrollen zu Netzen und Systemen

Wie in Kapitel 11 näher ausgeführt wird, muss zwischen mindestens drei Kategorien von Netzen (Internet, Intranet und Servernetz) unterschieden werden, die ihre getrennten Anforderungen an Zugangskontrollen haben und damit unterschiedliche Lösungen erzwingen oder angeraten erscheinen lassen. Dies legt bereits nahe, nicht alle Sicherheitsfunktionen auf einem System, einem Betriebssystem und/oder einer Applikation, abwickeln zu wollen.

Zugangs- und Zugriffskontrolle auf Applikationen kann nur ein Aspekt der Sicherheitsproblematik sein. Die Sicherung der Netzübergänge (siehe Kapitel 5) ist ein völlig anderer. Es ist anzunehmen, dass in zunehmendem Maße, insbesondere im Zusammenhang mit Electronic Commerce, die Sicherheitskomponenten von Betriebssystemen, Datenbanksystemen und Applikationsgeneratoren an sich verbessert werden. Auch werden zumindest Betriebssysteme zunehmend sicherheitszertifiziert werden, wie in Kapitel 12 näher ausgeführt wird.

Bei großen Applikationssystemen (z.B. SAP R/3) wird in der Regel im Teilhaberbetrieb gearbeitet, wobei Zugriffskontrolle nicht auf der Ebene des Betriebssystems sondern durch spezielle Transaktionsmonitore (Tuxedo, BS2000 UTM, IBM CICS) abgehandelt wird, die aber i. Allg. proprietär und mit dem zugrunde liegenden Betriebssystem sehr verquickt sind. Ferner sind die Datenbankhersteller bemüht, Zugriffskontrollen (Access-Control) auf der Datenbankebene anzubieten. Als Beispiel sei hier die Zugriffskontrolle im SQL-Standard angeführt.

Aus Gründen der Modularität, Skalierbarkeit und Handhabbarkeit bei Releasewechsel u.ä. sollte man aber, wie schon mehrfach erwähnt, Sicherheitsaspekte von den anderen Komponenten eines DV-Systems separieren. Ein deutliches Zeichen für diese Tendenz ist die zunehmende Verfügbarkeit von sog. Directory-Services mit genormten Schnittstellen LDAP und X.509. Sie werden objektorientiert konstruiert, um Erweiterungen mit kundenspezifischen Objekten (siehe unten) zuzulassen. Diese Systeme können verteilt eingesetzt werden. Sie besitzen Authentifizierungs-, Nachrichten- und Datensicherungsmechanismen unter Einsatz von Kryptographie, so dass sie über offene Netze betrieben werden können. Die bereits verfügbaren Novell Directory Services (NDS) sind ein Beispiel und ebenso der Directory Service von Microsoft, der für WINDOWSNT 5.0 angekündigt ist. Ebenso bietet UNISYS Directory Service und Single-Signon-Lösung für WINDOWSNT und gewisse UNIX-Dialekte.

Diese Directory Services sind so konzipiert, dass sie (Zugangs- und) Zugriffskontrollen für heterogene DV-Systeme (Betriebssysteme) von einer logischen Zentrale aus ermöglichen, dabei aber gleichzeitig eine physische Dezentralisierung erlauben. Der NDS z.B. soll künftig die Berechtigungsverwaltung für Novell NETWARE 4.x und SCO-UNIX, HP-UX, Solaris, AIX u.a. übernehmen können. Durch die Schnittstellen (LDAP) sind andere Systeme anbindbar.

Wie bereits mehrfach angemerkt, sollte hohe Sicherheit bei Applikationen durch Separierung von Zugriffskontrollsystemen bzw. Berechtigungssystemen angestrebt werden. Dazu könnte ein sog. Berechtigungsserver dienen, der aber über die Zugriffskontrolle auf Applikationen der DV hinaus noch weitergehende Berechtigungen verwalten kann und sollte.

Die Hochschulen werden zunehmend vor die Notwendigkeit gestellt, immer mehr Dienste und Endgeräte (z.B. Personalcomputer), zu sichernde Labore (Genlabore etc.) den Bediensteten und Studenten zu öffnen. Damit steigt die Gefahr von Diebstahl, Sabotage und Missbrauch. Ferner werden immer mehr DV-Verfahren für die Abwicklung von Verwaltungsvorgängen eingesetzt werden.

Als Beispiele seien hier angeführt:

- Zutritt zu Räumlichkeiten, wie Labore, CIP-Pools, RZ, UB etc.,
- Zugang zu DV wie Compute-Server, NETWARE-Server, CD-ROM-Server, etc.,
- Zugang zu kostenpflichtigen externen Diensten wie Fachinformationszentren,
- Zugang zu Verwaltungsanwendungen in Selbstbedienung wie Studenten- und Prüfungsverwaltung, Veranstaltungsmanagement, UB-Ausleihe, etc. und
- Einzelgebührenerhebung für Drucker-, Kopierernutzung, Nutzungsentgelte für Datenbanken, Mahngebühren etc.

All diese Systeme werden heute zum Teil schon praktiziert, dezentral und unkoordiniert verwaltet und es wird dafür Personal gebunden. Der Aufwand wird in der Regel nicht direkt sichtbar und es ist derzeit nur ein kleiner Prozentsatz der potentiellen „Kunden“ involviert. Wenn es aber dazu kommen sollte, dass alle Studenten und alle Bediensteten eingebunden werden sollen, dann wird der Aufwand auch für die Beratung der „Kunden“ erheblich steigen und zu zukünftigem Personalmehraufwand führen.

Deshalb und aus Gründen verbesserter Sicherheit muss eine logische Zentralisierung und eine Umstellung der Verwaltung von Berechtigungen in der Hochschule auf Selbstbedienung und Automation angestrebt werden. Unter Selbstbedienung und Automation ist hier zu verstehen:

- Berechtigungswunschanmeldung durch den „Kunden“ per E-Mail,
- Freigabe der Berechtigung durch einen Spezialisten der verwaltenden Organisationseinheit der Fakultäten oder Kliniken oder UB oder RZ auf elektronischem Wege,
- Mitteilung der (Nicht-)Durchführung an den Antragsteller per E-Mail,
- automatische Übermittlung des neuen Berechtigungsprofils an das betroffene System (Rechnersystem, DV-Anwendung, Zutrittskontrollsystem, externer Datenbankanbieter etc.),
- automatische Steuerung des Single-Signon,
- Ausgabe von Berechtigungslisten und -profilen,
- automatische Bereinigung bei Exmatrikel bzw. Ende eines Arbeitsverhältnisses,
- Missbrauchserkennung durch Auditing.

Dabei sind weitere Fragen zu klären, z.B. welche Berechtigungsobjekte zu pflegen sind, ob Berechtigungsklassen eingerichtet werden sollen, welche Attribute den einzelnen Berechtigungsobjekten zugesprochen werden, wie z.B. Zeitfenster der Berechtigung, Kostenpflichtigkeit unterschiedlicher Abrechnungsmodelle, Ausschlussregelungen für Nutzergruppen, Sperrkennzeichen, Verlustkennzeichen, Gültigkeitszeiträume etc.

Diese zentralen Funktionen sollten durch einen sog. Berechtigungsserver abgehandelt werden. Der Berechtigungsserver braucht Kopplungen zu diversen vor- und nachgelagerten Systemen.

8.3.2 Bewertung der Lösungsmöglichkeiten

Die bisher dargestellten Lösungsmöglichkeiten haben eine klare Hierarchie.

Bei der Zugangskontrolle kann folgende Stufung gesehen werden, wobei die Auflistung nach zunehmendem Sicherheitsniveau angeordnet ist:

- Firewall für kontrollierten Zugang bei Netzen,
- Benutzerauthentifizierung auf Betriebssystemebene mit unterschiedlich starken Methoden (Passwortmechanismen, verschlüsselte Passwortübertragung, Authentifizierung mit Einsatz von Identifikationsmedien),
- Benutzerauthentifizierung wie vorstehend, aber mit zertifizierten Betriebssystemen,
- Benutzerauthentifizierung wie vorstehend, aber auf Applikationsebene,
- Authentifizierung mit Identifikationsmedien und durchgängige Nutzung eines Private Virtual Channel, separiert von Betriebssystem und Applikation auf einem Spezialsystem (Provider-Gateway, siehe Kapitel 11).

Bei Zugriffskontrollen ist folgende Stufung zu sehen:

- Einsatz zertifizierter Betriebssysteme mit ausgefeilten Zugriffskontrollen (siehe 8.2). Die üblichen Verwaltungsapplikationen sind datenbankorientiert. Deshalb ist das Zugriffskontrollsystem der Betriebssysteme selbst i. Allg. zu grob und ohne Bedeutung.
- Einsatz von Transaktionsmonitoren als Ergänzung zum Betriebssystem,
- Zugriffskontrollsysteme auf Datenbankebene (SQL) und Applikationsgeneratorenebene,
- Einsatz vom Betriebssystem und von der Applikation unabhängiger externer Directory-Services (Berechtigungsserver), die die Zugriffe auf Betriebssystem- und Applikationsebene in einem heterogenen Umfeld von einer logischen Zentrale her unter Zusammenspiel mit den in der Applikation bzw. Datenbank definierten Nutzerprofilen zu steuern gestatten.

Viele Applikationen werden heute noch im sog. Teilnehmerbetrieb gefahren, d.h. jeder Benutzer eröffnet einen Betriebssystemprozess und alle Sicherheitsmechanismen stützen sich auf das zugrunde liegende Betriebssystem. Dies hat zur Folge, dass man auf der Ebene des Betriebssystems durch die Applikation festgelegt ist und damit nur soviel Sicherheit erreichen kann, wie das Betriebssystem bietet. Probleme mit der Sicherheit sind

bei allen Releasewechseln erneut zu untersuchen und zwar bei Releasewechseln des Betriebssystems und der Applikation. Entsprechender Aufwand ist zu treiben. Das betreuende Personal muss weitreichende System-, Netz- und Applikationskenntnisse besitzen.

Daneben gibt es Applikationen, die alle Zugangs- und Zugriffskontrollen selbst enthalten, eigenes Dispatching durchführen und im Grunde nur einen Betriebssystemprozess belegen. Solche Systeme heißen Teilhabersysteme. Sie sind leichter zu handhaben, weil alle Aspekte der Sicherheit in die Applikationsebene (einschließlich Transaktionsmonitor) verlagert sind. Releasewechsel sind weniger gefährlich für die Sicherheit.

Höchste Sicherheit wird bei separaten Zugriffs- und Zugangssystemen erreicht, weil hier Betriebssystem, Applikation und Sicherheitskontrollen unabhängig voneinander und von unabhängigem, eventuell auch externem Personal betrieben werden können. Die Sicherheitseinrichtungen sind unabhängig zertifizierbar. Releasewechsel für Betriebssystem und Applikation und die Auswahl des Betriebssystems, der Applikation und der Sicherheitstechniken und -stärken sind unabhängig voneinander möglich. Die erhöhte Flexibilität bei Technik und Personaleinsatz erhöht die Sicherheit erheblich.

8.3.3 Zusammenfassung

Die Öffnung kritischer Anwendungen wie Patientenverwaltung, Personalverwaltung, Prüfungsverwaltung etc. für Selbstbedienung aus offenen Netzen heraus setzt immer hohe Sicherheit bis hin zur Rechtsverbindlichkeit der Vorgänge voraus.

Damit gelten die eingangs erwähnten Forderungen :

- Betrieb und Betreuung des Betriebssystems,
- Betrieb und Betreuung der Applikation selbst,
- Zugriffs- und Zugangskontrollen inkl. zweiseitiger Authentifizierung und
- Auditing

sollten personell und technisch weitgehend getrennt werden.

Die kurze Begründung hierfür ist, dass man sich nur dadurch gegen Fahrlässigkeit des knappen eigenen Personals und gegen Innentäter sowie Außentäter schützen kann und bei Releasewechsel der Applikationen die Sicherheit nicht gefährdet wird. Ferner kann bei dieser Konstruktion die heute bei Verwaltungsanwendungen noch oft vorzufindende Bindung von Betriebssystem, Datenbanksystem und Applikation mit ihren z.T. unzureichenden Sicherheitsstrukturen überwunden werden.

Im übrigen wird auf die in Abschnitt 11.3 skizzierten Prinzipien, die bei integrierten Lösungen zu beachten sind, und deren Begründung verwiesen.

Die vorstehend aufgeführten Forderungen müssen nicht so hoch getrieben werden, wenn über das Internet nur Sachbearbeiter, d.h. eine geschlossene Benutzergruppe, deren Endgeräte in nicht öffentlich zugänglichen Räumen stehen und deren Endgeräte eventuell gewissen laufenden Kontrollen unterliegen (laufende Virenkontrolle, Verhinderung des Aufspielens nicht zertifizierter Software, Verpflichtung der Nutzer auf Nutzungsordnungen,

etc.), Zugang erhalten sollen. Die Verwendung persönlicher virtueller Kanäle (eventuell Kryptokanäle) ist aber in jedem Fall erforderlich. Es dürfte genügen, diese auf Betriebssystemebene zur Verfügung zu stellen (z.B. WINDOWSNT, Secure Shell bei UNIX). Normale gesicherte Passworttechniken dürften ausreichen. Da hier nur wenige Nutzer pro Applikation zu verwalten sind, ist eine Zugangs- und Zugriffsverwaltung innerhalb des Betriebssystems oder der Applikation durchaus akzeptabel.

Stehen die Endgeräte in einem durch eine Firewall gegen das Internet abgesicherten Verwaltungsnetz, das zum Rechnernetz einen virtuellen Kanal mit Nachrichtenverschlüsselung hat, so kann man weitere Vereinfachungen vorsehen, insbesondere wenn man sich nicht gegen Innentäter zu schützen hat. Diese Annahme widerspricht jedoch der Erfahrung.

8.4 Empfehlungen zu Zugangs- und Zugriffskontrollen

Aus den vorstehenden Ausführungen lassen sich folgende Empfehlungen ableiten, die im BASILIKA-Projekt (Kapitel 11) berücksichtigt werden:

- Trennung des Authentifizierungsvorgangs und der Berechtigungsverwaltung (Nutzer zu applikationsspezifischem Nutzerprofil) von jener der Applikationen und des Betriebssystems, auf dem die Applikationen laufen. Dieses Prinzip wird auch oft unter dem Akronym SSO (Single-Signon) diskutiert.
- Nutzung externer, marktgängiger Berechtigungsserver (z.B. Novell Directory Services) in heterogener Applikationslandschaft bei offenen Benutzergruppen.
- Sicherheitseinrichtungen und insbesondere Berechtigungsserver sollten als blackbox konzipiert werden, die auch von einer externen Institution bereitgestellt und gepflegt werden können. Die Basisadministration wird außer Haus gegeben und einem Spezialisten überlassen. Die Tagesüberwachung erfolgt durch Inhouse-Personal.
- Analog sollte man mit Firewall und Provider-Gateway (siehe Kapitel 11) verfahren.
- Ein möglicher Stufenplan ist in 8.3.2. skizziert worden.

Kapitel 9

Beitrag des Netz- und Systemmanagements zur Systemsicherheit

9.1 Netzmanagement und Sicherheit

9.1.1 Einführung

Netz- bzw. Systemmanagement umfasst die Gesamtheit der Vorkehrungen und Aktivitäten zur Sicherstellung des effektiven und effizienten Einsatzes eines Rechnernetzes bzw. eines verteilten Systems. Die vielfältigen Aufgaben des Managements werden zur besseren Übersicht in Dimensionen gegliedert (Abbildung 9.1). Dargestellt sind die Dimensionen ***Funktionsbereiche, zeitliche Phasen, Ebenen*** (oft auch als Szenarien bezeichnet), **Netztypen** und **Kommunikationsdienste.** Unter der Dimension der Funktionsbereiche werden *Konfiguration, Leistung, Fehler, Sicherheit* und *Abrechnung* zusammengefasst. Die Dimension der zeitlichen Phasen umfasst z.B. *Planung* und *Betrieb* und die Dimension der Ebenen umfasst *Netz-, System-, Anwendungs-* und *Enterprisemanagement.* Die Frage der Sicherheit betreffen insbesondere die Funktionsbereiche der *Konfiguration,* der *Sicherheit,* aber auch der *Abrechnung* in Kombination mit allen anderen genannten Dimensionen.

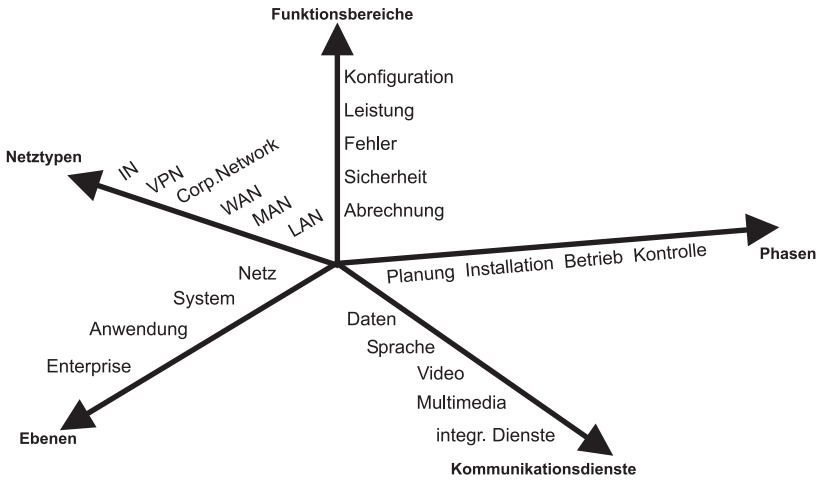


Abbildung 9.1: Aspekte des Netz- und Systemmanagements

Die Verwaltung von Rechnernetzen und Systemen wäre einfacher, wenn alle Bestandteile homogen wären und möglichst von einem Hersteller stammen würden. Theoretische und praktische Probleme entstehen, wenn ganzheitliche, integrierte Managementlösungen für heterogene, offene Systeme (d.h. herstellerunabhängig und produktübergreifend) realisiert werden sollen. Da DV-Strukturen jedoch einem stetigen Wandel unterworfen sind (Austausch veralteter Hardware und Software, Expansion), benötigt man meist nach kurzer Zeit ein Sammelsurium an unterschiedlichen Managementwerkzeugen für die Systeme der einzelnen Hersteller. Deshalb wurden schon frühzeitig von verschiedenen Gremien (ISO, IETF, ITU) Anstrengungen unternommen, um für die mit der Verwaltung beauftragten Personen eine einheitliche und standardisierte, rechnergestützte Umgebung zu schaffen. Dies beinhaltet insbesondere eine Architektur für definierte Modellierung, Gewinnung und Austausch von Managementinformation, aber auch die Integration der einzelnen Managementwerkzeuge in einer gemeinsamen Plattform.

Kommerzielle Lösungen (siehe auch Tabelle 9.1) sind — wenn überhaupt — nur für Teilbereiche der Managementfunktionen verfügbar. Umso wichtiger ist es, bei der Realisierung von Teillösungen ein Gesamtmodell zu verfolgen und dabei integrationsfähige Module auszuwählen.

Integriertes Management (Planung, Organisation und Kontrolle) erfordert nicht nur Aufwand, sondern es kann auch einen Beitrag zur Kostenreduzierung leisten: In Corporate Networks (CN) z.B. können last-, zeit- und tarifabhängig die Leitungen ausgewählt und damit Leitungskosten reduziert werden. Auf diese Weise kann auch die Verfügbarkeit durch Integration von Anwendungen erhöht werden.

Die sich abzeichnende und zunehmende Integration der Kommunikationsdienste in einem Netzverbund erfordert ein Sicherheitskonzept, das dem Benutzer Verfügbarkeit und Sicherheit und dem Betreiber Handhabbarkeit und Kostendeckung garantieren kann. Das Netz- und Systemmanagement kann dazu einen wesentlichen Beitrag leisten.

9.1.2 Konzepte des Netz- und Systemmanagements

Die International Organization for Standardization (ISO) definiert folgende Funktionsbereiche für das Netzmanagement:

- Konfigurationsmanagement:
  Dieser Bereich befasst sich mit dem Aufbau des Rechner- und Kommunikationsnetzes. Die Konfiguration der am Netz angeschlossenen Komponenten und der darauf befindlichen Softwarepakete wird erfasst, überwacht und nach Bedarf modifiziert. Beispiele für zu verwaltende Komponenten und Parameter sind Arbeitsplatz- und Server-Rechner, Leitungen, Netzkoppelelemente, Firewalls, aber auch Software-Versionen, Routing-Tabellen, Adressen und Namenstabellen sowie Schlüssel und Zertifikate.
- Fehlermanagement:
  Um die Verfügbarkeit eines Netzes zu erhöhen, müssen Fehlersituationen frühzeitig erkannt und Fehlerquellen lokalisiert werden. Zu diesem Zweck werden die Netzkomponenten im Rahmen von parametrisierbaren Tests auf ihre Funktionsfähigkeit hin untersucht. Bestimmte Daten (wie z.B. Datendurchsatz und Fehlerraten) über das Netz und seine Komponenten werden gesammelt und analysiert. Ein Überschreiten der voreingestellten Schwellenwerte löst einen Alarm aus.
- Leistungsmanagement:
  Durch Messungen der momentanen Netzleistung und der Ressourcenbelegungen werden Komponenten identifiziert, die zwar fehlerfrei arbeiten, die jedoch die geforderte Leistung nicht erbringen oder nur eine unzureichende Leistungsreserve aufweisen. Es werden Gegenmaßnahmen vorgeschlagen, um die Effizienz des Netzes zu steigern.
- Abrechnungsmanagement:
  Benutzer nehmen Ressourcen für Übertragung, Speicherung und Verarbeitung einschließlich Software in Anspruch. Die Belegung von Ressourcen muss dem Benutzer zweifelsfrei zugeordnet werden können, um sie verursachungsgerecht gegebenenfalls in Rechnung zu stellen. Dies erfordert ein Mitprotokollieren der Ressourcenbelegungen.
- Sicherheitsmanagement:
  Es ist Aufgabe des Sicherheitsmanagements, den Zugang zum Netz und den Zugriff auf Ressourcen und Dienste zu konfigurieren und zu überwachen. Es stellt Basisfunktionen zur Verwaltung von Sicherheitsdiensten und -mechanismen bereit.

Nach dem Modell des OSI Netz- und Systemmanagements basiert der Zugriff auf Managementinformation auf dem Client/Server-Prinzip. Der Server wird üblicherweise als Agent und der Client als Manager bezeichnet. Der Agent läuft auf einem Netzknoten wie beispielsweise einer Workstation, einem Drucker oder Router. Einerseits sammelt er managementrelevante Informationen aus der Komponente und stellt diese dem Manager zur Verfügung, der die eigentliche Verwaltung und Auswertung übernimmt. Andererseits erlaubt er dem Manager, das Verhalten einer Komponente gezielt zu beeinflussen. Die von einem Agenten verwalteten Informationen sind in einzelnen Objekten (managed objects)

enthalten, die zu sogenannten Management Information Bases (MIBs) zusammengefasst werden. Der Nachrichtenaustausch zwischen Manager und Agent erfolgt mittels standardisierter Managementprotokolle.

Im Umfeld TCP/IP-basierter Rechnernetze hat sich das „Simple Network Management Protocol“ (SNMP) als Standard etabliert. Es wird von den meisten Herstellern von Netzkomponenten unterstützt und ist deswegen weit verbreitet. Dem Manager stehen Kommandos für Lese- und Schreibzugriffe auf MIB-Objekte zur Verfügung. Der Agent antwortet auf Anfragen oder sendet in Ausnahmefällen Meldungen an den Manager. Im Zusammenhang mit der Verwaltung der Sicherheit ist ein besonderes Augenmerk auf die Sicherung der Managementvorgänge selbst zu legen. Da SNMP nur durch den Austausch unverschlüsselter Passwörter gesichert ist, gab es frühzeitig Entwürfe für die Integration von Authentifizierungs- und Verschlüsselungsmechanismen. Diese konnten sich jedoch nicht als Standard etablieren. Inzwischen existiert ein SNMPv3 genannter Vorschlag, der die verschiedenen Ansätze vereinheitlichen und auch sicherheitskritische Managementoperationen ermöglichen soll. Im Netz- und Systemmanagement finden inzwischen neue Internetbasierte Technologien Verbreitung. Deshalb sind die Erfolgsaussichten von SNMPv3 im Augenblick nur schwer abzuschätzen.

9.1.3 Beitrag des Netzmanagements zur Systemsicherheit

Die in Abschnitt 9.1.2 genannten Funktionsbereiche bedeuten in der Praxis keine strikte Trennung der Aufgaben des Netz- und Systemmanagements. Es handelt sich vielmehr um unterschiedliche, teilweise überlappende Sichtweisen auf dieselbe Managementinformation. Für den Beitrag des Netzmanagements zur Systemsicherheit spielen neben dem Sicherheitsmanagement die Funktionsbereiche des Konfigurations-, des Fehler-, aber auch des Leistungs- und Abrechnungsmanagements eine Rolle.

Die Bereiche Konfigurations- und Fehlermanagement haben zum Ziel, die Funktionsfähigkeit und Verfügbarkeit eines Netzes sicherzustellen, d.h. die erforderlichen Komponenten von Hardware und Software müssen an der erforderlichen Stelle vorhanden und geeignet konfiguriert sein sowie fehlerfrei arbeiten. Die Verfügbarkeit bezieht sich aber auch auf die Dienstgüte der Funktionen (QoS, Quality of Service), welche Gegenstand des Leistungsmanagements ist; d.h. die einzelnen Komponenten dürfen nicht überlastet sein, um die erforderliche Leistung zu erbringen. Die Verfügbarkeit eines Netzes muss auch finanziert werden. Bei einer Finanzierung durch die Benutzer sorgt das Abrechnungsmanagement für eine zweifelsfreie Zuordnung der Dienstleistungen zu einem Verursacher. Für entsprechende Belegungsdaten muss dabei ihre Integrität sichergestellt werden.

Der für die Systemsicherheit wichtigste Funktionsbereich des Sicherheitsmanagements hat die Aufgabe, sicherheitsrelevante Komponenten und Funktionen entsprechend einer definierten Sicherheitspolitik zu verwalten. Netz- und systemeigene Sicherheitsmechanismen wie beispielsweise die Zugangs- und Zugriffskontrollen unter dem Betriebssystem UNIX sind ebenso zu verwalten wie zusätzliche Sicherheitsapplikationen und/oder Sicherheitsmechanismen innerhalb einzelner Applikationen. Hierzu zählen Sicherheitsmechanismen

wie Verschlüsselung, elektronische Unterschrift (digitale Signatur) oder das Schlüsselmanagement. Die Sicherheitspolitik selbst muss ebenfalls überwacht und eventuell angepasst werden. Das Sicherheitsmanagement basiert auf Funktionen zur Gewinnung, Abfrage, Verarbeitung, Bewertung und Einstellung sicherheitsrelevanter Objekte wie beispielsweise Zugriffsrechte, Schlüssel oder Zugangskontroll-Tabellen. Weitere wichtige Funktionen sind die Protokollierung und Auswertung von Audit-Daten über sicherheitsrelevante Vorgänge.

9.1.4 Managementwerkzeuge und -plattformen

Für die Verwaltung von Netzen und Systemen existiert eine große Zahl von Managementlösungen. Diese lassen sich in folgende Kategorien einteilen:

- Speziallösungen, die nur einen bestimmten Aufgabenbereich, wie z.B. die Verwaltung eines Routers oder die Zugriffskontrolle von Benutzern, über zumeist proprietäre Protokolle abdecken und keinerlei Erweiterungsfähigkeit besitzen;
- alleinstehende Managementumgebungen, die ein Management verschiedener Funktionsbereiche erlauben, jedoch nur mit den Produkten eines oder weniger Hersteller;
- zentrale Managementplattformen, die die Integration verschiedener Werkzeuge, auch von anderen Herstellern, über eine genormte Schnittstelle ermöglichen;
- verteilte Managementplattformen, die ein Auslagern von Teilen der Managementanwendungen gestatten, um die Ressourcen (Netzbandbreite, Ausstattung der Managementkonsole) zu schonen.

Die Reihenfolge spiegelt auch in etwa die Entwicklungsgeschichte der Managementwerkzeuge wider. Vor allem den Managementplattformen kommt dabei eine entscheidende Bedeutung zu. Deshalb sollen ihre Eigenschaften hier kurz charakterisiert werden:

- modularer Aufbau,
- grafische Benutzeroberfläche,
- offene Systeme, d.h. Module von Fremdherstellern können vom Anwender integriert werden,
- allgemeine Schnittstelle (API) für Managementanwendungen von Komponentenherstellern,
- allgemeine Schnittstelle (API) für Kommunikation mit gebräuchlichen Managementarchitekturen (SNMP, Open Systems Interconnect (OSI), Desktop Management Task Force (DMTF), Common Object Request Broker Architecture (CORBA)),
- objektorientierte Modellierung von Komponenten und Managementinformation,
- unabhängig von Funktionsbereichen und herstellerspezifischen Ressourcen,
- in zunehmendem Maße Verteilbarkeit von Managementaufgaben (intelligente Agenten).

Die Managementplattformen ermöglichen die Integration der einzelnen Managementbereiche unabhängig von den zugrunde liegenden Komponenten und Managementarchitekturen. Sie stellen sicher einen großen Fortschritt gegenüber den herstellerspezifischen Insellösungen dar. Dennoch gibt es in diesem Bereich noch einige ungelöste Probleme.

Leider wird häufig noch die bloße Integration unabhängiger Speziallösungen unter einer gemeinsamen Benutzeroberfläche als integriertes Management angeboten. Viele Systemhersteller (HP, IBM, Sun, ...) haben eigene Managementplattformen entwickelt, die ihre besonderen Stärken meist mit den herstellereigenen Produkten ausspielen können. Die einzelnen Plattformen untereinander haben oft Probleme, wichtige Datenbestände, wie z.B. Topologieinformation, auszutauschen. So besitzen inzwischen die meisten Plattformen Anschlussmöglichkeiten an Datenbanksysteme über SQL, doch wurde bisher kein gemeinsames Datenmodell definiert. Bei der Definition von Protokollen zum Austausch von Information zwischen Plattformen unterschiedlicher Hersteller hat sich bisher noch kein Standard durchsetzen können.

Aufgrund der genannten Einschränkungen kann an dieser Stelle keine eindeutige Bewertung der zahlreichen Werkzeuge gegeben werden. Die in der Literatur (/Hegering93/ und /Seitz94/) verfügbaren Beschreibungen sind durch die schnellen Innovationszyklen nach kurzer Zeit nur noch eingeschränkt gültig. So hat 1996 z.B. im Bereich des Systemmanagements die Firma IBM durch den Kauf von ‚Tivoli' die Abkehr von ihrem Produkt ‚SystemView' begonnen.

In Tabelle 9.1 wurde dennoch versucht, eine Auswahl der bezüglich Verbreitung und Leistungsfähigkeit im Augenblick bedeutendsten Managementwerkzeuge und Plattformen zu geben. Neben der Angabe des Produktnamens in der Tabelle bezeichnet das Umfeld die Protokolle und Betriebssysteme, unter denen das Produkt lauffähig ist. Alle angegebenen Managementwerkzeuge und -plattformen decken den Protokollbereich SNMP und TCP/IP ab, zum Teil aber auch andere und proprietäre Protokollbereiche. Weitere Information findet sich für die Produkte der Hersteller unter den angegebenen URLs (WWW-Adressen) in der Tabelle und übergreifend z.B. unter `http://snmp.cs.utwente.nl/` (The simple Web, University of Twente) und/oder `http://netman.cit.buffalo.edu/` (Network Management Server, University at Buffalo, New York). Die Abkürzung NSM steht für Netz- und Systemmanagement.

Neben den in der Tabelle aufgeführten Plattformen existieren jedoch noch eine Reihe weiterer Produkte, die alle ihre Stärken und Schwächen besitzen. Deshalb sollte vor der Beschaffung der zumeist kostenträchtigen Werkzeuge eine genaue Problemanalyse durchgeführt werden, aus der sich ein Anforderungskatalog für eine Evaluierung ableiten lässt. Neben der Funktionalität im Bereich des Sicherheitsmanagements sind besonders die von Fremdherstellern verfügbaren Anwendungen kritisch zu betrachten.

Produktname	Umfeld	Charakteristik	Entwickler	weitere Information
HP OpenView - Network Node Manager - Operations Center - Workgroup Node Manager - Extensible SNMP Agent - IT/Operations	TCP/IP, SNA, IPX (Novell), HP-UX, Solaris, WINDOWS	Plattform für integriertes NSM, Autodiscovery, Konfigurationsmanagement, große Anzahl von integrierbaren NSM-Applikationen von anderen Herstellern, eigenes API, Ausbau zu verteilter Plattform möglich / intelligenter Agent	Hewlett-Packard	http://www.hp.com/openview/index.html
Tivoli Management Environment TME 10	UNIX/AIX, NT, OS/2, PC, OS/390, OS/400	Plattform mit objektorientiertem Ansatz für verteiltes NSM (∼CORBA) / IBM's SystemView wird mit TME vereinigt	Tivoli / IBM	http://www.tivoli.com/tivevery/prodhm.html
NetView/6000	SNA, TCP/IP, OS/2, AIX	Schwerpunkt Netzverwaltung, Verbindung TCP/IP u. SNA-Welt	IBM	http://www.raleigh.ibm.com/nv6/nv6prod.html
Solstice / SunNet Manager - Domain Manager 2.3 - Enterprise Manager - Site Manager	TCP/IP, OSI, Solaris	Plattform für integriertes NSM, Verteilung über X11/OpenLook, skalierbar durch Installation als intelligenter Agent, große Anzahl von integrierbaren NSM-Applikationen von anderen Herstellern / eigenes API	SunSoft	http://www.sun.co.jp:8080/solstice/index.html
CA-Unicenter	UNIX, NT, AS/400, NETWARE, Mainframe	Alleinstehende NSM-Lösung mit Schwerpunkt Systemmanagement, Sicherheit, Last, Speicher, ...	Computer Associates International	http://www.cai.com/products/uctr.htm
TransView - SNMP Domain Manager - Control Center	PC, RMxxx, SINIX	Plattform für integriertes NSM, Ereigniskorrelation mittels intelligenter Agenten / eigenes API	Siemens Nixdorf / Pyramid	http://www.sni.de/public/mr/network/network.htm

Produktname	Umfeld	Charakteristik	Entwickler	weitere Information
Cabletron SPECTRUM 4.0	SNA, NT, UNIX	Integrierte, verteilte, wissensbasierte NSM-Plattform, politikbasierte Ereigniskorrelation / erweiterte Skalierbarkeit, leistungsfähiges Netzmanagement	Cabletron Systems	http://www.ctron.com/spectrum/
CiscoWorks Cisco Windows Network Management Software	TCP/IP, IPX WINDOWS95/NT	PC-basierte NM-Plattform mit Schwerpunkt bei Cisco Netzprodukten; empfohlen für 5-50 Koppelelemente, integrierbar in HP OpenView	Cisco Systems	http://www.cisco.com/warp/cpropub/60/
Integrated System Management ISM/OpenMaster	TCP/IP, SNA, UNIX(BULL), PC	Integrierte, verteilte NSM-Plattform mit zentraler Datenbank für Managementdaten, ISM/OpenMaster Agenten	Groupe Bull S.A.	http://www.ism.bull.net/
Novell ManageWise	NETWARE, NT, PC, IPX, TCP/IP	Ursprünglich für NETWARE entwickelte Netz- und Systemmanagementplattform, inzwischen auch mit Verwaltung SNMP-fähiger Komponenten / eigenes API (NLM)	Novell	http://www.novell.com/catalog/bg/bge54110.html
Systems Management Server SMS (BackOffice)	NT, PC, IPX, Netbeui, TCP/IP, SNA	Anwendung für Systemmanagement von verteilten WINDOWS-basierten Systemen (DMI), integrierbar in NSM-Plattformen	Microsoft	http://www.microsoft.com/germany/backoffice/smsmgmt/

Tabelle 9.1: Eine Auswahl von Managementwerkzeugen und -plattformen

9.2 Verwalten von Sicherheitsmechanismen

Die Grundlage für die Verwaltung von Sicherheitsmechanismen ist die Sicherheitspolitik (siehe Kapitel 1). Diese legt grundlegende Anforderungen fest, z.B. wer welchen Dienst

nutzen darf, wer seine Identität wie nachzuweisen hat, welche Vorgänge aufgezeichnet werden müssen etc. Diese abstrakten Anforderungen der Sicherheitspolitik müssen durch geeignete Sicherheitsmechanismen realisiert werden. Dabei kann zuerst einmal das Problem auftauchen, dass notwendige Sicherheitsmechanismen nicht verfügbar sind und erst noch installiert werden müssen. Wenn sie aber vorhanden sind, müssen sie auch richtig konfiguriert und der laufende Betrieb überwacht werden, um z.B. Angriffe und Angriffsversuche erkennen zu können. Abbildung 9.2 verdeutlicht dies:

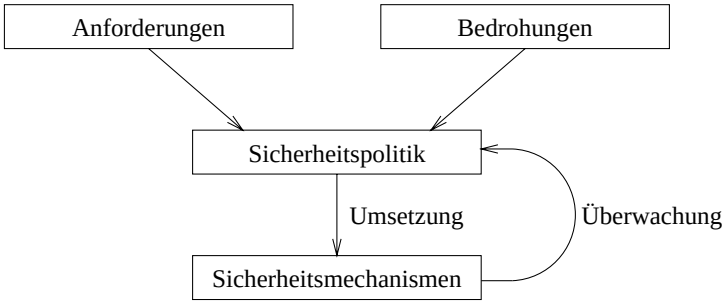


Abbildung 9.2: Umsetzung der Sicherheitspolitik

In der Praxis stellt sich die Frage, ob alle Sicherheitsmechanismen korrekt konfiguriert sind, also ob das informationstechnische System sicher ist. Diese Frage ist jedoch nicht entscheidbar, da es kein „sicheres“ und kein „unsicheres“ Netz gibt, sondern nur solche, die gegen bestimmte Bedrohungen angemessen geschützt sind oder nicht. Im Sicherheitskonzept ist festgehalten, welche Maßnahmen zu ergreifen sind. Davon ausgehend ist systematisch und nachvollziehbar die korrekte Konfiguration der Sicherheitsmechanismen vorzunehmen. Dafür gibt es derzeit jedoch noch keine Werkzeugunterstützung. Das Netz- und Systemmanagement stellt jedoch Methoden bereit, um Sicherheitsmechanismen zu konfigurieren und zu überwachen.

9.2.1 Sicherheits- und Zugriffsmodelle

Zugriffsmodelle geben an, welches Subjekt auf welchem Objekt welche Operation durchführen darf. Die Definition, welche Subjekte, Objekte und Operationen es gibt, hängt vom jeweiligen Einsatzgebiet ab. Subjekte können z.B. Personen, Rechner oder Prozesse sein. Objekte sind z.B. Daten oder Rechner. Operationen sind beispielsweise Lesezugriff, Schreibzugriff, Ausführen von Programmen oder Einloggen auf einem Rechner. Diese Modelle lassen sich grob in zwei Klassen einteilen:

- Informationsflussmodelle
  Durch die Art des Subjekts und des Objekts ist festgelegt, welche Operationen das Subjekt auf dem Objekt durchführen kann. Beispielsweise kann jedes Subjekt und jedes Objekt als offen, vertraulich oder geheim eingestuft werden. Ein Subjekt kann

auf ein Objekt nur lesend zugreifen, falls seine Geheimhaltungsstufe mindestens so hoch wie die des Objekts ist, auf das zugegriffen wird. Das Einsatzgebiet dieser Verfahren liegt v.a. im militärischen Bereich.

- Benutzerbestimmbare Zugriffsmodelle
  Bei diesen Modellen ist jedem Objekt ein Eigentümer zugeordnet, der die Zugriffsrechte beliebig vergeben kann. Um einen sicheren Betrieb zu gewährleisten, sind gewisse Regeln einzuhalten, z.B. dürfen Konfigurationsdateien nicht für alle schreibbar sein. Dieses Verfahren wird bei kommerziellen Rechnersystemen üblicherweise eingesetzt. Im Folgenden werden nur benutzerbestimmbare Zugriffsmodelle betrachtet.

Es gibt Unterschiede, mit welcher Granularität, d.h. wie fein abgestuft, die Rechtevergabe erfolgen kann. Bei einem Dateisystem beispielsweise können Rechte nur für ganze Dateien vergeben werden, nicht jedoch für Teile davon. Teilweise sind die Möglichkeiten zur Rechtevergabe dadurch eingeschränkt, dass nur die Rechte für den Eigentümer, für eine Gruppe und für Sonstige unterschieden werden können (UNIX). Weiterhin gelten üblicherweise die Zugriffsrechte unabhängig von anderen Bedingungen wie z.B. der aktuellen Tageszeit oder der Durchführung einer Aufgabe. Es ist darauf zu achten, dass die Granularität für eine Umsetzung der Sicherheitspolitik ausreicht.

Die Zugriffsmodelle beschreiben nur, welches Subjekt welche Operationen auf welchem Objekt ausführen darf. Es gibt jedoch weitere Sicherheitsdienste, die bei Zugriffsmodellen nicht betrachtet werden, deren Parameter und Schlüssel jedoch vom Sicherheitsmanagement verwaltet werden.

- Authentifizierung
  Wie weist ein Subjekt (z.B. ein Benutzer, Rechner) seine Identität nach. Eine Authentifizierung kann durch drei unterschiedliche Arten erfolgen, die auch kombiniert werden können:
  - Wissen
    Das Subjekt kennt ein Geheimnis, das es zum Nachweis der eigenen Identität verwendet. Beispiele hierzu sind Passwortverfahren und kryptographische Authentifizierungsverfahren.
  - Besitz
    Das Subjekt muss einen bestimmten Gegenstand besitzen, z.B. einen (physischen) Schlüssel, einen Ausweis, eine Magnet- oder Chipkarte.
  - Eigenschaften
    Bestimmte Eigenschaften des Subjekts werden geprüft, z.B. bei natürlichen Personen Fingerabdruck, Retinastruktur oder die Stimme.
- Datenintegrität
  Daten können nicht unbemerkt verändert werden.
- Vertraulichkeit
  Daten können nur von befugten Personen gelesen werden.
- Verbindlichkeit
  Eine Operation kann nicht abgestritten werden.

- Audit
  Vorgänge werden protokolliert.

Diese Sicherheitsdienste werden, soweit es von der Sicherheitspolitik gefordert wird, durch entsprechende Sicherheitsmechanismen realisiert.

9.2.2 Komponenten der Verwaltung von Sicherheitsmechanismen

Anhand einer Untergliederung in physische und logische Komponenten werden die Mechanismen angesprochen, die verwaltet werden müssen. Diese Aufstellung nennt nur beispielhaft häufig vorkommende Aspekte.

Physische Komponenten

- Verkabelung
  Da Kabel abgehört oder fremde Rechner an ein Kabel angeschlossen werden können, ist die physische Konfiguration zu verwalten, d.h. wo die Kabel verlegt sind, welche Netzkomponenten wo aufgestellt sind, wie diese Komponenten gegen Zugriffe von Unbefugten geschützt sind. Dies ist insbesondere wichtig, da in LANs Daten häufig unverschlüsselt übertragen werden und so mitgelesen werden können.
- Bridges/Hubs
  Bridges trennen Netze, d.h. nicht jedes Paket ist auf allen Netzsegmenten sichtbar, sondern nur die Pakete, die weitergeleitet werden müssen. Einen ähnlichen Dienst erbringen Switching Hubs. Bridges und Hubs können oft über das Netz administriert werden. Es ist sicherzustellen, dass nur befugte Administratoren die Konfiguration ändern können.
- Router
  Wie Bridges und Hubs dürfen Router nur von autorisierten Netzadministratoren verwaltet werden. Zusätzlich bieten viele Router die Möglichkeit, eine Filterung der übertragenen Pakete durchzuführen, z.B. abhängig von der Quellen- und Zieladresse, vom Protokoll, vom Sende- und Empfangsport und von bestimmten Flags. Die Konfiguration dieser Filterregeln erfordert ein gutes Verständnis der zugrunde liegenden Protokolle.
- Firewalls
  Firewalls dienen der Trennung von Netzen. Es ist zu konfigurieren, welche Dienste zugelassen werden, wer sie nutzen darf, wie sich ein Benutzer zu authentifizieren hat, welche Ereignisse festzuhalten sind.
- Serverrechner
  Server stellen im Netz bestimmte Dienste bereit, sie sind jedoch nur Systemadministratoren direkt zugänglich. Sie können z.B. in besonders gesicherten Räumen aufgestellt werden. Zu sichern sind v.a. die Dienste, die über das Netz zugänglich sind.

- Arbeitsplatzrechner
  Arbeitsplatzrechner werden von Anwendern eingesetzt. Vor allem PCs bieten nur wenige technische Möglichkeiten, Sicherheitskonzepte durchzusetzen. Eine Gefahr geht von Benutzern aus, die Sicherheitsmaßnahmen nicht beachten oder umgehen, sei es aus Unwissenheit oder weil die Sicherheitsmaßnahmen für hinderlich und nicht notwendig erachtet werden. Es können z.B. durch selbstinstallierte Software Viren eingeschleust werden, oder es können über Disketten vertrauliche Informationen an Dritte gelangen. Deshalb sind organisatorische Maßnahmen, v.a. eine Sensibilisierung der Benutzer für Sicherheitsbelange, notwendig. Die Einführung von Chipkarten und kryptographische Schlüssel können dazu sicher einen Beitrag leisten.

Logische Komponenten

- Benutzer- und Gruppenverwaltung
  Durch die Benutzer- und Gruppenverwaltung wird festgelegt, welche Benutzer es gibt, welche Gruppen es gibt, und welcher Benutzer Mitglied welcher Gruppen ist.
- Schlüssel- und Sicherheitsdienstverwaltung
  Wenn auch in heutigen informationstechnischen Systemen kryptographische Verfahren selten eingesetzt werden, wird deren Bedeutung mit dem Einsatz von Chipkarten zunehmen. Für die dann notwendige Schlüsselverwaltung ergeben sich folgende Aufgaben: Schlüssel sind zu generieren, zu verteilen bzw. auf Chipkarten zu laden und bei Bedarf zu zertifizieren. Da kryptographische Schlüssel nur eine begrenzte Verwendungsdauer haben, müssen in regelmäßigen Abständen neue Ersatzschlüssel erzeugt und die alten Schlüssel deaktiviert werden. Kompromittierte Schlüssel müssen gesperrt werden. Die Sicherheitsdienste selbst sind ebenfalls zu verwalten, d.h. sie müssen konfiguriert und ihr Einsatz überwacht werden.
- Dateisystem
  Über welche Rechte verfügt welcher Benutzer bzw. welche Gruppe. Unterschieden werden Lese-, Schreib- und Ausführungsrecht. Privilegierte Programme, das sind solche mit gesetztem Set-User-Id-Bit, sind besonders zu beachten.
- Datenbanken
  Es können für verschiedene Rollen unterschiedliche Sichten und Befugnisse festgelegt werden.

9.2.3 Konfiguration und Verwaltung von Benutzern, Diensten, Zugriffsrechten und Komponenten

Der Ausgangspunkt für die Konfiguration der Sicherheitsmechanismen ist die Sicherheitspolitik (siehe Kapitel 1). Diese sollte unabhängig von den bereits zur Verfügung stehenden Sicherheitsmechanismen entworfen werden. Die Sicherheitspolitik definiert auf einer abstrakten Ebene die Sicherheitsanforderungen, die das IT-System zu erfüllen hat. Die Sicherheitspolitik ist durch geeignete Maßnahmen, die technischer oder organisatorischer Art sein können, umzusetzen. Geeignete Sicherheitsmechanismen, die zur Umsetzung der Sicherheitspolitik erforderlich sind, sind auszuwählen und diese sind der Sicherheitspolitik

entsprechend zu konfigurieren. Diese Umsetzung muss nachprüfbar, d.h. revisionsfähig erfolgen. Es genügt nicht, die Sicherheitsmechanismen einmal korrekt zu konfigurieren, sondern die Konfiguration ist im laufenden Betrieb in regelmäßigen Abständen zu überwachen. Um dies effizient zu gestalten, ist eine Werkzeugunterstützung erforderlich.

Das zu verwaltende System ändert sich im laufenden Betrieb, da z.B. neue Benutzer und Gruppen eingerichtet und alte gelöscht werden. Neue oder erweiterte Dienste und Anwendungen werden installiert, geänderte Anforderungen führen zu einer Modifikation bestehender Anwendungen. Trotzdem muss die Konfiguration der Sicherheitspolitik jederzeit entsprechen. Bei der Dynamik informationstechnischer Systeme ist es unvermeidlich, dass auch die Sicherheitspolitik an neue Anforderungen angepasst werden muss.

Die Sicherheitspolitik legt auch fest, welche Ereignisse im laufenden Betrieb festgehalten werden sollen. Die Auswertung dieser Aufzeichnungen muss in regelmäßigen Abständen erfolgen, um versuchte oder erfolgreiche Angriffe erkennen und bei Bedarf Gegenmaßnahmen einleiten zu können. Dafür ist eine Werkzeugunterstützung wünschenswert.

9.3 Sicherheitsüberwachung

9.3.1 Einführung

Im Gegensatz zu baulichen und (programm-)technischen Maßnahmen zur Erhöhung der Netzsicherheit, die *direkt* wirken, bedürfen organisatorisch/administrative Maßnahmen der Kontrolle, um wirksam zu werden. Für datenschutzrechtliche Belange gibt es entsprechende Kontrollinstanzen und Rechtsnormen; für die Gewährleistung der Betriebsbereitschaft, Verfügbarkeit und Zuverlässigkeit muss der Netzbetreiber durch Sicherheitsvorgaben, Sanktionsmechanismen und Regularien selbst sorgen. Dadurch erhöht sich einerseits die Flexibilität, andererseits verstärkt sich aber die Notwendigkeit, Sicherheitspolitik und -konzept in einer organisatorischen Einheit durch aktive Kontrolle auch durchzusetzen.

Das setzt voraus, dass die Leitung sich der Sicherheitsproblematik bewusst ist und die Verantwortung dafür als Aufgabe personalisiert. Das im BSI-IT-Grundschutzhandbuch für Initiierung und Umsetzung von Maßnahmen zitierte IT-Sicherheitsmanagement ist in der Praxis oft der DV-Leiter oder die Aufgabe ist (implizit) auf mehrere Personen der DV-Abteilung aufgeteilt. Im Arbeitsalltag ergeben sich daraus offensichtlich Interessenkonflikte (Selbstkontrolle), die dem Problem nicht gerecht werden. Aus diesem Grund wird die Etablierung eines **IT-Sicherheitscontrolling** gefordert. Diese Stelle/Person ist verantwortlich für die Initiierung, Realisierung und Kontrolle sicherheitsrelevanter Maßnahmen[1].

[1] „Leider stellte der Bundesrechnungshof bei Prüfungen fest, dass das Sicherheitsbewusstsein, insbesondere beim Management nicht genügend ausgeprägt war, dass Mitarbeitern die nötige Schulung fehlte und die Funktion des IT-Sicherheitsbeauftragten noch nicht eingerichtet war. Als Alibi wurde gelegentlich auf den Datenschutzbeauftragten verwiesen, der sich jedoch zumeist nur um die Rechtmäßigkeit der Speicherung personenbezogener Daten, aber nicht um technische Aspekte der IT-Sicherheit kümmerte.“ Bunge, E., Leiter des Prüfungsgebietes „IT-Sicherheit“ des Bundesrechnungshofes (Business Computing 1/94, S. 22)

Das BSI empfiehlt, regelmäßig, mindestens monatlich einen Sicherheitscheck des Netzes durchzuführen, um folgende Fragen zu klären:

- Gibt es Benutzer ohne Passwort oder mit einem Passwort, das nicht die erforderlichen Bedingungen einhält?
- Gibt es Benutzer, die das Netz längere Zeit nicht benutzt haben?
- Welche Benutzer besitzen die gleichen Rechte wie der Superuser?

Hilfreich für Sicherheitskontrollen im UNIX-Bereich sind sogenannte Check-Listen z.B.:

`ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist`

`http://stimpy.cac.washington.edu/~dittrich/R870/security-checklist.html`

Sie enthalten umfangreiche und auch produktbezogene Informationen und Anweisungen zum Erkennen und Beseitigen von Sicherheits-Schwachstellen sowie Links zu relevanten CERT-Veröffentlichungen (advisories). Darüber hinaus werden frei verfügbare „Security Tools“ beschrieben und deren Bezugsquellen genannt. Prinzipiell können aber solche Check-Listen nie vollständig sein bzw. alle Schwächen aufdecken. Ein Sicherheitsbeauftragter muss deshalb laufend und wachsam die Fachpresse und Meldungen über entsprechende Mail- und WWW-Dienste verfolgen, diese in die lokalen Gegebenheiten umsetzen und die notwendigen Konsequenzen veranlassen (weitere Hinweise in Abschnitt 9.3.3).

9.3.2 Methoden der automatisierten Sicherheitsüberwachung

Security-Werkzeuge, speziell Scan-Tools, können die Überwachung der Sicherheit des Netzes und seiner einzelnen Systeme auf vielfältige Weise automatisieren. Eine Einteilung der Werkzeuge kann z.B. nach dem untersuchten Betriebssystem, der Art der untersuchten Sicherheitslücken und dem Ort, an dem die Untersuchung durchgeführt wird (lokal oder remote), vorgenommen werden. Man kann auch zwischen Werkzeugen unterscheiden, die das Entstehen von Lücken verhindern („proactive“) und solchen, die bestehende Lücken erkennen („reactive“).

Die Einteilung nach Betriebssystemen, für die Werkzeuge existieren, zeigt eine starke Polarisierung in Richtung UNIX, vor allem bei frei verfügbaren Tools. Dies mag hauptsächlich an der längeren Existenz des Betriebssystems und der Vielzahl seiner Derivate sowie an den häufig frei verfügbaren Quellentexten liegen.

Grundlegende Arten von Sicherheitslücken, die aufgespürt werden können, sind falsche Konfiguration, Bedienungsfehler, Softwareversionen mit bekannten Lücken sowie Viren, Trojanische Pferde etc. Methoden, um diese Lücken zu finden, sind z.B. Konfigurations- und Audit-Dateien zu analysieren, Programmversionen zu vergleichen, Dateien auf Viren zu durchsuchen, die Integrität des Systems sicherzustellten (Soll-Ist-Vergleich), Passwörter vor oder nach dem Ändern auf ihre Qualität zu überprüfen, den Netzverkehr zu überwachen, oder bekannte Angriffe probeweise anzuwenden.

Viele dieser Überwachungen sind nur lokal möglich, d.h. das Werkzeug wird direkt auf allen betroffenen Rechnern ausgeführt oder hat zumindest direkten Zugang zu den Dateien.

Viele Scans sind aber auch von zentraler Stelle aus durchführbar, es werden dann die betroffenen Rechner „von außen“ analysiert. Eine Sonderrolle stellen hier Firewalls dar, die den Netzverkehr an der Schnittstelle Intranet–Internet überwachen und kontrollieren.

Eine weitere Einteilung richtet sich nach dem relativen Zeitpunkt, an dem die Überprüfungen stattfinden. So kann etwa ein Passwort auf seine Qualität hin untersucht werden, bevor es vom System akzeptiert wird, oder es werden existierende Passwörter quasi nachträglich analysiert. Ähnliches trifft für Tests auf Viren zu. Häufig ist die Kombination beider Alternativen sinnvoll.

9.3.3 Werkzeuge und deren Einordnung

Dieser Abschnitt soll einen Überblick über frei verfügbare Security-Tools bieten. Leider gibt es keine übergreifenden Werkzeuge, die alle Lücken in den Systemen finden oder deren Auftreten verhindern könnten. Daher ergibt sich ein sehr zerstreutes Bild vieler Einzeltools, die jeweils sehr spezifische Eigenschaften aufweisen und oft für sehr spezifische Probleme ausgelegt sind. Im Allgemeinen wird man eine unbestimmte Anzahl dieser Tools einsetzen; die Auswahl hängt in großem Maße von den lokalen Gegebenheiten ab.

Die folgende Tabelle der Sicherheitswerkzeuge gibt neben dem Namen und einer Kurzbeschreibung der Werkzeuge deren Einsatzbereich an: für welches Betriebssystem (OS), ob lokal oder remote (Ort), ob vorbeugend oder nach einem Angriff (Zeit).

Name	Kurzbeschreibung	OS	Ort	Zeit
Sicherheit von Passwörtern:				
anlpsswd	Proaktives passwd-Programm: „schlechte“ Passwörter werden abgelehnt	UNIX	Lokal	Prä
Crack	Versucht, Passwörter zu knacken, um „schwache“ Passwörter zu entdecken	UNIX	Lokal	Post
cracklib	Bibliothek von Funktionen, die verhindern, dass Benutzer Passwörter verwenden, die „geknackt“ werden können	UNIX	Lokal	Prä
mangle	Qualitätskontrolle von Passwörtern bevor sie geändert werden	UNIX	Lokal	Prä
npasswd	passwd- und yppasswd-Ersatz: lässt keine „schlechten“ Passwörter zu	UNIX	Lokal	Prä
passwd+	Über eine regelbasierte Konfigurationsdatei wird festgelegt, welcher Typ von Passwörtern erlaubt ist und welcher nicht	UNIX	Lokal	Prä
shadow	Ersetzt den normalen Passwort-Kontroll-Mechanismus; die verschlüsselten Passwörter werden versteckt und sind nur für privilegierte Programme lesbar	UNIX	Lokal	Prä

Name	Kurzbeschreibung	OS	Ort	Zeit
Netz- und System-Scanner:				
COPS	Security Scanner mit unterschiedlichen Sicherheits-Tests: schlechte Passwörter, Zugriffsrechte, Existenz von root-SUID-File, nicht limitierter FTP. Integriert ist auch das Kuang-Expertensystem, mit dem regelbasiert die „Verwundbarkeit“ geprüft wird.	UNIX	Lokal	Prä
ISS	Internet Security Scanner; deckt in der frei verfügbaren Version nur offensichtliche Fehler auf (auch als wesentlich leistungsfähigere kommerzielle Variante verfügbar)	UNIX	Remote	Prä
netlog	Programm zum Lokalisieren verdächtiger Netzaktivitäten (enthält: tcplogger, udplogger: Auditing aller TCP- bzw. UDP-Aktivitäten im Subnetz; extract: die erstellten Logfiles auswerten; netwatch: Realtime network monitor)	UNIX	Remote	Post
SATAN	Programm zur Überprüfung von Netzen mit UNIX-Workstations. Getestet werden Schwachstellen, die ein Angreifer über das Internet ausnutzen kann. Alle Lücken werden gut dokumentiert. Benötigt werden: HTML-Viewer, Perl, C-Compiler	UNIX	Remote	Prä
strobe	Lokalisiert und beschreibt alle aktiven TCP-Ports auf einem oder mehreren (remote) Hosts	UNIX	Remote	Post
tiger	Mehrere Scripts, die UNIX-Systeme auf Sicherheitsprobleme prüfen	UNIX	Lokal	Prä
Anti-Scan-Tools:				
Argus	Generisches IP-Netz-Transaktion-Auditing-Programm. Geprüft wird z.B.: Hat jemand versucht, mit SATAN das Subnetz auf „Schwächen“ zu scannen? Welche Verbindungsversuche wurden durch die Firewall blockiert?	UNIX	Lokal	Post
Courtny	Überwacht das Netz und identifiziert Maschinen mit SATAN-Attacken	UNIX	Remote	Post
Gabriel	Speziell entwickelt, um SATAN-Scans und -Attacken aufzudecken	UNIX	Lokal	Post
Moni-Box	Netzmonitor für IP und IPX mit Erfassung von (evtl. auch virtuellen) Verbindungen. Über Auswertemechanismen sind Scanversuche zu erkennen. Verarbeitet ebenfalls Format von Drawbridge- und Cisco-Filterlisten zur Überprüfung der Firewallfunktionalität.	BSD-UNIX	Netz	Prä/Post

Name	Kurzbeschreibung	OS	Ort	Zeit
Firewalls etc.:				
drawbridge	Packet-Screen Firewall	PC	Netz	Prä
IPACL	Lokale Firewall, vergleichbar TCP-Wrapper: filtert kommende und gehende TCP-Pakete, abhängig von Quellen- und Zieladressen und Portnummern können Pakete passieren oder nicht	UNIX	lokal	Prä
karlbridge	Packet-Screen Firewall	PC	Netz	Prä
netlog	Untersuchen des Netzverkehrs	UNIX	Netz	Prä
socks	Generischer Proxy-Server, um einzelne Dienste über eine Firewall abzuwickeln	UNIX	Netz	Prä
TCP-Wrapper	Wrapper um *inetd* sowie Bibliothek, um ankommende TCP/IP-Verbindungen aufzuzeichnen, auszuwerten und eventuell abzublocken	UNIX	Lokal	Prä
tcpdump	Untersuchen des Netzverkehrs	UNIX	Netz	Prä
xinetd	Lokale Firewall, vergleichbar TCP-Wrapper	UNIX	Lokal	Prä
Auditing und Auswertungen:				
logdaemon	Programmpaket mit modifizierten Implementationen der gängigsten Netzserver (*rlogind, rshd, login, rexecd, ftpd,* S/Key)	UNIX	Lokal	Prä
Logsurfer	Kontextsensitive Echtzeit-Auswertung der anfallenden Audit-Daten; portables C-Programm, Fortentwicklung von Swatch, dynamisch	UNIX	Lokal	Post
lsof	Zuordnen von offenen Dateien und Netzverbindungen zu Benutzern, hilfreich bei der Spurensuche	UNIX	Lokal	Post
pident	Portabler *ident*-Server; kann bei der Spurensuche helfen	UNIX	Lokal	Post
portmapper, rpcbind	Ersatz für die originalen Tools mit Zugriffskontrolle und verbessertem Auditing	UNIX	Lokal	Prä
swatch	Verbreitetes Programm zur Online-Überwachung beliebiger Textdateien (z.B. Audit-Dateien: syslog). In einer Konfigurationsdatei wird festgelegt, wie auf gewisse Nachrichten reagiert werden soll; statische Regeln, kein „backtracking“.	UNIX	Lokal	Post
tripwire	Integritätsprüfung von Dateisystemen, Erkennen unerwünschter Änderungen am Dateisystem; benutzt kryptographische Verfahren	UNIX	Lokal	Post

Name	Kurzbeschreibung	OS	Ort	Zeit
Diverses:				
dnswalk	Prüft DNS-Datenbank auf interne Konsistenz	UNIX	Remote	—
doc	Analysiert DNS-Struktur und Autorisierungsprobleme	UNIX	Remote	—
merlin	Meta-Tool: Interface für verschiedene Scanner (COPS, TAMU-Tiger, Crack, tripwire und SPI)	UNIX	—	—
TAMU	Kombiniert *drawbridge, tiger, netlog*	—	—	—
Div. Viren-scanner	Bereits sehr große Auswahl an kommerziellen und frei verfügbaren Tools, etwa McAfee VirusScan, Dr. Solomon's Antivirus Toolkit, Norton Antivirus, DataFellows F-PROT...	Div.	Lokal	Prä/Post

Tabelle 9.2: Sicherheitswerkzeuge

Einen Überblick mit Verweisen zu Bezugsquellen und weiteren Informationen geben z.B. folgende WWW-Seiten (DFN-CERT, NIST-CSRC):

`http://www.cert.dfn.de/infoserv/dib/`
`http://csrc.ncsl.nist.gov/tools/tools.htm`

Eine in Deutschland sehr gut erreichbare Quelle für sehr viele Security-Tools ist der FTP-Server des DFN-CERT:

`ftp://ftp.cert.dfn.de/pub/`

Daneben können auch kommerzielle Produkte eingesetzt werden, z.B. Pingware (Bellcore), HORUS (SNI), Netprobe Commercial, ISS Commercial („mit mehr als 120 verschiedenen Tests, dem derzeit größten Umfang an Sicherheits-Checks"), Axent, Tivoli etc.

Naturgemäß können mit diesen Programmen, die auch Angreifer kennen, primär nur bekannt gewordene Schwachstellen aufgedeckt werden.

Besonderes Augenmerk bei Kontrollen ist den Default-Einstellungen zu widmen, die aus Gründen besserer Performance oder einer einfacheren Installation nicht geändert wurden. Die Ergebnisse der Sicherheitschecks sind zu dokumentieren. Sicherheitsprüfungen und *Penetrationstests* können auch durch externe Stellen (z.B. TrustCenter) durchgeführt werden.

Zu den Aufgaben des IT-Sicherheitscontrolling gehört auch die Analyse und Auswertung von Audit-Informationen. Voraussetzung ist, dass diese Daten auch aufgezeichnet werden, z.B. durch

- TCP-Wrapper: Protokollierung des Aufbaus von bestimmten Netzverbindungen
- logdaemon: Erweiterung der Protokollierung von Benutzerlogins

und das *syslog*-Protokoll verwendet wird. Durch dieses Client/Server-Konzept wird die Generierung einer Nachricht von der Speicherung getrennt. In der Datei *syslog.conf* kann disponiert werden über die

- Abspeicherung der Nachricht in einer Datei,
- Weiterleitung der Nachricht an einen anderen Rechner,
- Weiterleitung an bestimmte Benutzer, falls diese eingeloggt sind,
- Weiterleitung der Nachricht an alle eingeloggten Benutzer.

Wird das *syslog*-Protokoll verwendet, können die Informationen zentral (*syslog*-Server) gesammelt und ausgewertet werden, eine wichtige Voraussetzung für das rechtzeitige Erkennen von Attacken. Fehlende Audit-Daten erschweren die Entdeckung von Angriffen bzw. Angriffsversuchen aus dem Internet. Für die Auswertung der in der Regel sehr umfangreichen Audit-Daten können auch Tools (z.B. Swatch, Logsurfer) eingesetzt werden, wobei der automatischen Auswertung natürlich Grenzen gesetzt sind, da nicht alle möglichen Ereignisse und erforderlichen Konsequenzen vorgegeben werden können.

9.3.4 Ausblick: Intrusion-Detection-Systeme

Intrusion-Detection-Systeme (IDS) sollen Angriffe oder Angriffsversuche nicht nur nachträglich, sondern während ihres Ablaufens entdecken und augenblickliche Gegenmaßnahmen ermöglichen. Es gibt Bemühungen, Intrusion-Detection-Systeme der nächsten Generation zu entwickeln, wie sie beispielhaft in Tabelle 9.3 aufgeführt werden.

Die Ziele sind dabei

- sowohl die (alarmauslösende) Real-Time-Überwachung sämtlicher Netzaktivitäten als auch retrospektive Verfolgung von historischen Missbrauchs-Versuchen,
- Erkennen von Attacken sowohl von externen Nichtberechtigten als auch von internen Berechtigten, die ihre Rechte/Privilegien missbrauchen,
- Adaptions- bzw. Erweiterungsmöglichkeit für Nicht-UNIX-Umgebungen,
- Methoden-Mix bei der Analyse der Audit-Daten.

Folgende Methoden der Datenanalyse werden kombiniert:

a) *statistische Komponenten:* Benutzer- oder gruppenspezifische „Normalverteilungen“ (Profile) des Verhaltens werden definiert (anhand von Merkmalen wie z.B.: Zeit, in der der Computer normalerweise benutzt wird, Art und Anzahl der Kommandos, die der Benutzer normalerweise verwendet, Netzaktivitäten nach Typ, Tippgeschwindigkeit (keystroke dynamics) etc.)
b) *regelbasierte Komponenten:* bekannte Schwächen des eigenen Netzes, bekanntgewordene Angriffs-Szenarios, verdächtige Verhaltensmuster etc.

c) *sonstige Komponenten:* Falltüren (trap doors) für Angreifer (z.B. Schwindelnutzerkennungen mit „magischen“ Passwörtern etc.), Daten über Änderungen des Benutzerstatus, neue Nutzer, abgelaufene Nutzerkennungen, Urlaubszeiten von Nutzern, Umzüge von Nutzern etc.

Diese Systeme sind laufend iterativ an die (sich ändernden) lokalen Gegebenheiten anzupassen, um die Zahl der Fehlalarme auf ein akzeptables Maß zu beschränken, ohne dabei die verdächtigen Aktivitäten zu verlieren.

Name	Zweck	Entwickler	Informationen
NIDES	Next Generation Intrusion Detection Expert System	Computer Science Laboratory, SRI International, Menlo Park, California	http://www.csl.sri.com/trlist.html
IDIOT	Intrusion Detection in Our Time	COAST-Projekt (Computer Operations, Audit, and Security Technology)	http://www.cs.purdue.edu/coast/coast-tools.html
AID2	Adaptive Intrusion Detection and Defense System — ein System zur Erkennung und Bekämpfung von Einbrüchen in heterogenen Rechnernetzen	Brandenburgische Technische Universität Cottbus (Lst. für Rechnernetze und Kommunikationssysteme, Cottbus)	http://www-rnks.informatik.tu-cottbus.de/rnks/german/forsch.html
NSA	Network Security Agent	Touch Technologies, Inc. San Diego, CA	http://www.ttisms.com/tti/nsa_www.html
NADIR	Network Anomaly Detector and Intrusion Reporter	Los Alamos National Laboratory — Operated by the University of California for the US Department of Energy	http://www.c3.lanl.gov/cic3/Projects/projects/teams/Security.shtml
GASSETA	Genetic algorithm for Simplified Security Audit Trail Analysis	Université de Rennes (Institut de Formation Supérieure en Informatique et Communication)	http://www.supelec-rennes.fr/rennes/si/equipe/lme/these/these-lm.html

Tabelle 9.3: Intrusion-Detection-Systeme

9.3.5 Folgerungen

Das Sicherheitsmanagement erfordert neben Hardware-Komponenten und Software-Werkzeugen vor allem personellen Betreuungsaufwand. Bei letzterem ist zwischen einmaliger oder gelegentlicher Beratung und einer laufenden Betreuung zu unterscheiden.

Eine einmalige oder gelegentliche Beratung wird beim Einrichten oder bei wesentlichen Veränderungen einer Netz- und Systemkonfiguration erforderlich sein. Dabei ist auch eine

Typprüfung für eine ganze Klasse von Netz- und Systemkonfigurationen denkbar. Diese Beratung sollte durch einen Spezialisten für Netz- und Systemsicherheit erfolgen, der einem eigenen Kompetenzzentrum angehört oder von einer kompetenten Beratungsfirma im Einzelfall verpflichtet wird.

Die laufende Betreuung, welche eine ständige Überwachung jedes Rechnersystems vor Ort und ein Verfolgen der Fachpresse über Meldungen von Einbruchsgefahren mit Umsetzung in die lokalen Gegebenheiten erfordert, kann nur durch einen ständigen Beauftragten bzw. ein ständig verfügbares Team für die Netz- und Systemsicherheit erfüllt werden. Für welche Bereiche ein solcher „Sicherheitsbeauftragter“ einzurichten ist und wie die lokale Sicherheitspflege und -verantwortung personell zu strukturieren ist, muss in Abhängigkeit von der Größe und Struktur der Institution in ihrer eigenen Sicherheitspolitik festgelegt werden.

9.4 Empfehlungen zum Netz- und Systemmanagement

- **Notwendigkeit für das Netz- und Systemmanagement.**
  Das Sicherheitsmanagement ist Teil des Netz- und Systemmanagements. Entsprechende Werkzeuge sind sowohl einzelne und spezielle Sicherheitswerkzeuge als auch umfassende Plattformen. In jedem Fall sollte eine Sicherheitspolitik (policy) definiert werden, in der die Ziele, die Zuständigkeiten und das Sicherheitsberichtswesen festgelegt werden. Die Verantwortlichkeit für Fragen der Sicherheit muss auch in den höheren Stufen der Hierarchie verankert sein. Nur was dort gewollt wird, erfährt die erforderliche Förderung.
- **Auswahl der Sicherheitswerkzeuge.**
  Bekannte und verfügbare Sicherheitswerkzeuge sollten als Minimalaufwand im Sicherheitsmanagement immer benutzt werden. Solche Mindestmaßnahmen können durch umfassende Auswertungen bereits eine hohe Wirkung haben. Die Verfügbarkeit und Auswahl von Sicherheitswerkzeugen wird sich im Laufe der Zeit ändern. Welche Art von Werkzeugen jedoch in welchen Zeitabständen eingesetzt werden sollen und wie die Ergebnisse in Sicherheitsberichte einfließen, muss durch die Sicherheitspolitik festgelegt sein.

  Beispiele von Sicherheitswerkzeugen sind:
  - Auswerten von Audit-Daten einschließlich Intrusion Detection,
  - Passwort-Scanner (prüft die Sicherheit von Passwörtern),
  - Netz- und System-Scanner sowie Anti-Scanner (z.B. SATAN, Prüfangriffe durch einen Sicherheitsverwalter bzw. Feststellen von Angriffen mit solchen Tools von außen).
- **Auswahl von Plattformen für das Netz- und Systemmanagement.**
  Das Netz- und Systemmanagement kennt unterschiedliche Funktionsbereiche. Eine Plattform sollte aus Sicht der Sicherheit folgende Funktionsbereiche unterstützen:

- Konfigurationsmanagement (die zu überwachende Konfiguration von Hardware und Software einschließlich Netz und Firewalls sowie Applikationen muss aktuell bekannt sein),
- Fehlermanagement (Fehler sind oft Punkte des Angriffs oder auch Folgen von Angriffen),
- Leistungsmanagement (im Stau können auch Sicherheitsanforderungen nicht mehr erfüllt werden; manche Angriffe zielen auf einen Leistungskollaps mit Ablehnung berechtigter Zugriffswünsche (Denial of Service)),
- Sicherheitsmanagement.

Eine Plattform für das Netz- und Systemmanagement sollte ein integriertes Sicherheitsmanagement erlauben. Die Auswahl einer geeigneten Plattform wird in Abhängigkeit von dem Basispaket und den verfügbaren Komponenten der Hardware und Software, von dem Grad der erforderlichen Sicherheit sowie von übergeordneten Planungen zu treffen sein. Die zweckmäßige Wahl ist leider auch von der aktuellen Verfügbarkeit und von Ankündigungen der Hersteller nicht unabhängig. Gängige Systemmanagementprodukte sollten im Rahmen eines Pilotprojekts bezüglich ihrer Eignung als Sicherheitsmanagementsysteme getestet werden. Für eine erste Auswahl ist besonderer Kenntnisstand über Marktprodukte aber auch über lokale Gegebenheiten erforderlich. Für eine Bestandsanalyse und erste Auswahl wird es zweckmäßig sein, auch externe Berater in Betracht zu ziehen.

- **Aufwand für das Netz- und Systemmanagement.**
  Der Aufwand für das Netz- und Systemmanagement wird hauptsächlich durch die laufenden Personalkosten geprägt sein. Die Kosten für Hard- und Software werden, bezogen auf die Dauer der Wiederbeschaffung, nur einen kleineren Anteil der jährlichen Kosten ausmachen. Von der Sache her ist das Sicherheitsmanagement ein Teil des Netz- und Systemmanagements und muss von der entsprechenden Personengruppe wahrgenommen werden. Das Applikationsmanagement wird meist von der gleichen Personengruppe wahrgenommen und deshalb hier mit einbezogen. Sicherheit ist als Qualitätsmerkmal innerhalb des Netz-, System- und Applikationsmanagements zu sehen. Das schließt nicht aus, dass die Funktionen innerhalb dieser Gruppe geeignet strukturiert und aufgeteilt werden, so dass Häufungen von Verantwortlichkeiten und die Gefahr des Missbrauchs vermieden werden. Eine Trennung innerhalb der operativen Ebene zwischen Netzmanager und Sicherheitsüberwacher wird nicht vorgeschlagen. Eine Überwachung der Netzüberwachungsaufgabe sollte vielmehr durch das Berichtswesen und die oben bereits genannte Verankerung der Verantwortlichkeit für Fragen der Sicherheit in allen Stufen der Hierarchie sichergestellt werden.

Es ist zu erwarten, dass im Bereich der Hochschulverwaltungen und Kliniken etwa 1/4 bis 1/3 des Netz-, System- und Applikationsmanagements speziell den Anforderungen der Sicherheit zuzuordnen ist. Eine solche relative Angabe des Aufwands erscheint zweckmäßig, denn wenn der Administrationsaufwand z.B. je Rechnerarbeitsplatz wegen eines geringen Kenntnisstandes seiner Benutzer hoch ist, dann ist auch mit einer relativen Erhöhung des Aufwands für Aufgaben der Sicherheit zu rechnen.

Über den Personalaufwand für das Netz-, System- und Applikationsmanagement lassen sich allgemeingültige Aussagen nur mit großen Vorbehalten machen, zumal der Aufwand in hohem Maße von der Homogenität des Rechnernetzes, von der Konfigurationsfreiheit der Arbeitsplatzrechner und der DV-Kompetenz ihrer Benutzer abhängt. Als grobe Orientierung können Erfahrungswerte für den Personalaufwand aus dem Bereich von Lehrstühlen einerseits und von Banken andererseits für das Netz-, System- und Applikationsmanagement einschließlich Sicherheitsmanagement dienen:

Im Bereich großer Lehrstühle, die etwa 100 Rechnerarbeitsplätze verwalten, ist mit 3 bis 4 Personen zu rechnen, deren Aufgabe ausschließlich im Netz-, System- und Applikationsmanagement einschließlich Sicherheitsmanagement besteht. Die zugehörigen Stellenwertigkeiten sollten sich auf BAT IIa bis IV verteilen. Im Bankenbereich liegt dieser Aufwand bei ca. 3 Personen je 100 Rechnerarbeitsplätze. Die Aufwandsangabe bezieht sich auf Infrastrukturdienstleistungen mit IT-Sicherheit; weitere Aufwendungen wie die Entwicklung, Anpassung und Betreuung spezieller Anwendungssoftware sind darin nicht enthalten. Dieser im Vergleich zur obigen Angabe etwas kleinere Aufwand ist sicher dadurch bedingt, dass es sich im letztgenannten Beispiel um ein sehr großes und homogenes Rechnernetz mit geringer Konfigurationsfreiheit der Rechnerarbeitsplätze handelt und das Management-Team als zentrale Kompetenz eine große Breitenwirkung hat.

9.5 Literatur

/Garfinkel96/ Garfinkel, S. / Spafford, G.:
„Practical UNIX *and Internet Security“,*
Bonn: O’Reilly 1996

/Ghetie97/ Ghetie, I.G.:
„Networks and Systems Management“,
Hingham/MA, Kluwer Academic Publishers 1997

/Hegering93/ Hegering, H.-G. / Abeck, S.:
„Integriertes Netz- und Systemmanagement“,
Addision-Wesley 1993

/Hughes95/ Hughes, L.J.:
„Actually Useful Internet Security Techniques“,
Indianapolis: New Riders 1995

/Seitz94/ Seitz, J.:
„Netzwerkmanagement“,
Thomson’s Aktuelle Theorien, Thomson Publishing 1994

Kapitel 10

Organisatorische und administrative Maßnahmen zur Verbesserung der Sicherheit in lokalen Netzen

Bauliche, technische, organisatorisch/administrative und personelle Maßnahmen können einen Beitrag zur Verbesserung der Sicherheit in Netzen leisten. Die Zuordnung der Maßnahmen zu den oben genannten Maßnahmengruppen ist nicht immer eindeutig. Aus diesem Grund lassen sich Überschneidungen zu anderen Kapiteln dieses Berichtes teilweise nicht vermeiden.

10.1 Generelle organisatorische und administrative Maßnahmen

Die Vernetzung von Arbeitsplätzen im Verwaltungs- und Klinikbereich und die Integration von Diensten, die über das lokale Netz hinausgreifen, bedingen/bewirken eine übergreifende, weitgehend verfahrensunabhängige Funktions- und Datenintegration.

So ist z.B. das Problem der Zugangskontrolle sinnvoll und zweckmäßig mittelfristig nur über entsprechende multifunktionale Chipkarten und spezielle Single-Signon- bzw. zentrale Berechtigungsserver zu lösen (siehe Kapitel 11).

Der Schutz personenbezogener Daten bzw. die Verfahrens- und Datensicherheit muss deshalb als Forderung an die Qualität des Netzes, seiner Komponenten und Dienste angesehen werden. Die bisher übliche Klassifizierung (vgl. z.B. /DFN96/) von Aufgaben hinsichtlich der Schutzwürdigkeit personenbezogener Daten bzw. des Sicherheitsbedarfs (Beeinträchtigung der Handlungsfähigkeit) geht von festen Verfahrensgrenzen aus, die so bei multifunktionalen Clients unter Aspekten der Netzsicherheit nicht gegeben sind.

Jedes Verwaltungs- bzw. Kliniknetz muss einen Grundschutz gewährleisten, der sowohl Anwendungen als auch Basisdienste unter Wahrung der Vertraulichkeit, der Integrität, der

Verbindlichkeit bzw. Nichtanfechtbarkeit und der Verfügbarkeit zulässt. Erst dann ist eine Öffnung der Verwaltungs- und Kliniknetze zu vertreten.

Im Folgenden werden hauptsächlich organisatorisch/administrative Querschnittsmaßnahmen zur Verbesserung der Sicherheit in Netzen erörtert. Dabei stehen nicht so sehr Maßnahmen zur Abwehr von Attacken Externer im Vordergrund sondern solche Maßnahmen, die sich auf die Verfügbarkeit, also

- die Betriebssicherheit und Zuverlässigkeit bzw.
- die Reduzierung der durch menschliches oder technisches Versagen ausgelösten Fehlfunktionen

positiv auswirken. Diese Maßnahmen „rechnen sich“, da sie einen kontinuierlichen Beitrag zur Verbesserung der Qualität, Produktivität und Akzeptanz der IT leisten.[1] Angesichts spektakulärer, oft auch durch kommerzielle Interessen geprägter Publizität von Attacken treten diese Aspekte der Sicherheit allzu häufig in den Hintergrund.

Organisatorisch/administrative Maßnahmen leisten einen Beitrag zur Netzsicherheit, indem sie gestaltend auf Strukturen und Abläufe einwirken, damit Informationsverarbeitung sicherer ablaufen kann. Neben Auswahl, Kombination und Anordnung technischer Komponenten und Werkzeuge sind es Maßnahmen, die auf Mitarbeiter wirken, wie Aufgabenverteilung, Aus- und Fortbildung und nicht zuletzt die Schaffung eines Sicherheitsbewusstseins, die es ermöglichen, die Sicherheitspolitik und das -konzept in der Praxis um- und durchzusetzen.

10.1.1 Aufgabenverteilung und Zuständigkeiten

Die mit der Dezentralisierung der DV-Versorgung einhergehende neue Sicht von Verwaltungshandeln ist gekennzeichnet durch Ziele wie Kunden-, Mitarbeiter-, Prozess- und Management-Review-Orientierung. In dieser Umbruchsituation werden traditionelle Strukturen der Aufgabenverteilung und die Ablaufsteuerung, die aus der Zeit der zentralen Datenverarbeitung stammen, infrage gestellt. Es nimmt deshalb nicht Wunder, dass Prüfberichte von Rechnungshöfen in letzter Zeit die nicht oder nicht klar geregelte Geschäftsverteilung (Aufgaben, Zuständigkeiten, Vertretungen) beanstanden. Nicht vorhandene Ausbildungs- und Schulungskonzepte, die ebenfalls reklamiert werden, sind teilweise auch auf diese Umbruchsituation zurückzuführen; daneben spielen sicher auch Personalengpässe und teilweise auch mangelnder Qualifizierungswille für neue Aufgaben eine Rolle.

Die Umbruchsituation von der zentralen zur dezentralen DV-Versorgung wird von Fachabteilungen der Verwaltungen aber auch häufig dazu benutzt, an bestehenden Kompetenzen, Richtlinien und Regelungen vorbei, den Erfolg im Alleingang zu suchen. Die Verfügbarkeit von DV-Leistungen wird dabei vielfach gefährdet durch unkoordinierte Beschaffung, unkontrollierten Einsatz unterschiedlicher Softwareprodukte und inkompatibler Arbeitsplatzsysteme, dadurch zwangsläufig auftretende Medienbrüche und häufig auch mangelnde

[1] The Australian National University (ANU) definiert z.B. neben den allgemeinen Sicherheitsrisiken ausdrücklich auch „Loss of staff productivity, ineffective information sharing, under-utilisation of computing resources“ als IT-Risiken. (`http://www.anu.edu.au/its/policies/its3.html`)

Wartungssicherheit der Anwendungen. Nicht unterschätzt werden darf auch das von selbsternannten „PC-Experten“ in den Fachabteilungen ausgehende Gefährdungspotential.

Zunehmend zu einem Risiko werden die unterschiedlichen Reifegrade (Alter) der eingeführten und in der Übergangszeit weiter zu betreibenden Anwendungen, die nur schwer in die neuen Versorgungsstrukturen integriert werden können. Sie werden — obwohl teilweise Kernsysteme — oft als „auslaufende Modelle“ nicht mit der gebotenen Sorgfalt gewartet.

Flexible Teamstrukturen, die erforderlich sind, um eine prozessorientierte Reorganisation von Verwaltungsabläufen auf den Weg zu bringen, beginnen sich erst langsam zu bilden. Die praktische Umsetzung gewonnener Erkenntnisse dauert länger als erwartet und führt vielerorts zu Unzufriedenheit über DV-Verantwortliche und -Mitarbeiter.

Eine optimale, allgemeingültige Organisationsstruktur für die DV-Versorgung von Hochschulverwaltungen und -kliniken unter dem Aspekt der Netzsicherheit lässt sich derzeit nicht definieren. Zu unterschiedlich sind bestehende Organisationsformen, Technik- und Kommunikationsbedarf, Größe der Einheiten, Infrastruktur und Reifegrad der Anwendungen.

Kristallisationspunkte der diskutierten neuen Aufgabenverteilung sind:

- Analyse, Modellierung, Koordination/Organisation der Geschäftsprozesse unter Nutzung der neuen Netzdienste und Einsatz von Werkzeugen zu ihrer Optimierung,
- integriertes Netz-, System- und Sicherheitsmanagement (siehe Kapitel 9),
- Benutzerservice (Helpdesk),

wobei für alle Teilbereiche generell die Notwendigkeit systematischer, verstärkter Fortbildungsmaßnahmen betont wird.

Reorganisation der Geschäftsprozesse

Eine Menge von Aktivitäten, die von verschiedenen Personen in einer definierten Reihenfolge sequentiell, parallel oder alternativ ausgeführt werden, bilden einen Geschäftsprozess. Prozess-(Vorgangs-)orientierung beinhaltet die Abkehr von der funktionalen Trennung nach Aufgabengebieten; die durch die Aufbauorganisation vorgegebenen Grenzen und Strukturen in Form von Abteilungen werden im Interesse der ablauforientierten und integrierten Steuerung aufgebrochen. Jeder Mitarbeiter übernimmt nicht nur eine Funktion innerhalb einer organisatorischen Einheit sondern Verantwortung innerhalb von Prozessen.

Das systematische Management von Geschäftsprozessen unter Einsatz geeigneter informationstechnischer Hilfsmittel dient der Minimierung von Reibungsverlusten und leistet einen nicht zu unterschätzenden Beitrag zur Erhöhung der Verfügbarkeit, Sicherheit und Akzeptanz von IT-Leistungen:

- Stark strukturierte standardisierbare Prozesse mit hohem Koordinierungsbedarf (Optimierung durch Modellierung, Analyse/Abbildung in einer Organisationsdatenbank und Simulation) werden durch *Workflow-Management-Systeme* (Koordinierungssysteme),

- eher schwach strukturierte Abläufe werden durch *Groupware-Systeme* (variierendes kooperatives Agieren und Reagieren im kommunikativen Bereich) unterstützt.

Im Rahmen dieses Berichts kann auf Werkzeuge zur Unterstützung von Prozessmodellierung und kooperativem Arbeiten nicht näher eingegangen werden.

Impulsgebend für die Optimierung von Universitätsprozessen war ein vom Bayerischen Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst in Auftrag gegebenes Forschungsprojekt (1994 – 1996). Es hatte die „Analyse der Aufgaben im Bereich der Infrastruktur bayerischer Universitäten und die Erarbeitung von Vorschlägen zur strukturellen Neugestaltung von Aufgaben, Handlungsabläufen und Kompetenzen, die wirtschaftlich sind und den Erfordernissen von Forschung und Lehre optimal Rechnung tragen“, zum Inhalt.

Die in der Untersuchung aufgezeigten Rationalisierungspotentiale im Bereich standardisierter oder standardisierbarer Vorgänge durch Selbstbedienungskonzepte wurden durch das Pilotprojekt „Einführung einer Multifunktionalen Universitätschipkarte (MUCK)“ aufgegriffen und führen in einem ersten wesentlichen Schritt zur praktischen Umsetzung der im Rahmen des Forschungsprojekts „Optimierung von Universitätsprozessen“ gewonnenen Erkenntnisse.

Benutzerservice

Neben der prozessorientierten Betrachtungsweise und den sich daraus ergebenden tiefgreifenden Änderungen von Strukturen (Aufgabenverteilung, Verantwortung) und Abläufen wird besondere Bedeutung auch der Organisation der Benutzerbetreuung beigemessen. Stand bisher Hilfe bei Problemen mit der Anwendersoftware im Vordergrund, müssen Mitarbeiter des Benutzerservice das immens gewachsene Fehlerpotential komplexer Anwendersoftware, diverser Betriebssysteme und der Nutzung von Diensten und Netzen abdecken. Die zentrale Forderung lautet, das „Turnschuh“-Management durch ein effizientes Störungs-Management abzulösen. Dies kann erreicht werden durch strukturelle Maßnahmen, Regelungen und den Einsatz geeigneter Werkzeuge, wobei auch hier gilt, dass der Einsatz von Werkzeugen bestehende Organisationsdefizite nicht ausgleichen kann:

a) strukturelle Maßnahmen:
In dem weit gespannten Spektrum von totaler Auslagerung (outsourcing) bis „jeder Anwender hilft sich selbst“ kristallisiert sich ein Stufenmodell der Organisation des Benutzerservice heraus:

- Eine zentrale Anlaufstelle (Hotline) für alle Probleme,
- First-Level-Betreuung für den direkten Anwenderkontakt, für die sich „geduldige Generalisten“ mit sozialer Kompetenz am besten eignen,
- in der zweiten Ebene des Benutzerservice sollen verschiedene Experten (Kompetenzzentrum) mit breitem technischen Wissen eingesetzt werden, die auch präventiv Fehlerquellen erkennen und beseitigen.

An Hochschulen werden im Benutzerservice häufig Werkstudenten beschäftigt. Den daraus resultierenden Datenschutz- und Sicherheitsproblemen ist durch entsprechende Aufklärung, (Dienst-)Anweisungen und verstärkte Kontrolle Rechnung zu tragen.

Zur Vermeidung des Burn-Out-Syndroms der Mitarbeiter des Benutzerservice müssen diese Maßnahmen durch ausreichende Schulung/Fortbildung sowie durch Eigenmarketing begleitet werden, da diese Mitarbeiter problembedingt immer im Rampenlicht interner Kritik stehen.

b) Regelungen:

Anzustreben ist eine Servicevereinbarung. Diese enthält Festlegungen zum anspruchsberechtigten Benutzerkreis, Servicezeiten, Umfang und Qualität der zu erbringenden Dienste. In ihr werden auch die standardisierten Ablaufprozesse sowie die Eskalationsregeln für kritische Situationen aufgezeigt.

Die Inanspruchnahme des Benutzerservice ist intern zu verrechnen. Aus dem Berichtssystem können Aufschlüsse über einen evtl. vorhandenen Schulungs- oder Geräteerneuerungsbedarf gezogen werden.

c) Einsatz von Werkzeugen:

Nichtkommerzielle Problem-Management-Tools zur Störzettelverwaltung und Unterstützung des Benutzerservice wie z.B. Trouble-Ticket-Systeme (TT-Systeme) sind nicht sehr zahlreich und verfügen über einen recht unterschiedlichen Reifegrad:

Produkt	Charakteristik	Quelle
GNATS	Problemberichtssystem	ftp://prep.ai.mit.edu/pub/gnu/gnats-3.2.tar.gz
NEARnet	Trouble-Ticket-System	ftp://ftp.ccs.neu.edu/pub/sysadmin/tracking/
NETLOG	Trouble-Ticket-System	ftp://ftp.ccs.neu.edu/pub/sysadmin/tracking/
Open Track	Problemverfolgungssystem	http:/www.osf.org/mall/tools/ot/index.htm
PTS/XPTS	Problemverfolgungssystem	http://www.halcyon.com/dean/pts/html
Web/PTS	Problemverfolgungssystem	http://ftp.urz.uni-heidelberg.de/ftp.pub/x11/contrib/applications/pts/

Tabelle 10.1: Nichtkommerzielle Problem-Management-Tools

Oft sind Problemverfolgungssysteme auch Bestandteil sogenannter Management-Suites, die wegen der bestehenden Interdependenzen integrative Teillösungen für Softwareverteilung, Lizenzkontrolle, Virenschutz, Inventarisierung, Backup & Restore, Remote Control sowie Help-Desk-Unterstützung anbieten:

Hersteller	Produktname	Softw. Vertlg.	Inventarisierung	Virenschutz	Helpdesk	Lizenzkontr.	Backup u. Rest.	Remote control	Informationen
Capacity	Netcon Management Suite	x			x	x		x	www.capacity.com
Intel	LANDesk Management	x		x		x		x	www.intel.com
McAfee	McAfee Enterprise		x	x	x	x	x	x	www.mcafee.com
Seagate Software	Desktop Management Suite	x	x	x			x	x	www.seagate.software.com
Symantec	Norton Administrator Suite	x	x	x		x			www.symantec.com

Tabelle 10.2: Management Suites

Darüber hinaus werden für größere LAN's spezielle Problem-Management-Tools für verschiedene Plattformen angeboten z.B.:

- Action Request System (ARS) der Fa. Remedy Corp. (ca. 70% Marktanteil),
- Paradigm von Computer Associates — integriert z.B. in NetView's AIX „Trouble Ticket/6000" und TRANSVIEW's „ComConsult Communication Manager (CCM)",
- Expert Advisor von Software Artistry,
- Advanced Help Desk von Computer Associates.

Die Problemverfolgung durch Trouble-Ticketing ist eine besondere Art der Vorgangsbearbeitung und sollte in das unternehmenseigene Workflow-Management integriert werden. Ein TT-System sollte folgende Funktionen unterstützen:

- Annahme von Meldungen über Telefon (manuelle Erfassung), per E-Mail oder File-Transfer bzw. WWW sowie automatische Generierung von Trouble-Tickets aufgrund von Alarmen und Ereignissen aus dem Systemgeschehen (Netz-Monitor-Tool),
- Definition von Funktionen, Verantwortlichkeiten und Laufwegen,
- Time-out-Kriterien sowie Benachrichtigungs- und Eskalationsregeln,
- Generierung von Berichten und Statistiken.

Meldet z.B. das Netz-Monitor-Tool dem TT-System eine zu starke Serverbelastung, wird automatisch ein Trouble-Ticket generiert. Über E-Mail oder einen Pager wird versucht, den zuständigen Mitarbeiter zu veranlassen, z.B. Benutzerprozesse anzuhalten. Reagiert dieser innerhalb der vorgegebenen Zeit nicht, eskaliert dieses Trouble-Ticket und wendet sich automatisch an die nächst höhere Instanz. ARS (Remedy Systems) integriert darüber hinaus sogenannte *Flashboards* — Zustandsberichte, die Aussagen über häufig vorkommende Netzfehler, Überlastsituationen und Ausfälle beinhalten.

Bei der automatischen Erzeugung von TT ist darauf zu achten, dass die Zahl der übertragenen Störmeldungen durch den Einsatz von Filtern und Alarmkorrelationen relativ gering gehalten wird, da eine zu große Anzahl die Problemlösung selbst negativ beeinflusst. Werden TT-Systeme in Netz- und Sicherheitsmanagementsysteme integriert, ist darauf zu achten, dass diese dadurch nicht korrumpierbar werden. Fortgeschrittene TT-Lösungen integrieren Techniken von Expertensystemen, um das angesammelte Wissen besser zu strukturieren und allgemein (auch zur Entlastung des Benutzerservice) verfügbar zu machen.

10.1.2 Beschaffung unter Berücksichtigung von Sicherheitsaspekten

Werden bei der Entwicklung oder beim Kauf von IT-Systemen oder -Komponenten Sicherheitsmechanismen nicht oder nur unzureichend berücksichtigt oder unkoordiniert beschafft, müssen diese evtl. durch Zusätze realisiert werden bzw. es entstehen *Insellösungen* im Bereich der Verschlüsselungssysteme, Zugriffs- und Zutrittskontrollen, Chipkarten, Virenerkennung etc. Häufig werden durch neue oder durch Kombination unterschiedlicher nicht abgestimmter Sicherheitskomponenten auch neue Sicherheitslücken geschaffen.

In der Welt der offenen Systeme und oft frei verfügbarer Sicherheitskomponenten (z.B. TIS Security Toolkit, PGP, SSH Secure Shell etc.) bzw. kommerzieller Ergänzungsprodukte (z.B. UniDesk, KIOFFICE-UX, SAFEGUARD, F-Secure von DataFellows) wird es immer schwieriger, homogene Sicherheitskonzepte zu realisieren, die mit gegebener Personalausstattung in Verwaltungs- und Klinikumgebungen stabil und zuverlässig gepflegt werden können.

Vielfach gibt es von Standardprodukten Sicherheitslösungen, die ihren Preis auch hinsichtlich des erhöhten Administrationsbedarfs haben, z.B.: Trusted DG/UX von Data General, SINIX-S V5.42 (E2-Zertifikat), ICL-UNIX von International Computers Ltd. mit britischem E2-Zertifikat, DPX/20 CMW mit britischem E3-Zertifikat, IBM PR/SM ES/9000 mit britischem E4-Zertifikat.

Alle gängigen UNIX-Datenbanken haben Sicherheitsvarianten: INFORMIX-Online/Secure, Trusted ORACLE 7, INGRES/Enhanced Security, die nach ITSEC mit F3/E3 zertifiziert sind. Zu fragen ist, warum überhaupt noch „unsichere“ Produkte für UNIX und UNIX-Datenbanken angeboten werden und nicht — zumindest im Verwaltungs- und Klinikbereich — die Sicherheitsvarianten Standard sind? Ist der Bedarf nicht gegeben? Ist das Sicherheitsbewusstsein nicht ausgeprägt genug? Passen die Sicherheitsvarianten nicht zum Sicherheitskonzept? Sind sie in der Administrierung zu aufwendig bzw. zu teuer?

Beschaffungen für Komponenten in geöffneten lokalen Netzen werden künftig verstärkt den Sicherheitsaspekt zu berücksichtigen haben. Für jede Beschaffung ist zu überlegen, ob die zu beschaffende Komponente mit dem Sicherheitskonzept verträglich ist bzw. ob es unter dem Sicherheitsaspekt eine oder mehrere Alternativen gibt. Dabei ist der *built-in-security* in jedem Fall der Vorrang vor der *add-on-security* zu geben.

Für die existierenden Alternativen sollten „Rechnungen“ angestellt werden, die den Beitrag, den das Produkt zur Erhöhung der Sicherheit des IT-Systems leistet, ausweisen (Sicherheitsbeitrags-Rechnung). Dabei muss dem jeweils schwächsten Glied besondere Aufmerksamkeit gewidmet werden.

Vielfach, z.B. auch bei Firewall-Software, stellt sich die Frage, ob Sicherheitskomponenten mit angepasster „Freeware“ selbst realisiert oder ein kommerzielles Produkt gekauft werden soll.

Hier sollte das „Konzept einer Sicherheitsarchitektur“ wie sie als Ziel im Projekt „BASILIKA“ (Bayerische Sicherheitslösung für Dienstangebote in offenen Kommunikationsnetzen) formuliert wurde, berücksichtigt werden, nämlich „. . . marktgängige Sicherheitskomponenten und -standards zu einer modularen, offenen Sicherheitsplattform zu integrieren, die als eine eigene, unabhängig betreib- und wartbare Schicht zwischen offenem Netz und dem Dienstleistungsangebot im Behördennetz implementiert wird.“ [siehe Kapitel 11]

10.1.3 Erzielen von Interoperabilität durch Standards

Heterogene, offene (d.h. nicht proprietäre) IT-Strukturen und weltweite Kommunikation sind in hohem Maß auf Standardisierung von Ablaufprozessen und eingesetzter Technik angewiesen, wenn Dienste, Programme und Daten jederzeit verfügbar sein und die eingesetzten Komponenten möglichst reibungsarm zusammenwirken sollen. Standards sind notwendige Mittel, um Interoperabilität auf einem stark zersplitterten Markt (viele Anbieter, viele Komponenten, viele Käufer) mit immer kürzeren Innovationszyklen zu erreichen.

Extern definierte De-Jure- oder De-Facto-Standards

Die Schwierigkeit im Umgang mit Standards hat ihren Grund in der Vielzahl der Standards durch Normung (De-Jure-Standards) sowie der Industriestandards (De-Facto-Standards) bzw. in deren Antizipation zum Beschaffungszeitpunkt. Durch internationale Standardisierungskommissionen festgelegte Standards werden häufig durch Industriestandards, die oft weniger kompliziert sind und keine so aufwendigen Abstimmungsprozesse durchlaufen müssen, zeitlich überholt.

Häufig sind von Herstellern ins Leben gerufene Standardisierungsgremien kurzlebige strategische Allianzen, und erst der Markt entscheidet über die Durchsetzung.

Manchmal fehlen auch Brücken zwischen Standards: SNMP (Simple Network Management Protocol), das primär nicht für Desktop-PC entwickelt wurde, ist die eine Entwicklungslinie der Standardisierung im Bereich der Fern-Administrierung/Diagnose der Netzkomponenten, DMI (Desktop Management Interface)[2] im Desktop-PC-Bereich die andere.

In der Praxis besteht das Problem darin, durch Literatur- und Marktbeobachtung wichtige Trends rechtzeitig zu erkennen und in der Beschaffungspolitk für strategische Komponenten

[2] seit 1992 durch Digital, HP, IBM, Intel, Microsoft, Novell u.a.; Ziel „to make the unmanageable PC manageable“; um DMI-Produkte in Microsofts SMS einzubinden, sind jedoch Extensions erforderlich

zu berücksichtigen. Zu einem bestimmten Beschaffungszeitpunkt ist es jedoch oft schwer zu sagen, was Standard wird:

- So ist z.B. zum gegenwärtigen Zeitpunkt nicht klar, ob sich WINDOWSNT trotz Schwächen bei der Skalierbarkeit im unteren kommerziellen Bereich schon gegen die stark fragmentierte UNIX-Szene durchgesetzt hat.
- Über die Praktikabilität (besonders der „Remote Procedure Calls“) des von der Open Software Foundation propagierten Modells DCE (Distributed Computing Environment) für verteilte Datenverarbeitung gehen die Meinungen auseinander.
- Allgemein sind es die „Versus-Diskussionen“, denen besondere Beachtung geschenkt werden sollte (z.B. Thick Clients versus Thin Clients, ActiveX versus Java).

Welche Standards, insbesondere auch Sicherheitsstandards, für ein konkretes LAN von Bedeutung sind, ist auch davon abhängig, welche Standards die Hauptkommunikationspartner bzw. -Softwarelieferanten einsetzen. Hierdurch werden Sicherheitsvorgaben gemacht, ohne deren Erfüllung Kommunikationsmöglichkeiten nicht zugelassen werden.

Tendenziell werden immer mehr offene Standards (TCP/IP, HTTP, HTML, Java), auch Sicherheitsstandards wie z.B. Secure Hypertext Transfer Protocol (S-HTTP), Secure Sockets Layer Protocol (SSL), Secure Multipurpose Internet Mail Extension (S/MIME) aus dem innovativen Internet in das LAN übernommen, das sich dann als Intranet darstellt.

An Bedeutung gewinnen auch Standards, die durch internationale politische Gremien (UN, EU) vorangetrieben werden und — obwohl zunächst in der Privatwirtschaft eingesetzt — zu Katalysatoren im staatlichen Bereich werden:

- Electronic Commerce (EC): Projekt SEMPER (Secure Electronic Marketplace for Europe),
- EDI bzw. EDIFACT (Electronic Data Interchange for Adminstration, Commerce, and Transport) für den organisationsübergreifenden Dokumentenaustausch z.B. im Klinikbereich,
- EPHOS (The European Procurement Handbook for Open Systems), Richtlinien zur Beschaffung offener Systeme der Informationstechnologie und Telekommunikation,
- SANUS (Verbundvorhaben „Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmen auf der Basis internationaler Normen und Standards “, insbesondere die Umsetzung der EU-Richtlinie 90/270/EWG).

Hausstandards

Neben den für strategische Entscheidungen zu berücksichtigenden extern vorgegebenen Standards sind es jedoch vor allem die sogenannten Hausstandards, die einen wesentlichen Beitrag für den sichereren und verlässlicheren Einsatz der IT leisten können.

Unnötig viele unterschiedliche Komponenten für den gleichen Zweck im LAN erschweren die Administrierbarkeit, erhöhen den Schulungs- und Betreuungsaufwand, reduzieren die Austauschbarkeit technischer Komponenten, erschweren die Mobilität der Mitarbeiter und gefährden die Verfügbarkeit nicht nur der IT sondern auch des Benutzerservice.

Hausstandards sollten auf einem breiten Konsens beruhen, für einen definierten Zeitraum vorgegeben, fortgeschrieben und auch durchgesetzt werden, für:

- Standardarbeitsplätze hinsichtlich Konfiguration und Softwareausstattung, Versorgung mit Handbüchern etc., Regelungen zum Ersatz-Zeitpunkt von Altkomponenten,
- Standardisierung des Antrags- und Beschaffungsvorgangs, aber auch der Abnahme durch den Endnutzer (Qualitätskontrolle),
- Standardisierung der Einweisung und Schulung bei neuen Komponenten bzw. Nutzern inkl. Erläuterung des Sicherheitskonzepts, der Servicevereinbarung und Dienstanweisung.

Bei konkurrierenden Industriestandards (z.B. PostScript oder PCL) sollte man möglichst nur einen Standard unterstützen. Bei der Beschaffung von Standardsoftware ist zu regeln, wann bzw. für welchen Benutzerkreis neuere Versionen zur Verfügung gestellt werden sollen („Domino-Wirkung“ bei Einzelfallentscheidungen bzw. daraus resultierende Probleme im Rahmen des Versionsmanagements, Gewährleistung der Rückwärtskompatibilität). Die Beschaffungsvorgänge sollten gebündelt werden, um Pools von gleichartigen Geräten zu bekommen und Beschaffungskosten zu reduzieren.

10.1.4 Schulung und Fortbildung, Bewusstseinsbildung für IT-Sicherheit

Den größten Beitrag zur Betriebssicherheit und Zuverlässigkeit von Netzen und Systemen leisten gut aus- und fortgebildete Mitarbeiter in einem leistungsfördernden Betriebsklima. Ein nicht zu unterschätzendes Gefährdungspotential geht von schlecht ausgebildeten und/oder unzufriedenen Mitarbeitern aus.

Alle Schulungs- und Fortbildungsmaßnahmen sollen auch dazu genutzt werden, Sicherheitsbewusstsein zu schaffen und zu verbessern. Die Sicherheitspolitik und das Sicherheitskonzept müssen vorhanden sein und bekannt gemacht werden; die zum Teil vorhandene irrige Vorstellung muss ausgeräumt werden, dass Sicherheit nur den Schutz personenbezogener Daten beinhaltet.

Bei der Bewusstseinsbildung für Sicherheitsprobleme handelt es sich um einen permanenten Prozess, der innerhalb von Schulungsveranstaltungen aber auch punktuell durch den Benutzerservice aus aktuellem Anlass am Arbeitsplatz stattfinden muss. Dass dabei auf die jeweils neuen Dienste und deren spezifische Sicherheitsprobleme eingegangen wird, versteht sich von selbst.

Die Öffnung der engeren Verwaltung hin zu Verwaltungstätigkeiten an Fakultäten und Lehrstühlen (Prozessorientierung) wird durch vernetzte Arbeitsplätze und Dienste ermöglicht; sie bietet die Chance einer Annäherung und effizienteren Gestaltung von Abläufen, Annäherung aber auch im Verständnis für die unterschiedliche Sicht: Verwaltungshandeln ist auf Kontinuität und Stabilität ausgerichtet, vorschriftenorientiert und für

Mitarbeiter der Verwaltung dominant — wohingegen im Wissenschaftsbereich die dynamischeren, freieren Primärprozesse Lehre und Forschung dominieren und Verwaltungstätigkeiten eher nebensächlich und lästig sind.

Ausdruck dieser Annäherung muss eine Sicherheitspolitik sein, die die jeweils etwas andere Sicht akzeptiert, also auf einem breiten Konsens beruht und die im Bewusstsein der Benutzer präsent ist.

10.1.5 Notfallvorsorge in verteilten Systemen

Alle Maßnahmen, die ergriffen werden, um die Sicherheit in IuK-Systemen zu verbessern, haben u.a. das Ziel, den Notfall nicht eintreten zu lassen (disaster prevention), ihn vorbeugend zu vermeiden (siehe Kapitel 1). Trotzdem kann er nicht ausgeschlossen werden. Solche plötzlichen, unerwarteten Ereignisse treten erfahrungsgemäß immer zum ungünstigsten Zeitpunkt mit dem größtmöglichen Schaden auf und tendieren — sich selbst überlassen — zur Eskalation.

Zur Zeit der Zentralrechner konnte die Aufgabe der Notfallvorsorge für Anwendungen mit hohen Verfügbarkeitsanforderungen in Zusammenarbeit mit dem strategischen Lieferanten abgedeckt werden. Heterogene Systeme und verteilte Datenhaltung bei zunehmender Integration der Dienste erfordern im Rahmen der notwendigen Vorsorge geeignete infrastrukturelle Maßnahmen.

Datensicherungskonzept

Für die lokalen Netze der Hochschulverwaltungen und Kliniken mit mehreren Anwendungs- und Datenbankservern ist ein eigenes, konsistentes, zentralisiertes Backup/Recovery-Konzept zu realisieren, wenn die von den Hochschulrechenzentren für diese Aufgaben angebotenen Dienste keine Möglichkeit der Verschlüsselung schutzwürdiger und vertraulicher Daten bieten.

An dieses Konzept sind folgende Anforderungen zu stellen:

- Automatisches (scheduled) und benutzergesteuertes Backup/Restore,
- Unterstützung verschiedener Plattformen,
- einfaches Interface für Benutzer,
- Sicherungsmöglichkeit für geöffnete Dateien, logische und physische Laufwerke, Full- und Incremental Backups,
- möglichst geringe Beschränkungen der Speichergeräte/Formate, evtl. Storage-Roboter,
- integrierte Verwaltung der Sicherungsmedien,
- integrierter Virenscanner.

Unter WINDOWSNT verfügbare Backup- und Recovery-Systeme sind z.B. Cheyenne ARCserve, Legato Networker, Seagate Backup Exec. Das in WINDOWSNT standardmäßig

enthaltene eigene Backup-Programm (Utility) verfügt nur über einen begrenzten Leistungsumfang: eine zeitlich gesteuerte (scheduled) Datensicherung sowie das Sichern offener Dateien sind z.B. nicht möglich.

Notfallvorsorge

„Der Notfall tritt erst dann ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit nicht möglich ist und sich daraus ein sehr hoher Schaden ergibt“. (BSI, IT-Grundschutzhandbuch 1996)

Organisatorisch/administrative Maßnahmen begleiten planmäßig die Aktivitäten zwischen Feststellung des Notfalls, Wiederanlauf (disaster recovery), eingeschränktem Betrieb und Herstellung der Betriebsbereitschaft (business continuity). Die Maßnahmen basieren auf den in der Risikoanalyse definierten Verfügbarkeits- und Sicherheitsanforderungen und den Beschreibungen der Komponenten des IT-Systems.

Für das daraus abgeleitete **Notfall-Handbuch** empfiehlt das BSI folgenden Aufbau:

- **Sofortmaßnahmen**
  1. Alarmierung im Notfall: Alarmierungsplan, Adresslisten und Notrufnummern, Festlegung konkreter Aufgaben für einzelne Personen,
  2. Handlungsweisen für spezielle Ereignisse (z.B. Sabotage, Brand, Stromausfall, Diebstahl, Vandalismus etc.)
- **Regelungen für den Notfall**
  3. Allgemeine Regelungen (Notfallverantwortliche, Kompetenzverteilung, Verhaltensregeln)
  4. Tabelle der Verfügbarkeitsanforderungen
  5. Wiederanlaufplan für Komponenten (Wiederbeschaffungsmöglichkeiten, Ausweichmöglichkeiten, DFÜ-Versorgung, eingeschränkter Betrieb, Wiederanlaufreihenfolge)
- **Dokumentation**
  6. Beschreibung der IT-Systeme (Hard- und Softwarekomponenten, Bestandsverzeichnis der Systemsoftware und Systemdaten, Netzanbindungen, Beschreibung der IT-Anwendungen mit Dateiverzeichnis, Kapazitätsanforderungen, Datensicherungsplan etc.)
  7. Wichtige Informationen (Ersatzbeschaffungsplan, Hersteller- und Lieferantenverzeichnis etc.)

Bezüglich der Notfallvorsorge für den Ausfall der Firewall verweist das BSI auf die Maßnahmen für vernetzte UNIX-Systeme:

- Geeignete Aufbewahrung der Backup-Datenträger,
- Sicherungskopie der eingesetzten Software,
- sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen,

- regelmäßige Datensicherung.

„Die Einstellung der Filterregeln bei einer Erstinstallation und die Anordnung der Komponenten muss sicherstellen, dass alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Dies muss auch bei einem völligen Ausfall der Firewall-Komponenten gelten."

10.2 Spezielle organisatorische und administrative Maßnahmen

In diesem Abschnitt werden Maßnahmen dargestellt, die Teilaspekte der Verfügbarkeit betreffen, insbesondere solche Vorkehrungen, die den Umbruch der Informationstechnik begleiten und die Integration der neuen Dienste absichern können.

10.2.1 Datenträgerkontrolle und Virenschutz in lokalen Netzen

Für jedes lokale Netz mit PC-Clients stellt die Verwaltung insbesondere mobiler Datenträger eine organisatorische und administrative Herausforderung dar, die mit folgenden Teilaspekten beschrieben werden kann: Das Führen von Bestandsverzeichnissen, die äußerliche Kennzeichnung, die sachgerechte Behandlung und Aufbewahrung, der Versand sowie das Löschen von Datenträgern und die datenschutzrechtlich unbedenkliche Vernichtung ausgedienter Datenträger.

Das primäre Sicherheitsproblem bildet jedoch nicht die unzulängliche Verwaltung mobiler Datenträger, sondern deren Existenz und Verwendung am Arbeitsplatz schlechthin.

Wenn bzw. solange mobile Datenträger eingesetzt werden, müssen sie im Sicherheitskonzept berücksichtigt werden; dies gilt insbesondere auch für tragbare PCs (Laptop, Notebook).

Das Gefährdungspotential ist charakterisiert durch:

- Import/Export von Störprogrammen (Viren, Würmer, Trojanische Pferde),
- Verletzung lizenzrechtlicher Vorschriften,
- Datenverlust, Datenmanipulation, unberechtigte(s) Kenntnisnahme und Kopieren,
- Wiederanlaufprobleme wegen fehlender Notfalldisketten nach Zerstörung von Systemdateien.

Sicherheitsrelevante Vorkehrungen wie z.B. Arbeitsplatzcomputer ohne bzw. mit verschließbaren Diskettenlaufwerken (z.B. *PC-Security*, zertifiziert unter BSI-ITSEC-0040-1993), die diesen Risiken entgegenwirken, führen fast immer zu Einschränkungen für die Benutzer von Arbeitsplatzcomputern und damit häufig auch zu Akzeptanzproblemen gerade bei innovationsfreudigen Mitarbeitern. Um so wichtiger ist es, mit einem klaren, serverbasierten Konzept für Datensicherung, Softwareverteilung und -verwaltung die Zahl

der mobilen Datenträger in einem lokalen Netz auf ein unumgänglich nötiges Maß zu reduzieren.

Serialisierungssysteme und selbstentladende Datenträger

Eine Maßnahme zur Kontrolle virulenter Aktivitäten und des rechtmäßigen Datenaustausches in einem geschlossenen Benutzerkreis mittels Datenträger bilden sogenannte *Serialisierungssysteme*: Über einen Gateway-PC (auch Quarantäne-PC) wird der Import und Export von Daten und Programmen aus einem bzw. in ein Netz kontrolliert. Auf diesem Gerät werden alle für den Datenaustausch bestimmten Datenträger (hauptsächlich Disketten) serialisiert, d. h. auf eine bestimmte Art formatiert, gekennzeichnet und verschlüsselt. Nur der Gateway-PC kann auf serialisierte und fremde Datenträger zugreifen. Auf normalen Arbeitsplatzcomputern wird ein Serialisierungsprogramm in das Betriebssystem integriert, das lediglich das Lesen und/oder Schreiben von serialisierten Datenträgern ermöglicht. *Ringfence*, *PC-Bastion*, *Tb-Fence* und *D-Fence* sind etablierte Serialisierungssysteme im DOS/WINDOWS-Bereich.

Für den kontrollierten Datenaustausch zwischen UNIX-Systemen mit mobilen Datenträgern können selbstentladende, verschlüsselte Datenträger erzeugt und eingesetzt werden. Die Diskette enthält die zur Entschlüsselung benötigte Software: eine Startprozedur, ein Archiv mit der Decodierungssoftware und das eigentliche Datenarchiv. Voraussetzung zum Lesen des Datenträgers ist die Kenntnis eines Passwortes.

Tragbare PCs

Die Zunahme des *mobile computing* erfordert auch dessen Berücksichtigung im Sicherheitskonzept. Dabei ist dem besonderen Gefährdungspotential durch Diebstahl, Verlust und den daraus sich ergebenden Missbrauchsmöglichkeiten Rechnung zu tragen.

Bei namhaften Anbietern von Notebooks sind standardmäßig schon Schutzmechanismen gegen Missbrauch, Verlust oder Diebstahl integriert, z.B.:

- Passwort für den Systemstart,
- softwaremäßiges Sperren der Tastatur mit Freischaltung über ein Tastatur-Kennwort,
- Sperren der Boot-Möglichkeit über die serielle Schnittstelle,
- Ausschalten des Disketten- und Festplatten-Controllers,
- Sperren der seriellen und parallelen Schnittstelle,
- Deaktivieren des ROM-Setups,
- abschließbares Gehäuse, Sicherheitsbügel gegen Diebstahl.

Durch nicht allzu teure Ergänzungsprodukte kann die Sicherheit noch weiter verbessert werden, z.B.:

- zum Schutz gegen Diebstahl/Verlust durch alarmauslösende Bewegungsmelder, die nicht nur das Gerät sondern auch das Gerät im Behälter schützen können (siehe z.B. /DEFCON/)

- durch lokale Verschlüsselungssoftware, die kostenlos zur Verfügung gestellt wird, wie z.B. bei
  - F-Secure Desktop (/DataFellows/),
  - Verschlüsselungssoftware MIC (Bundesamt für Sicherheit in der Informationstechnik),
  - Wisocrypt (Wiso-Redaktion des ZDF /Wiso-ZDF/)

  oder kommerziell angeboten wird, wie z.B. bei
  - CryptoCard, Elkey, CompuSec; DataCrypt (/CE-Infosys/),
  - Cryptware (/Utimaco/).

Virenschutzkonzept als Teil des Sicherheitskonzepts

Die seit 1988 bekannt gewordenen *Viren* wurden im Wesentlichen aktiviert und verbreitet durch:

- Aufruf eines infizierten Programms (File-Viren),
- Starten eines Rechners mit einer infizierten Diskette (Boot-Viren).

Das bloße Lesen einer infizierten Datei oder Diskette führte nicht zu einer Aktivierung.

Mit dem Auftreten von *Makro-Viren* ab etwa 1994 entstand ein neues Gefährdungspotential:

- Ihre Aktivierung durch vermeintlich bloßes Lesen einer *Daten*-Datei ist möglich.
- Eine plattformübergreifende Ausbreitung kann nicht mehr ausgeschlossen werden.
- Das Verbreitungsrisiko ist gewachsen, da sie kommunikative Anwendungen wie E-Mail, das Herunterladen von Daten von WWW-Servern und Groupware-Anwendungen bedrohen.

Das Virenschutzkonzept als Teil des Sicherheitskonzepts hat folgende Aufgaben:

- Es soll das Problembewusstsein insbesondere auch bei den Internet-Anwendern schärfen. Dabei genügt es nicht, nur die Opfer-Rolle zu sehen; jeder PC-Nutzer kann unbeabsichtigt auch zum Täter werden, indem er Datenträger für andere Nutzer erzeugt bzw. Dateien im Netz bereitstellt oder übermittelt, die Viren o.Ä. enthalten.
- Weiterhin soll es durch den Einsatz von geeigneten, aufeinander abgestimmten lokalen bzw. serverbasierenden Tools dem Import und der Verbreitung von Viren entgegenwirken. Neben den herkömmlichen lokalen *On-Demand-Virenscannern* bzw. systemresidenten Virenwächtern (TSR-Scanner, Monitor/Behaviour-Blocker, Change-Detectors, Checksummers, Integrity-Checkers) sind dies neuerdings auch dienste-integrierte Virenwächter, die aus dem Netz empfangene Dateien automatisch auf bekannte Schadensfunktionen untersuchen.
- Schließlich soll es durch Regelungen bzw. Handlungsempfehlungen für den Schadensfall zur Schadensminimierung beitragen.

Nachdem die Hochschulrechenzentren für verschiedene Antiviren-Programme Landeslizenzen erworben haben, sprechen im Hochschulbereich keine Kostengründe mehr gegen ihren flächendeckenden (lokalen) Einsatz.

Antivirenprogramme für Netze sind z.B.

- McAfee mit VirusScan: kann separat gestartet werden, Vshield als speicherresidente Version,
- DataFellows F-Prot Professional, ebenfalls mit einer proaktiven Version Gatekeeper, sowie
- Dr. Solomons Antivirus Toolkit, Norman Virus Control, Thunderbyte Antivirus Utilities, IBM Antivirus Edition, Intel Landesk Virus Protect, Norton Antivirus etc.

Größtenteils können durch sie auch gepackte Archive (ZIP, ARJ, LZH etc.) gescant werden. Einige verfügen über eine Anbindung an Datensicherungssysteme (z.B. Norman Virus Control, McAfee, Cheyenne Inoculan). In den Virenscannern sind teilweise auch regelbasierte Komponenten enthalten, um bisher unbekannte Viren zu erkennen.

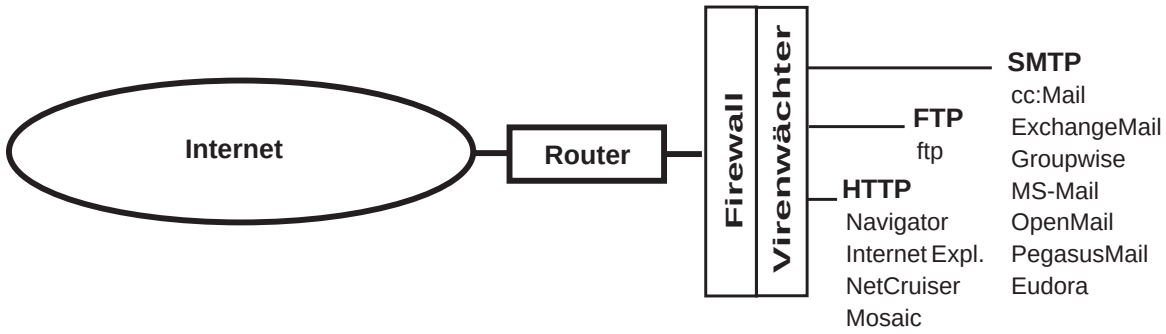


Abbildung 10.1: Internet-Gateway mit Virenschutz

Internet-Virenwächter stehen in ihrer Entwicklung erst am Anfang; im Zusammenspiel mit einer Firewall kann erzwungen werden, dass der netzübergreifende Datenverkehr auf Viren untersucht wird und infizierte Daten gar nicht erst an den Arbeitsplatz gelangen bzw. das LAN verlassen.

Hersteller	Produkt	Bemerkungen
McAfee	WebShield	für Intel-Plattformen, scant HTTP-, FTP- und SMTP-Pakete; kompatibel mit TCP/IP-basierten Firewalls; Schalter (on/off) für Java-Applets im HTTP-Protokoll
Trend Micro Inc.	InterScan VirusWall bzw. E-Mail VirusWall	für viele UNIX-Plattformen und als E-Mail-VirusWall für WINDOWSNT; integrierbar in Firewalls (BorderWare, Raptor Eagle, Checkpoint)
Integralis	MIMEsweeper	für WINDOWSNT primär zum Schutz von E-Mail-Systemen; ab Version 3.0 auch WWW (http und ftp) und NEWS (nntp)

Tabelle 10.3: Internet-Virenwächter

Lässt sich dies für E-Mail-Dienste, die im *Store/Forward-Verfahren* arbeiten, noch relativ leicht realisieren, so ist für Dienste, die normalerweise direkte Verbindungen aufbauen (FTP, HTTP), ein Proxy zwischen Client und Server erforderlich. Werden verschlüsselte Dokumente übertragen, ist die Grenze ihrer Einsatzmöglichkeiten erreicht, weshalb eine Virenüberprüfung auf jeden Fall auch am Endgerät erfolgen sollte.

10.2.2 Zertifizierte Netz- und Systemverwalter

Der Umbruch der IT und die daraus resultierende Dezentralisierung der DV-Versorgung und die Aufgabenumverteilung auf der Basis von Geschäftsprozessen und in Organisationseinheiten erfordern eine ständige Fortbildung der betroffenen Mitarbeiter.

Fehlende allgemeine Qualifikationsstandards bzw. die Freiwilligkeit der Qualifizierung für die neuen Aufgaben bergen Gefährdungspotentiale für die Verfügbarkeit und Sicherheit in lokalen Netzen. Netz- und Systemadministration und technischer Support auf hohem Qualifikationsniveau können einen wesentlichen Betrag zur Verbesserung der Verfügbarkeit und Sicherheit von Netzen und Diensten leisten.

Novell (Certified NETWARE Engineer: CNE) und Microsoft (Microsoft Certified Systems Engineer: MCSE) versuchen durch ihre Qualifikationsprogramme für ihre Produkte Anreize für eine standardisierte und kontrollierte Aus- und Weiterbildung (weltweit z.B. ca. 50 000 CNE's mit vergleichbarem Ausbildungssniveau) zu schaffen.

Ähnliche produktbezogene Zertifizierungsprogramme gibt es auch von Cisco, Bay Networks, Lotus Notes, Network General, IBM und anderen Herstellern.

Produktorientierte Zertifikate bestätigen die Fähigkeit, die Herstellersoftware ordnungsgemäß bedienen zu können. Sie sagen nichts aus über die Erfahrungen des Zertifizierten in einer Produktionsumgebung, in der besonders die Anwendung von *Troubleshooting-Techniken* gefordert ist.

Im Gegensatz zur Zertifizierung technischer Netzkomponenten kann man auch nicht davon ausgehen, dass der *Certified Engineer* die Leistung immer in gleicher Güte und auch im Alltagsstress erbringt.

Die Aus- und Weiterbildung von Mitarbeitern mit abschließender Zertifizierung stellen einen Anreiz dar, sich für eine Aufgabe zu qualifizieren. Punktesammeln allein bietet jedoch keine Gewähr für das Verständnis der zugrunde liegenden Methoden, wofür eine breitere Wissensbasis erforderlich ist. Ein Zertifikat sagt auch nichts über das in der Praxis erworbene Erfahrungswissen aus.

System-, Netz- und Datenbankadministratoren sollten über

- eine breite Wissensbasis,
- Qualifikationen hinsichtlich der eingesetzten Produkte,
- Erfahrungen in der Produktionsumgebung,
- ein großes Maß an Zuverlässigkeit bei der Aufgabenwahrnehmung sowie

- Vertrauenswürdigkeit

verfügen.

Administratoren von Firewall-Lösungen sowie deren Vertreter werden bei Bundesbehörden nach dem Sicherheitsüberprüfungsgesetz für VS-Vertraulich überprüft; damit wird die Dominanz von Vertrauenswürdigkeit[3] und Zuverlässigkeit zum Ausdruck gebracht.

Der hohe Stellenwert der Zuverlässigkeit von Personen, die an Zertifzierungsverfahren oder an der Ausstellung von Zeitstempeln mitwirken, wird auch in §10 der Signaturverordnung (SigV) betont.

10.2.3 Rekomposition der *root*-Rechte

UNIX-Systemverwalter mit Kenntnis des *root*-Passwortes haben uneingeschränkte Rechte; sie haben Zugriff auf alle Dateien und Kommandos und können auch mit technischen Mitteln nicht daran gehindert werden, alle Daten — auch Protokolldaten — abzufragen, zu verändern und zu löschen. Solche *Superuser* sind mit allgemein akzeptierten Sicherheitsanforderungen nicht vereinbar:

- Das Destruktionspotential ist zu groß.
- Es widerspricht dem Prinzip der geringsten Berechtigung.
- Die Zuordnung von Aktionen zu einem Benutzer (accountability) ist nicht gewährleistet.

Für den Umgang mit dem *root*-Account gelten deshalb besondere Regelungen:

- Die Zahl der Mitarbeiter, die das *root*-Passwort kennen, ist auf das Notwendigste zu beschränken.
- Die Anmeldung unter *root* ist nur an der Konsole, nicht aber aus dem Netz erlaubt.
- Der Superuser darf nach der Systeminstallation an den sicherheitsrelevanten Dateien keine Rechteänderungen vornehmen.
- Der Superuser darf keine zusätzlichen SUID- bzw. SGID-Programme mit privilegiertem Eigentümer einrichten.
- Der Superuser darf keine ihm unbekannten Programme unter seiner Kennung ausführen.
- Die Anmeldung darf nicht direkt unter *root* erfolgen sondern unter einer normalen Benutzerkennung unter Verwendung des Kommandos */bin/su*.

[3] etwas weitergehende Regelungen gelten für US-Behörden und auch deren Auftragnehmer: „All personnel doing work for or on behalf of the U.S. Government need to be trained on their overall responsibilities, have a security background check performed and be made aware of all aspects of security. This is particularly true for the Information Systems Security Officer (ISSO), the database administrator (DBA), and the system administrator (SYSADMIN).“ (Automated Information System (AIS) Design Guidance: `http://138.27.209.61/integ/`, Originalquelle mittlerweile passwortgeschützt)

- Beim Aufruf von Programmen sind immer absolute Pfadnamen zu verwenden (/bin/find, /bin/passwd etc.).
- *root* darf keine */.rhosts-Dateien* haben.
- Der Suchpfad von *root* darf das Verzeichnis „.“ nicht enthalten.

Das Problemfeld wird teilweise durch das frei verfügbare *sudo* abgedeckt. Es erlaubt limitierte *root*-Logins z.B. für Backups. Dabei benutzt *sudo* eine Datei /etc/sudoers, in der die *sudo*-Berechtigten gespeichert sind.

Allgemein wird jedoch empfohlen, das Aufgabengesamt der regelmäßigen Systemadministration in Teilaufgaben aufzuteilen, und zu Rollen gebündelt neu zusammengestellt (menügeführt — ohne Shell-Zugang) ausführbar zu machen. Das Einloggen unter *root* ist dann auf wenige Ausnahmen beschränkt und kann nur an der Konsole nach dem *Vier-Augen-Prinzip* erfolgen.

Zum Teil wird dieser Forderung in kommerziellen Standard-UNIX-Produkten schon Rechnung getragen (z.B. HP-UX ab Vers. 10.10 — *multiple administrators*).

Es sind auch kommerzielle Ergänzungsprodukte (RootManager, UniShield von NIT, SuSub von Technologic Inc.) sowie umfassendere Administrierungstools (z.B. AS/X von SNI) verfügbar. Für hohe Sicherheitsanforderungen stehen die speziell darauf ausgerichteten „B-Varianten“ von UNIX (siehe Kapitel 12.2) zur Verfügung.

Adminstrierungsaufgaben z.B.	wer ? (unter welchem user account)	was ? (mit welchen Privilegien)	wo ? (auf welchem System)	wann ? (zu welcher Zeit)
Konfigurierung der Audit-Subparameter				
Schreibzugriff auf Audit-Daten				
Abschalten des Audits				
Ändern des Eigentümers einer Datei				
Start von Programmen mit gesetztem SUID-Bit				
Montieren und Demontieren von Dateisystemen				
Einrichten von Gerätedateien				
Konfigurieren von Netzkomponenten				
Stellen/Synchronisieren der Systemuhr				
System herunterfahren (Shutdown)				
Installieren von Software				
Datensicherung				
Verwalten der Netzdienste				
Benutzerverwaltung				
Datenbankverwaltung				
Druckerverwaltung				
Einsatz von Sicherheits-Tools				
Auswertung von Protokolldateien				
Fernwartung				

Tabelle 10.4: Aufgaben der Systemadministrierung

10.2.4 Trennung von Test- und Produktionsbetrieb

Netzbasierende IT-Systeme sind ausgesprochen dynamisch. Verfügbarkeitsprobleme und Sicherheitslücken entstehen häufig dadurch, dass dem Einsatz neuer Komponenten — insbesondere neuer (auch konfektionierter) Software — kein dem Ausmaß der Änderung angemessener, geplanter Test vorausgeht.

- Werden Softwaretests mit Produktionsdaten oder Kopien von Produktionsdaten durchgeführt, ohne diese vorher zu anonymisieren, können Nichtbefugte Kenntnis von schutzwürdigen oder vertraulichen Daten erlangen.

- Wird neue Software mit Produktionsdaten im Produktionsbetrieb getestet, können Fehlfunktionen die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten beeinträchtigen; unvorhergesehene Seiteneffekte können zu Performanceverlusten oder Abstürzen des IT-Systems führen; durch Fehlverhalten der zu testenden neuen Software oder Bedienfehler können Produktionsdaten ungewollt verändert werden. Das Wiederherstellen des Ausgangszustands stellt sich bei vernetzten dynamischen Systemen und mehrfach genutzten (verteilten) Datenbeständen als schwierige Aufgabe dar (Problem der rückwärtsgerichteten Restauration in verteilten Rechnersystemen); bereits erstellte Arbeitsergebnisse müssen zeitaufwendig auf ihre Integrität überprüft werden.
- Verbleiben auf dem Produktionsrechner benutzerzugängliche Entwicklungswerkzeuge, können daraus erhebliche Sicherheits- und Datenschutzprobleme resultieren.

Das Aufstellen von Testplänen und die Durchführung der Tests nach diesem Plan können einen Beitrag zur Erhöhung der Sicherheit in Netzen leisten, da bereits im Test sicherheitsrelevante Probleme erkannt werden können:

- Die Testumgebung sowie das zu testende Produkt müssen vorher auf Störprogramme untersucht werden.
- Die Testumgebung, die unter Berücksichtigung von Kostengesichtspunkten die Produktionsumgebung möglichst genau abbilden soll, darf keine Seiteneffekte zum Echtbetrieb aufweisen.
- Bei der Generierung von Testdaten sind Standard-, Fehler- und Ausnahmefälle zu berücksichtigen; werden Kopien von Echtdaten verwendet, sind diese zu anonymisieren.
- Wurden im Testplan sicherheitsspezifische Anforderungen definiert, sind diese auf Wirksamkeit und Korrektheit, Stärke und Zwangsläufigkeit (Unumgänglichkeit) zu prüfen.
- Penetrationstests können potentielle Schwachstellen aufzeigen; sie sollten durch Protokollierungstools ergänzt werden.
- Mit Crashtests wird festgestellt, welche Schäden durch mutwillig oder zufällig herbeigeführte Systemabstürze entstehen können; gleichzeitig wird der Aufwand für einen ordnungsgemäßen Wiederanlauf des Produkts ermittelt.
- In Performancetests wird der Produktionsbetrieb im Hinblick auf eine starke Auslastung simuliert; sie liefern Indikatoren für Komponentenengpässe.

Schließlich muss sichergestellt werden, dass das Produkt in der Konfiguration, die aufgrund des Testbetriebs eingestellt wurde, in den Produktionsbetrieb übernommen wird und keine Entwicklungswerkzeuge in der Verfügbarkeit der Endnutzer verbleiben.

10.2.5 Fernzugriffe

Der Wunsch nach einem ortsungebundenen Netzzugriff hat viele Ursachen:

- Ferndiagnose, Fernwartung, Fernsteuerung, Fernadministration von Rechnern und technischen Komponenten — verstärkt durch die hohen zeitlichen und qualitativen Verfügbarkeitsanforderungen,
- zunehmende Mobilität der Mitarbeiter bzw. die Entwicklung immer leistungsfähigerer portabler Rechnertechnik und die Verfügbarkeit drahtloser Netzschnittstellen,
- Fernzugriffe auf Datenbanken (Remote Database Access) sowie Kommunikation und Kooperation in verteilten Systemen (Workgroup Computing, Computer Supported Cooperative Work (CSCW)),
- verteilte Anwendungen wie Telemedizin, Telearbeit, Teleteaching bzw. -learning.

Bei der Art der Realisierung von *Fernzugriffen* lassen sich folgende Varianten unterscheiden:

- Die klassische *Terminalemulation*, bei der sich der entfernte Benutzer direkt oder über einen Terminalserver einwählt,
- Fernsteuerung mit Hilfe von Remote-Control-Software (z.B. Timbuktu, Carbon Copy, Reachout, pcAnywhere, WinFrame); dabei übernimmt der entfernt stehende PC die Steuerung des Zielrechners,
- LAN-Erweiterung (Remote Node); der ferne Rechner verhält sich wie ein weiterer Netzknoten; der Benutzer hat transparenten Zugriff auf alle zur Verfügung stehenden LAN-Ressourcen und Netzdienste,
- anwendungsspezifische Lösungen (z.B. Lotus Notes Server) bzw. Zwischenformen.

Das Gefährdungspotential lässt sich global wie folgt beschreiben:

- Fernzugriffsmöglichkeiten sind die Hintertüren zum LAN und damit bevorzugte Angriffspunkte,
- Fernzugriffe laufen peripher, d.h. am Rande des normalen Betriebsgeschehens ab und sind in der Regel nicht auf Bürozeiten beschränkt,
- bei der Vielzahl der eingesetzten Technikkomponenten ist die Eingrenzung und Lokalisierung von Fehlern oft langwierig und schwierig.

Durch die zunehmende Öffnung lokaler Netze für den Fernzugriff ergibt sich ein erhöhter Sicherheitsbedarf gegenüber missbräuchlicher Verwendung, dem in einem **Sicherheitskonzept für Fernzugriffe** Rechnung zu tragen ist. Einige Grundsätze sind dabei unabhängig von den lokalen Gegebenheiten zu beachten:

- Da mit einem rasch zunehmenden Bedarf zu rechnen ist, sollte die Benutzer- und Rechteverwaltung möglichst frühzeitig auf der Basis nichtproprietärer Sicherheitsserver wie RADIUS (Remote Authentication Dial-In User Service) oder TACACS+ (Terminal Access Controller Access Control System) realisiert werden. RADIUS (RFC 2058) ist ein leistungsstarkes Werkzeug, mit dem sich Remote-Access-Sicherheitskonzepte

flexibel planen und einrichten lassen und das neben Authentifizierung (Prüfung der Identität) und Autorisierung (Prüfung der Rechte) eine Abrechnungsfunktion (Accounting) enthält.

- Erfolgt die Authentifizierung des Nutzers nicht über auf Token-Mechanismen basierende Einmalpasswörter (z.B. Defender, Secure ID), müssen Passwörter periodisch geändert werden.
- Nicht nur der Benutzer sondern auch der Einwahlort (Call-Back-Mechanismen) sollte überprüft werden.
- Nach Möglichkeit sollte eine einzige Sammelnummer für alle Fernzugänge angestrebt werden.
- Die Zahl sicherheitskritischer Einwahlpunkte sollte defensiv konfiguriert, unerwünschte Dialout-Verbindungen sollten explizit unterbunden werden.
- Fernzugriffsrechte sollten immer nur für eine bestimmte Zeit eingerichtet werden.
- Offene Netzverbindungen müssen korrekt abgebaut werden, damit die Übernahme der Verbindung von Nichtberechtigten ausgeschlossen ist.
- Hängende Modemverbindungen müssen durch einen Reset aufgelöst werden.
- Um die Nutzer vor überraschend hohen Telefonrechnungen zu schützen, sollte eine bestehende Verbindung bei längerer Inaktivität automatisch abgebaut werden.

Telearbeit als Spezialform des Fernzugriffs

Obwohl Telearbeit bereits seit zwei Jahrzehnten unter den verschiedensten Aspekten diskutiert wird, ist die praktische Relevanz eher untergeordnet (BRD: max. 3000 Arbeitsplätze — BMWi 31.10.1995). Eine revolutionäre Verbreitung der Telearbeit wird nicht mehr prognostiziert, eher eine evolutionäre. Die Probleme bei der Durchsetzung der Telearbeit sind primär nicht technischer oder wirtschaftlicher Art sondern liegen in den notwendigen, tiefgreifenden Veränderungen der Management- (Führung durch Zielsetzung und Eigenmotivation) und Arbeitstraditionen.

Allgemein werden folgende Aufgaben als telearbeit-geeignet angesehen:

- hoher Autonomiegrad der Aufgaben,
- Ansiedlung der Aufgaben im dispositiven und kreativen Bereich,
- ergebnisorientiert bewertbare Aufgaben.

Einzelfälle oder gelegentliche bzw. temporäre Telearbeit sind individuell zu regeln. Ein genereller organisatorisch/administrativer Regelungsbedarf stellt sich erst schritthaltend mit oder nach konkreten Pilotprojekten, u.a. auch deshalb, weil es sehr unterschiedliche Ausformungen und auch Mischformen der Telearbeit gibt: Normalarbeitsverhältnisse, Heimarbeit oder selbständige freiberufliche Tätigkeit, die nicht nur gelegentlich räumlich außerhalb der Hochschule in Nachbarschaftsbüros (Mitarbeiter verschiedener Unternehmen unter einem Dach), Satellitenbüros (ausgelagerte Zweigstellen) oder in der Privatwohnung ausgeübt werden.

Folgende Problemfelder werden diskutiert, die beim Start eines Telearbeitsprojekts von Bedeutung sind und sicherheitsrelevante Komponenten haben:

- **Weisungsrecht, Kontrolle, Zugangsrecht:**
  Telearbeit ist ergebnisorientiert; daraus ergibt sich in besonderem Maße die Möglichkeit des Einsatzes von technisierten Verhaltens- und Leistungskontrollen. Aber auch Methoden der Zeiterfassung und das Zutrittsrecht des Arbeitgebers sind im Rahmen solcher Projekte problembehaftet. Dieses Spannungsfeld zwischen grundgesetzlich geschützter Privatsphäre und arbeitsrechtlichem bzw. arbeitsschutzrechtlichem Zugangsrecht zur Privatwohnung des Telearbeitnehmers kann im Rahmen einer Dienstvereinbarung geregelt werden.
- **Kosten des Telearbeitsplatzes und Haftungsrisiko:**
  Ein Gefährdungspotential liegt in der Regel in der häuslichen Umgebung (sieht man von selteneren Satelliten- oder Nachbarschaftsbüros ab), der privaten Mitnutzung der vom Arbeitgeber zur Verfügung gestellten Arbeitsmittel sowie im Fehlverhalten von Familienmitgliedern und Besuchern. Haftungsfragen sollten nach bestehenden arbeits- und zivilrechtlichen Grundsätzen gelöst werden; auch der Abschluss einer Versicherung durch den Arbeitgeber ist möglich. Die Höhe des finanziellen Ausgleichs für den zur Verfügung gestellten Raum sowie der nachgewiesenen Nebenkosten ist (ggf. einzelvertraglich) regelungsbedürftig ebenso wie Umfang und Kostenzurechnung der privaten Mitnutzung.
- **Datenschutz, Datensicherheit:**
  Auf die Verarbeitung personenbezogener oder besonders schutzwürdiger (klassifizierter) Daten in Telearbeitsprojekten sollte verzichtet werden. Lässt sich dies nicht vermeiden, sollten sie frühzeitig gelöscht oder anonymisiert bzw. verschlüsselt werden.
- **Mietrechtliche Probleme:**
  Wird Telearbeit in Mietwohnungen ausgeübt, stellt dies eine teilweise gewerbliche Nutzung der Wohnung dar, mit der der Vermieter einverstanden sein muss. Zu bedenken sind auch (bauliche) Maßnahmen des Hauseigentümers, die Auswirkungen auf die Funktionsfähigkeit technischer Komponenten des Telearbeitsplatzes haben können.

Mit zunehmender Zahl von Telearbeitsplätzen wächst die Komplexität des Gesamtsystems und damit die Fehleranfälligkeit; bei verteilter Arbeit wächst gleichzeitig die Abhängigkeit von der eingesetzten Kommunikationstechnik. Dadurch erhöhen sich die Forderungen an die technische Zuverlässigkeit des IT-Systems sowie die Einbindung in optimierte Service-Strukturen.

Externe Fernwartung als Spezialform des Fernzugriffs

Die Problematik der Fernwartung unter datenschutzrechtlichem Aspekt zeigt folgendes Beispiel: In einer Klinik wird eine Patientenüberwachungsanlage (Hardware und Software) der Intensivstation vollständig per Standleitung aus San Diego/Kalifornien ferngewartet. An die technische Sicherheit und an den Betrieb des Verfahrens (Verfügbarkeit) sind sehr

hohe Anforderungen zu stellen. In den USA existieren keine mit deutschen Regelungen vergleichbaren Datenschutzgesetze.

Der zuständige Datenschutzbeauftragte schlug folgende Mindestmaßnahmen vor:

- Sämtliche über Namen und Geburtsdatum hinausgehenden personenbezogenen Merkmale sollten auf einem separaten PC, der nicht ferngewartet wird, gespeichert werden,
- alle Fernwartungsaktivitäten sollen manipulationssicher protokolliert werden,
- der Datenverkehr mit San Diego soll per Monitor überwacht werden können,
- der Systemzugriff per Fernwartung soll abgestuft erfolgen; erst wenn der nicht-privilegierte Zugriff nicht ausreicht, soll in den privilegierten Superuser-Status gewechselt werden können.

Die letzte Forderung wurde vom Hersteller abgelehnt. Datenmissbrauch (Kenntnisnahme von (Prominenten-)Patientendaten und deren Weitergabe) durch Fernwartungstechniker kann in einer solchen Konstellation nicht ausgeschlossen, die Strafandrohung nach §203 StGB (Verletzung der ärztlichen Schweigepflicht) schwerlich durchgesetzt werden.

Allgemein wird empfohlen, zur Sicherung der Fernwartung folgende Maßnahmen zu ergreifen:

- Die Modalitäten (Abgrenzung der Kompetenzen und Pflichten) der Fernwartung sollten in einem eigenen Vertrag geregelt werden, in dem auch die Weitergabe von Kundendaten an Dritte untersagt wird;
- der Verbindungsaufbau für die Fernwartung muss stets durch den Kunden erfolgen; die Anschlussnummern der zulässigen Partner sind fest zu verankern;
- das Wartungspersonal muss sich einer Anmeldeprozedur unterwerfen, die aus Identifikation und Authentifizierung besteht;
- die Fernbetreuung von Anwenderprogrammen ist unter einer Kennung vorzunehmen, die keine Systemverwalterprivilegien einschließt;
- es muss ausgeschlossen werden, dass Anwendungsprogramme durch die Fernwartung aktiviert werden können, solange noch Kundendaten in direktem Zugriff stehen;
- der Kreis des autorisierten Wartungspersonals ist genau festzulegen;
- der Zugriff auf Kundendaten ist grundsätzlich zu verhindern (z. B. physische Abtrennung von Laufwerken, Beschränkung der Zugriffsrechte); wird in einem Ausnahmefall der Zugriff auf personenbezogene Daten erforderlich, ist die Erlaubnis von einer vom Kunden autorisierten Person einzuholen;
- es muss ausgeschlossen werden, dass Kundenprogramme und -daten verändert werden können;
- alle Wartungs- und Übertragungsaktivitäten müssen vom Kunden mitgelesen werden; der Kunde muss die Fernwartungsarbeiten jederzeit abbrechen können; alle Aktivitäten des Wartungsvorgangs sind in einer Protokolldatei festzuhalten;

- werden Test- und Serviceprogramme des Herstellers auf der DV-Anlage gespeichert, sind diese unter der Wartungskennung zu speichern;
- das Einspielen von Änderungen ins Betriebssystem und in systemnahe Software im Rahmen der Fernwartung ist nicht zuzulassen, die Änderungen sind ausschließlich vor Ort vom Kunden oder nach Freigabe durch eine vom Kunden autorisierte Person des Herstellers durchzuführen.

10.2.6 Nutzungsrichtlinien im Verwaltungs- und Klinikbereich

Im Verwaltungs- und Klinikbereich werden der Betrieb, die Nutzung von Diensten, Ressourcen, Programmen und Daten durch Benutzerordnungen, Dienstanweisungen, Dienstvereinbarungen und allgemeine Appelle geregelt. Zweck dieser Ordnungen und Regelungen ist es, die IuK-Technologie ordnungsgemäß, d.h. rechtmäßig und zweckmäßig zu nutzen. Das Gefährdungspotential besteht darin, dass

- bei gleichzeitiger Gültigkeit einer Vielzahl von Regelungen ein eher diffuses Problembewusstsein vorhanden ist,
- verwaltungstypische Nutzer dabei mit Rechtsnormen und Strafandrohungen sowie DV-technischen Sachverhalten konfrontiert werden, die sie in vielen Fällen inhaltlich und in den Konsequenzen nur schwer beurteilen können,
- eine sachgerechte Information und mündliche Belehrung in der Regel nur bei der Beantragung einer formalen Benutzungsberechtigung *(account)* stattfindet. Die dabei zu unterschreibende Verpflichtung oder Erklärung ist kontextbezogen (Erlangung eines Rechts) und trägt schwerlich zu einer nachhaltigen Bewusstseinsbildung für den verantwortungsvollen Umgang mit den Ressourcen bzw. sicherheitsrelevanten Problemen bei.

Im Bericht der Arbeitsgruppe „Zugangs- und Nutzungsregelungen für die bayerischen Hochschulnetze“ /BSTUKWK97/ werden dort in Anhang A, B und C

- „Muster-Benutzungsrichtlinien — Benutzungsrichtlinien für Informationsverarbeitungssysteme der Universität ..... (1997)“, die
- „Benutzerordnung des DFN-Vereins — Benutzerordnung für das Zusammenwirken der Anwender der DFN-Kommunikationsdienste (1994)“ sowie
- „Datennetze — Ein Leitfaden zur veranwortungsvollen Nutzung von Datennetzen für Mitglieder von Institutionen in Bildung und Wissenschaft (gemeinsam herausgegeben vom Arbeitskreis der Leiter wissenschaftlicher Rechenzentren ALwR und vom DFN-Verein, Version 06.04.1993)“

aufgeführt, die einen akzeptierten Rahmen für die Nutzungsregelung der DV-Ressourcen an Hochschulen insbesondere im Bereich der Lehre und Forschung darstellen.

Die „Benutzerrichtlinien für die Nutzung des Internet“ des Bayerischen Landesbeauftragten für den Datenschutz — Referat Technik und Organisation — werden wegen ihrer Relevanz für Behörden/Nutzer in Hochschulverwaltungen im Anhang abgedruckt.

Ziel eines vernünftigen, d.h. rationalen und einsichtigen Sicherheitskonzepts muss es sein,

- die Nutzung der neuen Dienste durch klare Führungsentscheidungen gruppen- bzw. nutzerspezifisch zugunsten einer bedarfsgerechten Rechtevergabe zu regeln, und diese den Mitarbeitern verständlich und nachvollziehbar zu erläutern,
- die Benutzer schriftlich auf die Benutzungsrichtlinien zu verpflichten; bei deren Ausgestaltung ist „im Hinblick auf die rechtliche Beurteilung stets die Prüfung durch die Rechtsabteilung der Hochschule und/oder ein spezialisiertes Anwaltsbüro unverzichtbar“ (vgl. /BSTUKWK97/),
- jedem Nutzer eine eigene Ausfertigung der Benutzungsrichtlinien auszuhändigen, Stichproben bezüglich der Einhaltung der Regelungen — nach Ankündigung — durchzuführen, und jedem Missbrauchsverdacht nachzugehen,
- die darüber hinaus organisatorisch/administrativ zu regelnden Sachverhalte (Rechteerlangung und -verwaltung) durch Einsatz geeigneter systemimmanenter Sicherheitswerkzeuge und -prozeduren zu automatisieren (z.B. unsichere Passwörter gar nicht erst zuzulassen). Im Idealfall ist der typische Nutzer der Verwaltung nach Erhalt seiner Benutzerkennung nur für die sichere Verwahrung der Chipkarte und zur Geheimhaltung der PIN verantwortlich.

10.2.7 Organisationshaftung

Nachdem Rechtsfragen bei der Nutzung von Datennetzen im Arbeitsbericht „Hochschulnetze in Bayern“ /BSTUKWK97/ ausführlich behandelt werden, soll hier lediglich auf zwei Teilaspekte eingegangen werden, die organisatorisch/administrative Regelungen erfordern. Im Übrigen sei auf den o.g. Bericht verwiesen.

a) Die nicht lizensierte Nutzung von Computerprogrammen (inkl. Schriften und Dokumentationen)

„Behörden und Unternehmen, in denen Raubkopien zum Einsatz kommen, können im Rahmen des *Organisationsverschuldens*, unabhängig von der Schuldform (Vorsatz oder Fahrlässigkeit) vom Urheberrechtseigentümer schadenersatzpflichtig gemacht werden.“ (BSI: IT-Grundschutzhandbuch 1996, G 2.28)

Diese Gefährdung resultiert aus der mit Wirkung vom 9. 6. 1993 in Kraft getretenen Änderung des Urheberrechtsgesetzes (UrhG). Die eingesetzte Software und die erworbenen Lizenzen sind zu bilanzieren; nicht lizensierte Software ist entweder zu löschen oder durch Nachkauf zu legalisieren.

Solange Campus-Lizenzverträge *(site licenses)* unter Einschluss der Verwaltungen, Bibliotheken und Kliniken für Standardanwendungen nicht durchgesetzt werden können, muss darüber hinaus das unkontrollierte Einspielen von Software erschwert bzw. dem Problem der Haftung infolge Organisationsverschuldens durch organisatorische Maßnahmen Rechnung getragen werden:

- Verbot des Einspielens nicht lizensierter Software in der Dienstanweisung,

- Kontrollen (Stichproben) beim Endanwender durch die zuständige Stelle und Protokollierung (Beweissicherung).
- Einsatz von *Software-Metering-Werkzeugen* z.B:

Firma	Produkt
Network Utilities	AppMeter
Tally Systems	CentaMeter
Express Systems	Express Meter
LanMarque	KeyServer
ABC Systems & Developments	LAN Licenser
Target/Intel	LANDesk Management Suite
Target/Horizons Technology	LANrecord
Kernel Tweaks	License Track
Target/Attachmate	NetWizard
Symantec	Norton Administrator for Networks
McAfee	Saber LAN Workstation
McAfee	SiteMeter
Target/Seagate	SMART
ON Technology	SofTrack
Accurate Technology	Software Sentry
Microsystems Software	Software Sentry (Sentry Family Suite)

Tabelle 10.5: Software-Metering-Werkzeuge

b) Das Bereitstellen von Daten auf Servern

Werden auf Servern Bilder, Audiodaten, Videosequenzen oder Texte angeboten, ist zu prüfen, ob dadurch nicht urheberrechtliche Verwertungs- und Verbreitungsrechte verletzt werden. Beim Anbieten von Daten muss jede einzelne Datei kontrolliert werden, bevor sie allgemein verfügbar gemacht wird. Als praktikabel wird folgender Weg vorgeschlagen: In einen (Upload-)Bereich werden Dateien abgelegt; nur ein autorisierter Mitarbeiter kann den Bereich lesen; er kontrolliert die Dateien unter urheberrechtlichen (ggf. auch strafrechtlichen) Aspekten und kopiert sie anschließend in den allgemein zugänglichen Bereich.

Zum Problem der Haftung der Hochschule oder Hochschuleinrichtung für rechtswidriges oder inhaltlich falsches Informationsmaterial, das auf Servern der Einrichtung

zum Abruf gehalten wird, wurde vom DFN-Verein ein Rechtsgutachten in Auftrag gegeben, das unter dem Titel „Haftung des Vereins zur Förderung eines Deutschen Forschungsnetzes e.V. als Online-Diensteanbieter“ als DFN-Bericht Nr. 83 erschienen ist.

10.2.8 Organisatorische Maßnahmen zum sicheren Betrieb einer Firewall

Das BSI schlägt vor, neben den obligatorischen technischen Maßnahmen für den Betrieb von Firewalls folgende organisatorischen Maßnahmen zu ergreifen:

a) Sicherheitspolitik

In der Sicherheitspolitik (siehe Kapitel 1) muss festgelegt werden, welche Anwendungen für welche Benutzer und/oder Rechner zugelassen werden sollen und für welche Anwendungen Vertraulichkeit und/oder Integrität gewährleistet sein müssen.

Es muss festgelegt werden, welche Ereignisse protokolliert werden und wer die Protokolle auswertet. Die Protokollierung muss den datenschutzrechtlichen Bestimmungen entsprechen.

Die Benutzer müssen über ihre Rechte und insbesondere über den Umfang der Nutzdatenfilterung umfassend informiert werden.

Die Sicherheitsvorgaben sollen so beschaffen sein, dass sie auch zukünftigen Anforderungen gerecht werden, d. h. es sollte eine ausreichende Anzahl von Verbindungsmöglichkeiten vorgesehen werden. Jede spätere Änderung muss streng kontrolliert und insbesondere auf Seiteneffekte überprüft werden.

Es ist nötig, Ausnahmeregelungen insbesondere für neue Dienste und kurzzeitige Änderungen (z.B. Tests) festzulegen.

b) Geschlossener Sicherheitsbereich

Ein geschlossener Sicherheitsbereich für die Komponenten einer Firewall ist erforderlich. Es müssen mechanisch stabile Umfassungen (einbruchs- und feuerhemmend) für die beteiligten aktiven Geräte verwendet werden. Zutrittskontrolle hat zu erfolgen.

c) Administratoren

Den Administratoren der Firewall und deren Vertretern muss vom Betreiber großes Vertrauen entgegengebracht werden können. Sie haben in Abhängigkeit vom eingesetzten System weitgehende und oftmals alle Befugnisse. Sie sind in der Lage, auf gespeicherte Daten zuzugreifen, diese ggf. zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich ist.

Das eingesetzte Personal muss daher sorgfältig ausgewählt werden. Es muss in regelmäßigen Abständen darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administratoraufgaben verwendet werden dürfen.

Bei Administrierung durch Externe darf nur überprüften Personen unter Beachtung festzulegender erhöhter Sicherheitsmaßnahmen der Zugriff erlaubt werden.

d) Revision
Die Revision der Sicherheitsmaßnahmen (z.B. Access-Listen) und Protokolldateien muss durch eine unabhängige Stelle sowohl innerhalb der Behörde wie auch durch Externe unterstützt erfolgen. Dies können z.B. vom Hersteller beauftragte Fachleute sein. Die durchzuführenden Prüfungen sind in einem Prüfkonzept festzulegen, welches sich eng an die erstellten Sicherheitsvorgaben hält.

10.2.9 Der Umgang mit sicherheitsrelevanten Ereignissen

Das Gefährdungspotential im Umgang mit sicherheitsrelevanten Ereignissen liegt darin, dass

- Anomalien häufig zunächst dem weiten Bereich System-/Nutzer-Fehlverhalten, Kapazitätsengpässe und dergleichen zugeordnet werden und wertvolle Zeit vergeht, bis geplante Maßnahmen bzw. Regelungen greifen,
- Regelungen zur Behandlung solcher Ereignisse und zur Schadensbegrenzung — soweit es sie gibt — zu spät ergriffen werden, da Systemadministratoren zunächst Attacken als persönliche Herausforderung ansehen und durch ungeeignete Maßnahmen z.B. Panikreaktionen des Angreifers provozieren können,
- zum Zeitpunkt des Erkennens des Angriffes es oft schwer einschätzbar ist, welcher Phase der Kompromittierung des IT-Systems die Aktivität zuzuordnen ist:
  - lauschen, schnüffeln, Angriffspunkt finden,
  - sich maskieren, Privilegien erreichen,
  - stören, manipulieren, Schaden verursachen,
  - Spuren verwischen,

  bzw. welche Ziele der Angreifer verfolgt:
  - Anwesenheitsbeweis hinterlassen,
  - Störprogramme installieren,
  - sich rächen, d.h. Schaden verursachen,
  - unentdeckt in den Besitz von Informationen gelangen oder Daten manipulieren,
- in dem Bemühen, die Systemintegrität möglichst schnell wiederherzustellen, Spuren und Beweismittel vernichtet werden,
- durch verspätetes Einschalten von besonders ausgewiesenen Experten (z.B. DFN-CERT) gegebenenfalls falsche oder unzureichende Maßnahmen ergriffen werden,
- durch falsche Informationspolitk das Ansehen der betroffenen Institution beschädigt wird.

Sicherheitsrelevant sind alle Ereignisse, die die Integrität des IT-Systems gefährden bzw. es kompromittieren. Hinweise auf sicherheitsrelevante Ereignisse können gewonnen werden durch Informationen

- aus eingesetzten Sicherheitswerkzeugen,

- von externen Stellen (z.B.: Adresse des eigenen Rechners oder Nutzerkennungen tauchen in externen *Sniffer-Log-Dateien* auf),
- aus dem Betriebsgeschehen z.B. durch
  - Systemzusammenbrüche,
  - neue, unbekannte, seltsame Benutzerkennungen,
  - neuartige Dateinamen mit eigenartigem Konstrukt oder Suffix,
  - Account-Diskrepanzen (z.B. bei UNIX in der Datei /usr/admin/lastlog),
  - auffallende Änderungen der Dateigröße (z.B. bei DOS die *.EXE-Dateien),
  - Versuche, Systemdateien zu ändern,
  - das Verschwinden von Dateien, ohne dass diese gelöscht wurden,
  - die Verweigerung von Diensten (z.B. UNIX-System beendet Sitzungen zwangsweise und schaltet in den *Single-User-Mode*),
  - einen unerklärbaren System-Durchsatz (Performance),
  - Anomalien (z.B. unerklärbare *beeps* oder seltsame Meldungen am Bildschirm),
  - häufige, missglückte Login-Versuche insbesondere von anderen Rechnern aus,
  - verdächtiges, systematisches Durchsuchen von Systemdateien durch einen Benutzer mit *root*-Rechten,
  - aber auch durch auffälliges Verhalten unzufriedener (evtl. ausscheidender) Mitarbeiter.

Wenn sich der Verdacht erhärtet oder feststeht, dass eine Attacke stattfindet oder stattgefunden hat, sollte ein vorher definierter Regelmechanismus einsetzen. Ziel aller Aktivitäten sollte es sein, die Kontrolle über das Geschehen zu behalten bzw. wiederzugewinnen und das Ausmaß des Schadens so gering wie möglich zu halten. Es mag zwar interessant sein, die Aktivitäten eines Hackers zu beobachten, um ihn dingfest zu machen; aber unter dem Aspekt der Schadensminimierung kann es sinnvoller sein, den Rechner herunterzufahren oder vom Netz zu nehmen und die Sicherheitslücke zu schließen. Bis zur Klärung des Sachverhalts sind alle IT-Komponenten als suspekt anzusehen.

Damit ergibt sich folgende Vorgehensweise:

1. **Systematische Feststellung der Reichweite und Schwere des Ereignisses**
   Hierbei geht es zunächst wesentlich um die Beantwortung folgender Fragen:
   - Wo ist der Eindringungspunkt (Netz, Telefon, lokales Terminal etc.)?
   - Handelt es sich um ein lokal begrenztes Ereignis oder sind mehrere Computer des LAN bzw. auch externe LANs betroffen?
   - Sind schutzwürdige, insbesondere klassifizierte Informationen betroffen?
   - Welcher Schaden kann verursacht werden bzw. worden sein?
   - Welche strafbedrohten Tatbestände liegen vor und sollen Strafverfolgungsbehörden eingeschaltet werden?

   Die Kenntnis der möglichen Strafrechtstatbestände (siehe Kapitel 2) ist Voraussetzung für eine gezielte Beweissicherung, auch wenn zunächst Strafverfolgungsbehörden noch nicht eingeschaltet werden.

2. **Informationswege, Informationspolitik**
   Aufgedeckte sicherheitsrelevante Ereignisse sind meist spektakulär und damit für eine breitere Öffentlichkeit interessant, image-schädigend und verursachen nicht zuletzt auch materiellen Schaden. Zum frühestmöglichen Zeitpunkt ist die als zentrale Koordinationsstelle im Sicherheitskonzept bestimmte Stelle/Person zu informieren, die alle Aktivitäten koordiniert und verantwortet.

   Zu klären ist, wer informiert und in welchem Umfang informiert wird. Auch der Sprachgebrauch (je nach Adressatengruppe) ist zu regeln, insbesondere wann das Top-Management, die Presse oder die Strafverfolgungsbehörden unterrichtet werden.

   Wird ein CERT (Computer Emergency Response Team) z.B. das DFN-CERT eingeschaltet, ist es sinnvoll und nützlich, schon vorher vertrauenswürdige Kontakte (durch einen getesteten, verschlüsselten Informationsaustausch) aufgebaut zu haben und die unterschiedlichen Kommunikationswege zu kennen:
   - für konkrete Vorfälle oder Sicherheitslücken: `dfncert@cert.dfn.de`
   - für Anfragen und Kommentare: `info@cert.dfn.de`
   - für Subskription einer der Mailing-Listen: `win-sec-request@cert.dfn.de` bzw. `win-sec-ssc-request@cert.dfn.de` für den Arbeitskreis Sicherheit bzw. für Warnungen und Information des DFN-CERTs.
3. **Beweissicherung**
   Ein Protokollbuch ist zu führen, in dem das Systemgeschehen (mit Zeitstempel versehen), Handlungen und deren Begründung möglichst detailliert abgebildet und wichtige Gespräche chronologisch protokolliert werden.
4. **Wiederherstellung der Systemintegrität**
   Wenn gewährleistet ist, dass keine Beweismittel mehr verloren gehen können und alle nötigen Informationen über Art und Umfang der Attacke vorliegen, kann mit der Wiederherstellung der Systemintegrität und der Schließung der Sicherheitslücke begonnen werden.

10.3 Empfehlungen zu organisatorisch/administrativen Maßnahmen

Organisatorisch/administrative Maßnahmen leisten in Verwaltungs- und Kliniknetzen einen Beitrag zur Erhöhung der Sicherheit, indem sie gestaltend auf Strukturen und Abläufe einwirken. Gegenüber Attacken von außen wirken sie eher mittelbar und nur, wenn ihre Einhaltung auch kontrolliert wird; sie beeinflussen die Verfügbarkeit positiv und reduzieren das Gefährdungspotential, das von Innentätern, sei es fahrlässig oder vorsätzlich, ausgeht. Zu den organisatorischen Maßnahmen zur Verbesserung der Sicherheit von Netzen zählen auch Schulungs- und Fortbildungsmaßnahmen für alle Mitarbeiter, die IuK-Dienste nutzen oder administrieren.

- Dezentrale DV-Versorgungsstrukturen und neue Netzdienste bedingen eine Analyse und Neustrukturierung der DV-Aufgaben, die fokussiert werden durch

  - die Organisation der Geschäftsprozesse unter Nutzung der neuen Dienste,
  - ein integriertes Netz-, System- und Sicherheitsmanagement und
  - die Organisation eines effizienten Benutzerservice.
- Die Neustrukturierung muss ihren Niederschlag finden in einer klar geregelten Geschäftsverteilung (Aufgaben, Kompetenzen und Verantwortlichkeiten, Vertretung), insbesondere auch an der Schnittstelle zwischen Fach- und EDV-Abteilung sowie innerhalb von Geschäftsprozessen.
- Als neue Aufgabe ist das **IT-Sicherheitsmanagement** zu etablieren. Diese Aufgabe kann zweckmäßigerweise einem Team übertragen werden.
- Die zeitliche Verfügbarkeit und der Leistungsumfang des Benutzerservice sollten in einer *Service-Vereinbarung* geregelt, für die *Störzettelverwaltung* sollten geeignete Werkzeuge (z.B. ein Trouble-Ticket-System) eingesetzt werden.
- Beschaffungsmaßnahmen, insbesondere für strategische Komponenten, sind stärker als bisher auch im Hinblick auf ihre Verträglichkeit mit dem Sicherheitskonzept zu bewerten (Sicherheitsbeitrags- und Schwachstellenanalyse).
- Voraussetzung für eine hohe Verfügbarkeit und ein möglichst reibungsarmes Zusammenwirken von Diensten, Programmen und Daten (aber auch Mitarbeitern) sind neben der Reduktion der Komponentenvielfalt eine Standardisierung von Ablaufprozessen und eingesetzten Technik-Komponenten.
- Stark strukturierte Verwaltungsprozesse mit hohem Koordinierungsaufwand sollen durch Workflow-Management-Systeme unterstützt werden.
- *To buy or to make* sollte zumindest für sicherheitsrelevante Komponenten zugunsten von marktgängigen Sicherheitskomponenten und -standards entschieden werden. Bei Beschaffungsalternativen ist der *Built-in-Security* der Vorrang vor *Add-on-Security* zu geben.
- Die Kenntnis und das Bewusstsein über vorhandene Risiken bei der Inanspruchnahme der Netzdienste ist bei jedem einzelnen Nutzer zu verbessern; dies ist ein permanenter Prozess und kann im Rahmen von Schulungs- und Fortbildungsmaßnahmen aber auch aus aktuellem Anlass vor Ort erfolgen.
- Die Sicherheitspolitik und das Sicherheitskonzept müssen bekannt gemacht und durchgesetzt werden, Regelverstöße müssen auch Folgen haben. Die Ausgestaltung der Benutzerordnungen ist durch die Rechtsabteilung bzw. durch ein spezialisiertes Anwaltsbüro zu überprüfen. Jeder Benutzer ist auf die Benutzungsrichtlinien zu verpflichten. Jedem Benutzer ist ein Exemplar der Regelungen, zu deren Einhaltung er sich verpflichtet hat, auszuhändigen.
- System-, Netz- und Datenbankadministratoren sollten neben einer breiten Wissensbasis über ein hohes Maß an Zuverlässigkeit bei der Aufgabenwahrnehmung sowie Vertrauenswürdigkeit verfügen. Sie sind in besonderem Maße in Fortbildungsmaßnahmen einzubinden und durch leistungsgerechte Bezahlung zu motivieren. Die Aus- und Weiterbildung von System- und Netzadministratoren durch Zertifizierung können einen Anreiz darstellen, sich hinsichtlich der eingesetzten Produkte zu qualifizieren.

- Der Notfallvorsorge für Anwendungen mit hohen Verfügbarkeitsanforderungen ist durch ein durchgängiges Backup- und Recovery-Konzept Rechnung zu tragen. Die organisatorischen Maßnahmen, die die Aktivitäten zwischen Feststellung des Notfalls und Wiederherstellung der Betriebsbereitschaft planmäßig begleiten, sind im **Notfall-Handbuch** niederzulegen.
- Der Gebrauch mobiler Datenträger sollte auf ein unumgänglich notwendiges Maß beschränkt werden. Für schutzwürdige Datenbereiche sollten Serialisierungssysteme bzw. selbstentladende, verschlüsselte Datenträger eingesetzt werden. Für den Einsatz von tragbaren PCs sind je nach Einsatzgebiet eigene Sicherheitskonzepte zu entwickeln, die zumindest Maßnahmen gegen Verlust/Diebstahl und die Möglichkeit der lokalen Verschlüsselung von schutzwürdigen Daten beinhalten.
- Dem Gefährdungspotential durch Viren ist durch Einsatz geeigneter aufeinander abgestimmter lokaler (aktuelle Version eines der durch Landeslizenz erworbenen Antivirenprogramme) bzw. serverbasierender Programme Rechnung zu tragen. Herkömmliche On-Demand-Virenscanner und systemresidente Virenwächter sind in das Virenschutzkonzept einzubinden. Diensteintegrierte Internet-Virenscanner sollen die aus dem Netz empfangenen oder im Netz zur Verfügung gestellten Dateien automatisch auf Schadensfunktionen untersuchen, insbesondere auch um die Verbreitung von Makroviren zu verhindern.
- Superuser sind mit allgemein akzeptierten Sicherheitsanforderungen nicht vereinbar. Das Aufgabengesamt Systemadministrierung ist in Teilaufgaben aufzuteilen und zu Rollen gebündelt neu zusammengestellt ausführbar zu machen (Rekomposition der *root*-Rechte).
- Der Testbetrieb ist vom Produktionsbetrieb strikt zu trennen. Auf dem Produktionsrechner dürfen keine Entwicklungswerkzeuge verbleiben. Planmäßig durchgeführte (auch Crash- und Penetrations-) Tests können sicherheitsrelevante Probleme aufzeigen und zur Beseitigung von Schwachstellen beitragen.
- Den besonderen Risiken durch die zunehmende Zahl der Fernzugriffe (Tele- und Gruppenarbeit, Fernwartung) ist durch ein Remote-Access-Konzept Rechnung zu tragen, das Regelungen und Komponenten beschreibt.
- Die Modalitäten einer Fernwartung sollten in einem eigenen Vertrag geregelt werden.
- Eine mögliche Verletzung urheberrechtlicher Vorgaben, wettbewerbsrechtlicher Bestimmungen, des Rechts am eigenen Bild oder datenschutzrechtlicher Vorschriften durch Bereitstellung von Informationen auf Servern, auf die über Computernetze zugegriffen werden kann, werfen vielfältige Haftungsprobleme auf. Die ergriffenen organisatorischen Maßnahmen sind zu dokumentieren und dem jeweiligen Stand der Rechtsprechung anzupassen.
- Das Procedere für den Fall des Auftretens eines sicherheitsrelevanten Ereignisses ist im Sicherheitskonzept festzulegen; es soll Regeln für die Feststellung, die Informationswege und -politik, für die Beweissicherung bis hin zur Wiederherstellung der Systemintegrität beinhalten.

10.4 Literatur

/BaWü94/ Rechnungshof Baden-Württemberg:
„Untersuchung der Organisationsstrukturen der zentralen Verwaltungen der Universitäten in Baden Württemberg, Abschlussbericht“,
September 1994

/BayDs/ Bayerischer Landesbeauftragter für den Datenschutz:
„UNIX-Sicherheit“

/Behö96/ Zweiter Bericht über den Aufbau des Behördennetzes, 1996

/Beyer96/ Beyer, T.:
„Störungsmanager“,
iX 4/96 S. 164 ff

/Brunns95/ Brunnstein, K.:
„Noch fehlen Qualifikationsstandards“,
Business Computing 10/95

/BSI96/ Bundesamt für Sicherheit in der Informationstechnik:
„Maßnahmenempfehlungen für den mittleren Schutzbedarf“,
IT-Grundschutzhandbuch 1996

/BSTUKWK93/ Bayer. Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst:
„Datenverarbeitung in Lehre und Forschung“,
München, 1993
insbes. *6.7 „Organisatorische und personelle Maßnahmen“,* S. 124ff

/BSTUKWK97/ Bayer. Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst:
„Hochschulnetze in Bayern — Zugang, Nutzung, Schutz vor Missbrauch und damit zusammenhängende Rechtsfragen, Bericht der Arbeitsgruppe Zugangs- und Nutzungsregelungen für die bayerischen Hochschulnetze“
München, Februar 1997

/Bunge94/ Bunge, E.:
„Wie sicher sind IT-Systeme?“
Business Computing 1/94 S. 22 ff

/Burr95/ Burr, B.:
„Schulung für die Verwaltung“,
in: Deutsches Forschungsnetz – DFN –:
„Sichere Datenübertragung in offenen Netzen“
DFN-Bericht Nr. 79, August 1995

/CCI/ CCI (Competence Center Informatik GmbH), Meppen:
`http://www.cci.de`

/CE-Infosys/ Computer Elektronik Infosys, Bodenheim
`http://www.ce-infosys.com/german/index.htm`

/CW25-96/ *„Berufserfahrung steigert den Wert zertifizierter Profis“*,
Computerwoche 25/96

/DataFellows/ F-Secure Desktop
`http://www.datafellows.com/f-secure/desktop/`

/DEFCON/ DEFCON1 Notebook Security System
`http://www.portinc.com/NoFrames/defcon.htm`

/DFN96/ Deutsches Forschungsnetz – DFN –:
„Koexistenz von Verwaltung und Wissenschaft in hochschulweiten Backbone-Netzen unter besonderer Berücksichtigung des Datenschutzes und der Verfahrens- und Datensicherheit“,
DFN-Bericht Nr. 80, Januar 1996

/DFN97/ Deutsches Forschungsnetz – DFN –:
„Haftung des Vereins zur Förderung eines Deutschen Forschungsnetzes e.V. als Online-Diensteanbieter“,
DFN-Bericht Nr. 83, Juli 1997

/DG/ Data General:
„Trusted DG/UX“,
`http://www.dg.com/services/html/dg_ux_b2_security_option.html`

/EKKS/ EKKS Erlanger Klinikkommunikationssystem:
„Datenschutz im Klinikum der Universität Erlangen-Nürnberg“

/Ermer96/ Ermer, D.J.:
„Grundsätze für Benutzerrichtlinien für das Internet“,
KES 96/4 S. 37 ff und auch unter:
`http://www.bayern.de/DSB/O-Hilfen/IBenRiLi.htm`

/EWKR/ *„Encryption Without Key Recovery“,*
`http://www.data.com/roundups/encrypt.html`

/Felz96/ Felzmann, F.W.:
„Computer-Viren — eine ständige Gefahr“,
Vortrag im Rahmen eines BSI-Sicherheitsseminars an der Universität Ulm am 6.11.1996

/Fuhr96/ Fuhrberg, K. (BSI V2):
„Sicherheitsanforderungen an Internet-Firewalls“,
30.01.1996

/Gaiss96/ Gaissmaier, K.:
„Sicherheitsaspekte bei Dial-In Zugängen“,
in: Deutsches Forschungsnetz – DFN –:
„Sicherheit in vernetzten Systemen“
DFN-Bericht Nr. 81, April 1996

/Gerling95/ Gerling, R.W.:
„Internet: juristische Probleme und kein Ende“,
1995

/HaDs93/ Der Hamburgische Datenschutzbeauftragte:
`http://www.rewi.hu-berlin.de/Datenschutz/DSB/UNIXKonzeptHbg`
März 1993

/HaDs94/ Der Hamburgische Datenschutzbeauftragte:
„Datenschutz in Netzen“,
Hamburg, Oktober 1994

/HaDsTä/ Tätigkeitsbericht des Hamburgischen Dateschutzbeauftragten:
„21.7 Fernwartung der Patientenüberwachungsanlage im Universitäts-krankenhaus Eppendorf (UKE)“,
`http://www.rewi.hu-berlin.de/Datenschutz/DSB/HmbDSB/TB13/21_7.html`

/Hafner96/ Hafner, H.:
„Gegen Serverwahnsinn gewappnet“,
Gateway, Juli 1996, S.59 ff

/Hamm/ Hammerschmidt, Ch.:
„Welle offener Systeme nervt die DV-Leiter“,
`http://bda.web.aol.com/bda/nat/cz/archiv/192.html`

/Hoeren97/ Hoeren, Th.:
„Recht im Netz — Hinweise zur Haftung von Rechenzentren beim Umgang mit Telediensten“,
DFN Mitteilungen 44 — 6/97 S. 20ff

/Hübner96/ Hübner, M. / Kleff, N.:
„Zusammen stark — UNIX *plus zusätzliche Sicherheitstools“,*
KES 96/4 S. 28 ff

/IETF96/ Internet Engineering Task Force (IETF):
„Site Security Handbook“,
March 1996

/ITMin91/ *„Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (IT-Mindestanforderungen)“,*
Mai 1991

/Jacob93/ Jacob, R.:
„Wem gehört der Quellcode?“,
Business Computing, 1/93 S. 49 ff.

/Jatzlaug94/ Jatzlaug, P.:
„Remote Control beschleunigt den Service“,
Business Computing 4/94 S. 98 ff

/Kossa95/ Kossakowski, K.-P.:
„Sicherheitsberatung für DFN-Mitglieder und Reaktion im Schadensfall“,
in: Deutsches Forschungsnetz – DFN –:
„Sichere Datenübertragung in offenen Netzen“
DFN-Bericht Nr. 79, August 1995

/LANline96/ *„Netzmanagement über das Internet — Herstellerinitiative für gemeinsamen Standard“,*
LANline 10/96 S. 12

/LRZ/ *„Achtung Makroviren!“*
`http://www.lrz-muenchen.de/services/schriften/rundschreiben/`

/MaßFern/ *„Maßnahmen zur Sicherung einer Fernwartung“*
`http://www.schwaben.de/home/tichy/dsbfernw.html`

/Niemann95/ Niemann, F.:
„Verwaltung im Wandel“,
Gateway, Oktober 95 S. 32 ff

/Schröder95/ Schröder, K. / Hartmann, W.:
„Punkte sammeln ade“,
Gateway, September 1995

/Schröder95a/ Schröder, K. / Hartmann, W. :
„Netware Advanced Administration 4.1x“,
Gateway, November 1995

/SEMPER/ SEMPER:
„Secure Electronic Marketplace for Europe (ACTS Project AC026)
European Commission’s ACTS Programme
(Advanced Communications Technologies and Services)“

/SZ179-96/ *„Künftig alle drei Jahre neuer PC fällig“,*
Südd. Zeitung 1996/Nr. 179 S. 21

/Unixchk/ *„Unix-Sicherheitscheckliste“,*
`ftp://ftp.auscert.org.au/pub/auscert/papers/`
`unix_security_checklist`

/Utimaco/ Utimaco Safeware AG, Oberursel
`http://www.utimaco.com/utimacode.nsf?opendatabase`

/VDMA/ *„Sicherheit für die Informationsgesellschaft“*,
Schriftenreihe des Fachverbands Informationstechnik
im VDMA und ZVEI 66,
`http://www.bmwi-info2000.de/gip/studien/sicher/index.html`

/Wiso-ZDF/ `http://www.zdfmsn.de/ratgeber/wiso/index.asp`

/Wobst95/ Wobst:
„Diskette voller Geheimnisse, Erzeugung und Verwendung selbstentlandender, verschlüsselter Datenträger“,
UNIXopen 9/95 S. 54 ff

10.5 Anlage

Der Bayerische Landesbeauftragte für den Datenschutz
— Referat Technik und Organisation —

Benutzerrichtlinien

des/der _____ < Unternehmens/Behörde > _____

für die Nutzung des Internet

Vorwort

Für das Netz des/der __ < Unternehmens/Behörde > __ ist ein Internetzugang hergestellt worden. Als Mitarbeiter, der für die Nutzung der Dienste des Internet berechtigt ist, sind Sie über dieses von außen __(mittelbar bzw. unmittelbar)__ erreichbar. Desgleichen können Sie __unternehmens-/firmeneigene__ Informationen über das Internet an andere übermitteln bzw. im Internet bereitstellen.

Im Internet sind grundsätzlich keinerlei Maßnahmen zur Sicherstellung der Integrität, Vertraulichkeit und Authentizität der übertragenen Daten, der Kommunikation und der Kommunikationspartner an sich vorgesehen und realisiert. Die Auswahl und die Anwendung von geeigneten Datensicherheits- und Datenschutzmaßnahmen ist im Internet also jedem Teilnehmer selbst überlassen.

Die Auswahl der zu ergreifenden Sicherheitsmaßnahmen wurde durch die Leitung __des/der Unternehmens/Behörde__ getroffen; ebenso deren technische Realisierung. Diese Maßnahmen können aber nur zu einem gewissen Teil von sich aus ihre Wirksamkeit entfalten. Ein ganz entscheidender Faktor zur Gewährleistung und Verbesserung des vorhandenen Sicherheitsniveaus ist deren konsequente und gewissenhafte Anwendung in der täglichen Arbeit durch jeden Einzelnen.

Daher sind die Kenntnis dieser nachfolgenden Regelungen und deren Einhaltung durch jeden einzelnen berechtigten Mitarbeiter eine wesentliche Voraussetzung für die Sicherheit dieses neuen Kommunikationsmittels und __des/der Unternehmens/Behörde.

Jede Missachtung und Nichteinhaltung dieser Regelungen gefährdet nicht nur die Vertraulichkeit, Verfügbarkeit und Integrität der von Ihnen auf Ihrem eigenen DV-System unmittelbar be- und verarbeiteten Daten, sondern es wird dadurch auch die Vertraulichkeit, Verfügbarkeit und Integrität aller sonstigen __Unternehmens-/Behörden__-daten gefährdet. (Eventuell wird das gesamte Unternehmensziel gefährdet.)

Diese Benutzerrichtlinien stehen ergänzend zu den geltenden sonstigen Regelungen und Vorschriften bzgl. der Anwendung von Informationstechnik und für den Umgang mit personenbezogenen oder sonstigen schutzwürdigen Daten.

Regelungen

Verantwortung

- Sie sind als berechtigter Mitarbeiter in Ihrem Zuständigkeitsbereich verantwortlich für die vollständige und korrekte Anwendung der jeweils geltenden Regelungen, Anweisungen und Vorschriften zur Gewährleistung von Datenschutz und Datensicherheit (ggf. Verweis auf diese Dokumente).
- Sie sind als berechtigter Mitarbeiter insbesondere zuständig und verantwortlich für die in Ihrem Zuständigkeitsbereich liegende Anwendung der vorgesehenen und vorhandenen Zugangskontrolleinrichtungen und -maßnahmen (ggf. Aufzählung der getroffenen Maßnahmen wie z. B. Verschluss der Büroräume, gesicherte Aufbewahrung von externen Datenträgern wie Disketten, usw. oder Verweis auf entsprechende sonstige Regelungen und Vorschriften).
- Sie sind als berechtigter Mitarbeiter zuständig und verantwortlich für die wirksame Anwendung der vorgesehenen und vorhandenen Zugriffssicherungseinrichtungen und -maßnahmen (ggf. Aufzählung der getroffenen Maßnahmen wie z.B. Bootpasswort, Zugriffsschutz-Software, Passwortwahl, -aufbau und -verwahrung, mechanische Sperreinrichtungen, Ausweislesesysteme, usw. oder Verweis auf entsprechende sonstige Regelungen und Vorschriften) .

Nutzung des Internet

- Das Einbringen von privater Hard- und/oder Software in das lokale Netz ist unzulässig, weil dadurch Sicherheitslücken eröffnet werden können.
- Die Einrichtung und der Betrieb eines nicht bereitgestellten Anschlusses an ein öffentlich zugängliches Netz (mittels Datenübertragungseinrichtungen wie Modem, ISDN-Einbaukarten, usw.) ist nicht zulässig, weil dadurch weitere, unkontrollierbare und ungesicherte Übergänge in das lokale Netz geschaffen werden (evtl. Ausnahmegenehmigung regeln).
- Es ist lediglich die Nutzung derjenigen Dienste des Internet gestattet, die in Ihrem spezifischen Berechtigungsprofil ausdrücklich festgelegt sind. Die Nutzung aller nicht ausdrücklich erlaubten Dienste ist nicht gestattet.
- Weitere benötigte Dienste sind bei __(gem. interner Organisation)__ zu beantragen.
- Nicht mehr benötigte Dienste sind __(gem. interner Organisation)__ zur Änderung Ihres Berechtigungsprofils umgehend mitzuteilen.
- Die Nutzung der erlaubten Dienste ist ausschließlich zu __dienstlichen/geschäftlichen__ Zwecken und im ausdrücklich erlaubten Umfang zur Erledigung Ihrer Aufgaben gestattet. Die Nutzung der Dienste zu privaten Zwecken ist — auch aus Kostengründen — untersagt.
- Das Ausprobieren, ob weitere Dienste als die ausdrücklich erlaubten zur Verfügung stehen und evtl. genutzt werden können, ist unzulässig.
- Das Ausprobieren, das Ausforschen und die Benutzung fremder Zugriffsberechtigungen (ggf. Aufzählung wie z.B. Benutzerkennungen, Passworte, persönliche Identifika-

tionsausweise oder Verweis auf entsprechende sonstige Regelungen und Vorschriften) und sonstiger Authentifizierungshilfsmittel (ggf. Aufzählung wie z.B. Chipkarten, Magnetkarten, usw. oder Verweis auf entsprechende sonstige Regelungen und Vorschriften) ist unzulässig.

- Die Weitergabe und das Zurverfügungstellen von eigenen Benutzerkennungen und sonstigen Authentifizierungshilfsmitteln für eine Benutzung durch Dritte ist unzulässig. Es wird ausdrücklich darauf hingewiesen, dass in einem derartigen Fall aus den Protokolldaten Ihre Identität hervorgeht. Jegliche Aktivität — auch unzulässige — durch diesen Dritten wird also Ihnen zugeschrieben.
- Das Ausführen von Programmen oder von ausführbarem Programmcode, die aus dem oder über das Internet beschafft wurden, ist ohne vorherige Prüfung und Freigabe durch __unternehmens-/behördeneigenes Sicherheitsteam, CERT__ untersagt, um insbesondere das Risiko des Einschleppens von Computerviren im lokalen Netz zu reduzieren.

Verschlüsselung der Datenübertragung (Kryptographische Schutzmaßnahmen)

- Die Übertragung von sensiblen, schutzwürdigen und insbesondere von personenbezogenen Daten (z. B. mittels E-Mail) über das Internet ist, zur Wahrung der Vertraulichkeit, ausschließlich in verschlüsselter Form zulässig.
- Zu Ihrer Entlastung wird dies automatisch durch technische Einrichtungen sichergestellt. Oder Die Beurteilung, ob derartige Daten zur Übertragung vorliegen, erfolgt durch Sie als Absender selbst. Dabei ist ein strenger Maßstab anzulegen. Diese Daten sind mit __spezifisches Hilfsmittel wie Software__ durch Sie vor dem Versand zu verschlüsseln.
- Gleiches gilt für die Anwendung und Nutzung der digitalen Signatur.

Sicherheitsrelevante Ereignisse

- Alle sicherheitsrelevanten Ereignisse (ggf. Aufzählung wie z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzerkennung, usw.) sind sofort an __unternehmens-/behördeneigenes Sicherheitsteam, CERT__ zu melden. Dort wird der Angelegenheit nachgegangen.
- Unternehmen Sie keine eigenen Aufklärungsversuche, da evtl. wertvolle Hinweise und Spuren verwischt werden oder verloren gehen könnten.

Protokollierung und Kontrollen

- Jeder Datenverkehr innerhalb des lokalen Netzes und zwischen dem lokalen Netz und dem Internet __kann/wird__ einer automatischen __vollständigen/gezielten__ Protokollierung unterliegen.
- Die Protokolle werden für den Zeitraum von __wenigstens einem Jahr__ aufbewahrt und bei Verdacht auf einen Sicherheitsverstoß durch eigens hierfür Berechtigte (z.B. Datenschutzbeauftragter, Sicherheitsteam) ausgewertet.

- Die Protokolldaten dienen ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebes. Sie werden nicht für Zwecke der Leistungskontrolle verwendet.
- Die Einhaltung dieser Richtlinien kann durch __unternehmens-/behördeneigenes Sicherheitsteam, CERT__ stichprobenartig und anlassbezogen kontrolliert werden.

Sanktionen

Verstöße gegen diese Benutzerrichtlinien und die sonstigen Regelungen und Vorschriften bzgl. der Anwendung der Informationstechnik und bzgl. des Umgangs mit personenbezogenen Daten können dienst- und arbeitsrechtliche sowie strafrechtliche Konsequenzen haben. __Sie können auch Grund für eine fristlose Kündigung sein.__

Verpflichtung

Der Benutzer

- bestätigt die Kenntnisnahme der vorstehenden Regelungen,
- verpflichtet sich zu deren Einhaltung und
- bestätigt durch die nachfolgende Unterschrift den Erhalt eines Abdruckes.

Eine Ausfertigung erhält darüber hinaus der Datenschutzbeauftragte, eine weitere Ausfertigung wird zum Personalakt genommen.

. . . .
(Ort, Datum)

. . . .
(Verpflichtete/r) (Verpflichtender)

Kenntnisnahme durch den Datenschutzbeauftragten:

. . . .
(Ort, Datum) (Unterschrift)

Stand: 10.07.1996

Kapitel 11

Integrierter Lösungsansatz im Projekt BASILIKA

Die nachfolgende Zusammenstellung gibt einen kurzen Überblick über die Zielsetzungen im Rahmen des BASILIKA-Projekts (**BASILIKA**: „Bayerische Sicherheitslösung für Dienstangebote in offenen Kommunikationsnetzen“).

Das Projekt BASILIKA wird im Rahmen von BayernOnline II gefördert und hat als Querschnittsaufgabe für die bayerischen Behörden die Schaffung einer prototypischen Sicherheitsinfrastruktur zum Ziel, um einen gesicherten Zugang zu schützenswerten DV-Verfahren der Verwaltungen aus offenen Netzen heraus einer offenen Benutzergruppe (allen Bürgern) zu ermöglichen.

Beteiligt sind folgende Institutionen:

- Bayerisches Staatsministerium des Inneren als Projektführer,
- Landesamt für Statistik und Datenverarbeitung,
- Bayerisches Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst,
- Julius-Maximilians-Universität Würzburg als technischer Projektführer,
- Bayerisches Staatsministerium der Justiz,
- Siemens AG (Geschäftsbereich ANL) Erlangen,
- Bayerische Landesbank,
- und kooperierend das Bayerische Staatsministerium für Arbeit und Soziales.

11.1 Sicherheitsmaßnahmen in einem Unternehmen

Die Sicherheit eines Unternehmens muss auf mehreren Ebenen angestrebt und realisiert werden. Hierzu gehören:

1) Nutzungsvereinbarungen, Verpflichtungen der Mitarbeiter und Vorschriften, um den rechtlichen Rahmen bei Missbrauch oder Fahrlässigkeit in Ergänzung zu den allgemeinen Gesetzen klarzulegen.
2) Einüben von Verhaltensmaßregeln und Entwicklung eines Sicherheitsbewusstseins, d.h. die Mitarbeiter müssen dahingehend geschult werden, dass sie Abweichungen von den Regeln, Missbrauchsversuche, Nachlässigkeiten erkennen und aktiv monieren.
3) Technische Einrichtungen zur Zutrittskontrolle zu Räumlichkeiten und Maßnahmen innerhalb der Datenverarbeitung.
4) Organisatorische Maßnahmen in Ergänzung zu den technischen Einrichtungen, die beschreiben, wie die technischen Einrichtungen zu betreiben sind.

Im Rahmen des BASILIKA-Projekts werden die Ebenen 3 und 4 und z.T. auch 2 abzudecken versucht.

Auf technischer Ebene ist der gesamte Weg zwischen Benutzer und Applikation auf Sicherheitsmängel und Lösungsmöglichkeiten hin zu überprüfen. Hierzu gehören

- Sicherheitsaspekte beim Einsatz von Identifizierungsmedien (z.B. Chipkarten, Challenge-Response-Verfahren, Passwörter etc.),
- Eigenschaften des Arbeitsplatzes / Clients, mit dem der Endnutzer Zugang zu den Applikationen sucht, wie
  - die lokale Speicherung von Daten und
  - der Einsatz einer beglaubigten graphischen Benutzerschnittstelle (Graphical User Interface, GUI) ohne Nebeneffekte,
- die Gestaltung von Netzstrukturen, wie
  - Internet / Bürger- / Verwaltungsnetz,
  - Hochschulverwaltungsnetz / Behördennetz und
  - Servernetze,
- die Ausgestaltung der Übergänge zwischen separierten Netzbereichen, die unterschiedlichen Aufgaben dienen,
- die Kopplung gleicher Netzbereiche,
- die Administrierung der Sicherheitseinrichtungen, wie
  - die Homogenisierung und
  - der Aufwand für Sicherungsmaßnahmen,
- sowie die Akzeptanz von Selbstbedienungsfunktionen durch die potentiellen Nutzer.

11.2 Ziele einer Lösung für elektronische Geschäftsabwicklung

Das Ziel von BASILIKA ist nicht, vorhandene Sicherheitslücken oder Bedrohungsszenarien im Internet zu beseitigen. Vielmehr geht es darum, trotz dieser Lücken eine möglichst modulare Lösung zu suchen, wie zwei Partner, der Nutzer und eine DV-Anwendung, sich gegenseitig vertrauen können. Damit ist ein enger Zusammenhang mit dem 1997 verabschiedeten Signaturgesetz gegeben. Dieses deckt aber keineswegs alle Aspekte ab, die für vertrauenswürdige geschäftliche Beziehungen erforderlich sind.

11.2.1 Zweiseitiges Vertrauen zwischen Nutzer und DV-Anwendung

Folgende Funktionen sollen mit BASILIKA erfüllt werden:

- Integrität der Datenübermittlung,
- Ermöglichung von (rechts-)verbindlichen elektronischen Vorgängen,
- Vertraulichkeit bei der Datenübermittlung (confidentiality, user privacy),
- zweiseitige Authentifizierung der Partner (authentication),
- Nichtanfechtbarkeit einer Transaktion (non-repudiation),
- Zugangsregelung zu Teilen einer Anwendung; zentrale Zugangskontrolle über alle Applikationen eines Unternehmens (zentraler Berechtigungsserver und Single-Signon),
- Kontrolle des eingesetzten Authentifizierungsmediums gegen Missbrauch, Verlust (black list, revocation lists) und Vergesslichkeit,
- Zeitkontrolle bestehender Client/Server-Verbindungen auf Inaktivität, insbesondere bei multifunktionaler Nutzung von Endgeräten (Timeout-Überwachung),
- Verfügbarkeit von Zusatzdiensten wie z.B.
  - Abwicklung von Zahlungsverkehr über das Internet,
  - Erstellung signierter Dokumente,
- zentrale Auslieferung von zertifizierter und beglaubigter Software (trusted Software),
- Verwaltung und Distribution der geheimen und öffentlichen Schlüssel für Signaturen und Verschlüsselung (*Key Management*).

Dabei reicht es z.B. nicht, nur zwischen Client auf der einen Seite und Betriebssystem, auf dem die Applikation läuft, andererseits Vertrauenswürdigkeit herzustellen.

Ein weiterer wichtiger Aspekt der Vertrauenswürdigkeit ist, dass die eingesetzten Sicherheitstechniken von unabhängiger Stelle, wenn schon nicht zertifiziert, so doch mindestens validiert sind.

11.2.2 Sicherung gegen Wirtschaftsspionage

Wie allseits bekannt, ist die Frage gesicherter und vertraulicher Kommunikation im Internet ein durchaus politisches Thema. Dabei geht es auch um Vertraulichkeit bzw. die Möglichkeit der Einsichtnahme in den internationalen Nachrichtenverkehr durch nationale Institutionen.

Aufgrund der einseitigen Marktlage auf dem Gebiet der Hardware und Software haben die Lieferanten von Kommunikationseinrichtungen die Möglichkeit, sich Vorteile zu verschaffen und die Vertraulichkeit des Nachrichtenaustausches ohne Wissen der betroffenen Nutzer von Soft- und Hardware durch verdeckte Nachrichtenkanäle zu korrumpieren. Deshalb müssen einige kritische Teile eines Sicherheitskonzepts diese Tatsache berücksichtigen. Hinter und vor dem sog. Provider-Gateway (PG; siehe unten) kann marktgängige Soft- und Hardware genutzt werden.

Nutzer und Diensteanbieter setzen marktgängige Produkte in Clients, Servern, Netzkomponenten etc. ein, über deren Vertrauenswürdigkeit keiner der Beteiligten sich sicher sein kann. Es müssen also Techniken angestrebt werden, die auch bei manipulierter Standardsoftware ein gewisses Maß an Sicherheit bieten. D.h. die auf dem Client eingesetzte Software muss aus „trusted GUIs“ bestehen, die von einem unabhängigen TrustCenter abgeholt werden kann oder die vom Provider-Gateway mit Software-Signatur in den Client geladen wurde. Umgekehrt ist es genauso wichtig, dass der Nutzer nur mit sicherer Software auf der Anwendungsseite zu tun hat. D.h. pro Sitzung wird ein virtueller privater Kanal aufgebaut, der sich bezüglich des Nachrichteninhalts nicht auf Standardsoftware verlässt. Nur die beiden Partner Clientsoftware, geladen von einem vertrauenswürdigen (dritten) Partner und verifizierbar durch den Nutzer, und das Provider-Gateway bilden einen privaten virtuellen Kanal, der auf keine Funktionen auf Netz- und Betriebssystemebenen angewiesen ist.

Kein Diensteanbieter und kein Nutzer kann es sich leisten, nur zertifizierte Software einzusetzen, sofern er sie überhaupt erhält. Deshalb ist der öffentliche (kostenlose) Zugang zu TrustCentern als Verteiler geprüfter Software für Client und Sicherheitseinrichtungen auf der Seite der DV-Anwendungen ein sehr wichtiger Faktor für die Nutzerakzeptanz.

Die Sicherheit kann nicht in bestehende Applikationen eingebaut werden. Das würde einen prohibitiven Aufwand verursachen. Deshalb muss eine Lösung gesucht werden, die den Applikationen vorgelagert die nötige Sicherheit gegen manipulierte Software bereitstellt.

11.2.3 Sicherung gegen Sabotage

Jede Lösung muss auch Vorkehrungen treffen, dass keine Sabotage durch Einschleusen von Viren oder ähnlicher Sabotagewerkzeuge beim Client, temporär während einer Sitzung, und in der Sicherheitsschicht auf der Seite der Anwendungen möglich ist. Das Provider-Gateway hat die Aufgabe, nach Entschlüsselung des Nachrichtenverkehrs vor Weiterleitung einer Nachricht an die Applikation einen diesbezüglichen Check durchzuführen.

11.3 Grundsätze einer Lösung

Es wird eine Lösung gesucht, die sich auf wenige aber umfassende Grundsätze aufbauen lässt:

Breite der Lösung und umfassende Sicherheitskonzeption

- Die Lösung ist primär für offene Benutzergruppen gedacht.
- Die Lösung wird auch gleichermaßen zum Schutz gegen Innentäter geplant.

Trennung der Sicherheitstechniken von allen Aspekten der Netze, Endgeräte, Betriebssysteme und Applikationen

- Die Sicherheit wird von der Applikation völlig entkoppelt, da Betriebssystem und Applikation einem ständigen Wechsel unterliegen und von einer anderen Mannschaft betreut werden (sollten) als derjenigen, die für Sicherheit zuständig ist.
- Es werden keine speziellen Anforderungen an die Clients oder an die Netzkonfiguration gestellt, die die Nutzer einsetzen wollen/sollen, mit Ausnahme einer Leseeinrichtung am Client für ein Identifikationsmedium (z.B. Chipkarte), wenn eine bestimmte Sicherheitsstufe erreicht werden soll.

  Es wird nicht auf die Verfügbarkeit von Sicherheitsdienstleistungen eines Netzbetreibers abgehoben, weil diese potentiell unsicher, weder durch den Nutzer noch den Betreiber der Applikation überwachbar sind und durch politische Vorgaben manipuliert sein könnten.
- Es wird eine Ende-zu-Ende-Sicherheit, Nutzer–Applikation und nicht nur Endgerät–Betriebssystem oder dergleichen, angestrebt.
- Dabei kann der Eintritt in den gesicherten Bereich der Applikationen in einer Domäne erfolgen, zu der die angewählte Applikation nicht gehört. Die Kopplung zwischen gesicherten Domänen erfolgt über Krypto-Routerverbindungen.
- Damit wird die beidseitige Authentifizierung zwischen Nutzer und Applikation in eine Sicherheitsschicht vor der Applikation ausgelagert. Zwischen diesen beiden findet das Nachrichtenspiel im Sinne eines privaten virtuellen Kanals (privat: im Sinne des einzelnen Nutzers) statt, unter der Nebenbedingung, dass beide Partner nur sich selbst und gegenseitig vertrauen, aber keinem Dritten, außer einem TrustCenter. Die Sicherheit verlässt sich nicht auf Techniken der Transportebene, die von niemandem kontrollierbar sind. Der private virtuelle Kanal ist nutzerspezifisch und sitzungsspezifisch.

Zentralisierung der Sicherheitsfunktionen

- Zentralisierung soll hier nicht im Sinne einer physischen sondern einer logischen und konzeptionellen verstanden werden.

- Alle sicherheitsrelevanten Funktionen werden logisch so konzentriert, dass sie gleichmäßig über das ganze Unternehmen zugänglich und auch gewährleistet werden.
- Der private virtuelle Kanal wird zeitüberwacht und vom Provider-Gateway automatisch geschlossen, wenn er über eine einstellbar lange Zeit inaktiv sein sollte.
- Das zentrale Provider-Gateway verwaltet neben dem privaten virtuellen Kanal zum Nutzer die zentralisierte Berechtigungsverwaltung (Zugangsberechtigung im Sinne eines Single-Signon) und das Auditing des Nachrichtenverkehrs.
- Die Zentralisierung ermöglicht es, den Aufwand für Zertifizierung in Grenzen zu halten.
- Die Administrierung wird an einer Stelle konzentriert, so dass unternehmensweit die gleichen Regeln sicher zum Einsatz kommen, das Adminstrationspersonal optimal ausgebildet und erfahren sein kann.
- Auditing erfolgt an genau einer Stelle, was auch die Gefahr des Missbrauchs von Audit-Daten reduzieren hilft.
- Die Wartung wird unabhängig von den Wartungsintervallen der Betriebssysteme und Applikationen.
- Externes Wartungspersonal für die Sicherheitseinrichtungen hat auch versehentlich keine Zugriffe auf Nutzerdaten, da die Sicherheitsrechner keinerlei Nutzerdaten tragen.
- Sicherheitseinrichtungen können als Black Box von autorisierten Institutionen bezogen werden.
- Zentrale Dienste werden realisiert, die von allen Applikationen und Nutzern grundsätzlich und unternehmensweit gleichwertig und einheitlich angesprochen werden können:
  - zweiseitige Authentifizierung,
  - privater virtueller Kanal,
  - Auditing,
  - Berechtigungsverwaltung mit Sperrverwaltung,
  - Homogenisierung der Berechtigungsverwaltung und der Nutzeroberflächen über eine heterogene Applikationslandschaft hinweg,
  - elektronische Zahlungsfunktionen,
  - Signatur und Zeitstempeldienste (Notariatsdienste).

Skalierbarkeit, Modularität und Sicherheitsstufen

- Die Sicherheitslösung muss in sich modular gestaltet werden und in Bezug auf Durchsatz und Ausfallsicherheit skalierbar sein (Clusterlösung).
- Eine Sicherheitslösung muss sich nach den wachsenden Bedürfnissen eines Unternehmens inkrementell aufbauen lassen. Sicherheitslösungen, die nur extreme Lösungen (alles oder nichts) zulassen, werden nicht verwendet.

- Modularität erhöht die Sicherheit und die Wartbarkeit.
- Modularität erlaubt eine Verteilung der Verantwortlichkeiten bei der Administrierung.
- Modularität ermöglicht eine inkrementelle Zertifizierung.

Beglaubigung durch eine dritte Instanz

- Nutzerakzeptanz wird auf breiter Basis nur erreicht, wenn zweiseitiges Vertrauen zwischen Nutzer und Applikation besteht. Dazu bedarf es des Einsatzes vertrauenswürdiger Software auf Seiten des Clients wie auch der Applikationen. Dies muss durch die zwischengeschaltete (und zertifizierte) Sicherheitsschicht gewährleistet werden. Eventuell ist es sinnvoll, eine Beglaubigungsinstanz einzuschalten, die als Lieferant für vertrauenswürdige Software fungiert. Das vermindert den Aufwand und sichert Nachhaltigkeit.

Minimierung des Administrierungssaufwands

- Der größte Schwachpunkt einer Sicherheitslösung besteht in ungepflegten Datenbeständen und in weitreichenden Berechtigungen von Administratoren sowie in unzureichendem Personal, das zu wenig geschult oder überlastet ist.
- Die Sicherheitslösung muss weitestgehend automatisiert werden.
- Sie muss sich selbst überwachen und alle Abläufe dokumentieren (Auditing).
- Die technischen Sicherheitseinrichtungen sollten von externen, zertifizierten Spezialisten installiert und gewartet werden.

Aus diesen Grundsätzen ist nachfolgend die in Abschnitt 11.4 dargestellte Modularisierung und Funktionsaufteilung abgeleitet worden. Dabei wurde natürlich berücksichtigt, welche Marktentwicklungen sich abzuzeichnen beginnen. Ein wesentlicher Grundsatz für erfolgreiche Sicherheitsmaßnahmen ist, dass sie bezahlbar bleiben müssen. Deshalb müssen die Lösungen so konstruiert werden, dass weitestgehend auf dem Markt verfügbare (zertifizierte) Komponenten zum Einsatz kommen. Diese sind aber so zu kombinieren und nur an wenigen kritischen Punkten durch Sonderentwicklungen zu ergänzen, dass die gesetzten Ziele erreicht werden können.

11.4 Lösungsstrukturen

11.4.1 Technische Lösungen

Nachfolgend werden folgende Kürzel verwendet:

AA	Application-Adapter
AU	Auditserver
BS	Berechtigungsserver
BVS	Berechtigungsverwaltungsserver
ESTS	Electronic Signature and Timestamp Server
FW	Firewall
PG	Provider-Gateway
PS	Payment-Server
PVC	Private-Virtual-Channel
SC	Signatur-Client
SSO	Single-Signon
TC	TrustCenter

Netzstrukturen

Spezielle Netzstrukturen (virtuelle Netze) oder Netzprotokolle werden zur Lösung nicht herangezogen.

Falls Innentäter ein Problem sein können, müssen die Endgeräte, zu denen mögliche Innentäter Zugang haben, aus dem gesicherten Netz herausgenommen werden und die Netze der Endgeräte wie jene aus dem externen Netz über das Provider-Gateway (PG) geführt werden.

Es wird also eine dreistufige Netzkonfiguration vorgesehen:
Internet, Intranet, Servernetz mit den Applikationsservern. Der Übergang Internet–Intranet wird durch eine handelsübliche Firewall ermöglicht. Der Übergang Internet–Servernetz bzw. Intranet–Servernetz wird (zusätzlich) durch ein Provider-Gateway abgesichert.

Kopplung sicherer Netzinseln über offene Netze

In jeder Netzinsel kann davon ausgegangen werden, dass alle erforderlichen Sicherheitsmaßnahmen, insbesondere auch gegen Innentäter, ergriffen sind. Dort gibt es eine strenge Benutzerverwaltung und einen Zugriffsschutz, der in den Applikationen integriert ist. Die Applikationen werden nur von einer geschlossenen Benutzergruppe verwendet, die nur Zugriff innerhalb der Netzinsel auf die Applikationen hat, d.h. alle Netzinseln sind von gleicher Sicherheitskategorie.

Der Markt hält hierfür diverse fertige Lösungen in Form von generalisierten Krypto-Routern mit zentralisierter Schlüsselverwaltung parat oder Lösungen, die in Applikationen oder auf Transportebene oder in Filetransferlösungen etc. eingebaut sind.

Dieses Thema ist nicht Gegenstand der BASILIKA-Entwicklung wohl aber des BASILIKA-Prototypeinsatzes.

Sicherheitskomponenten

Bei der Analyse der Anforderungen an die BASILIKA-Lösung haben sich folgende Komponenten mit abgrenzbarer Funktionalität ergeben. Diese sollen nachfolgend kurz skizziert werden. Die Komponenten können physisch eigenständige Module sein oder Softwarepakete. Dies bleibt als ein Skalierungsmerkmal offen. Es wird zu untersuchen sein, ob zwischen den Modulen ein eigenständiger Authentifizierungsvorgang erforderlich sein wird, um einen hohen Sicherheitslevel zu erreichen, weil man dadurch erschweren kann, dass ein Eindringling in einer Komponente sich in andere Sicherheitskomponenten ausbreiten kann (z.B. vom Provider-Gateway (PG) in den Berechtigungsserver (BS) etc.).

Firewall und Krypto-Router

Zur Absicherung gegen Eindringen aus dem Internet in ein Intranet haben sich die aus Packet-Screen und Application-Gateway bestehenden Firewall-Lösungen (siehe Kapitel 5) etabliert. Damit kann gewisser Internet-Verkehr gefiltert werden. Dies sind marktgängige Funktionen.

Moderne Firewall-Lösungen bieten auch zusätzlich die Möglichkeit, einen privaten virtuellen Kanal (PVC) zum Nutzer mit wählbaren Kryptographieverfahren, optional gesteuert über Chipkarten, aufzubauen.

Ferner werden Krypto-Router-Funktionen zur Kopplung gesicherter Netzinseln kombiniert mit einer Firewall angeboten.

Auditfunktionen sind üblicherweise verfügbar.

Darüber hinaus ist in der Regel ein generischer Proxy verfügbar, auf dem weitere anwendungsspezifische Funktionen erstellt werden können.

Auf solchen Lösungen kann das BASILIKA-Projekt aufsetzen.

Provider-Gateway (PG)

Das Provider-Gateway (PG) ist das zentrale Sicherheitsmodul des BASILIKA-Projekts. Das PG übernimmt folgende Funktionen, sofern diese nicht schon von einer vorgelagerten Firewall übernommen wurden:

- Paketfilterung,
- Applikationsfilterung für Internet-Applikationen (Ports etc.),
- Authentifizierung des Nutzers mit Chipkarten oder Passwortmechanismen,
- Nachweis der eigenen Authentizität gegenüber dem Nutzer,
- Laden von trusted Software in den Client (mit sitzungsspezifischer Signatur des Codes), eventuell über eine dritte Instanz (siehe TrustCenter (TC)),

- Aufbau und Aufrechterhaltung eines privaten, nutzerspezifischen und sitzungsspezifischen, virtuellen Kanals (PVC),
- Sitzungsüberwachung mit Timeout,
- Berechtigungsprüfungen und Zuordnung eines Nutzers zu vordefinierten Nutzerprofilen der Applikationen (Single-Signon-Funktionalität (SSO);
  siehe auch Berechtigungsverwaltungssystem (BVS) und Berechtigungsserver (BS)),
- Homogenisierung der Benutzeroberfläche (über den Application-Adapter (AA)),
- Auslösung von Internet-Zahlungsfunktionen (siehe Payment-Server (PS)),
- Mitführung eines Protokolls des Nachrichtenverkehrs und (verschlüsselte) Speicherung auf dem Auditserver (AU).

Das PG nutzt zur Aufgabenerfüllung eine Reihe von separierten Hilfsserverfunktionen (TC, BS, BVS, AU, AA, SC, PS), die nachfolgend skizziert werden.

Alle Hilfsserver sind im gesicherten Netz anzusiedeln und stellen z.T. wie im Falle des Berechtigungsverwaltungsservers (BVS), eine eigene Applikation dar, die der Nutzer in Selbstbedienung ansprechen kann.

Das Provider-Gateway (PG) ist der zentrale Sicherheitspunkt. In ihm werden alle Sicherheitsfunktionen konzentriert. Er bedarf der Zertifizierung, wenn eine gewisse Sicherheitsstufe erreicht werden soll. Welche Anforderungen an das Betriebssystem und die Applikationssoftware auf dem PG zu erfüllen sein werden, ist Gegenstand der Validierung des BASILIKA-Konzepts.

Das grobe Zusammenspiel der Komponenten wird in nachfolgendem Diagramm skizziert. Dabei ist bei einer Installation zu beachten, dass alle Hilfsfunktionen des PG im gesicherten Servernetz angesiedelt werden müssen. Sie dürfen auch nicht im Intranet installiert werden.

Es handelt sich hier um höchst schützenswerte Applikationen, die mindestens die gleiche Schutzstufe wie Verwaltungsapplikationen haben müssen.

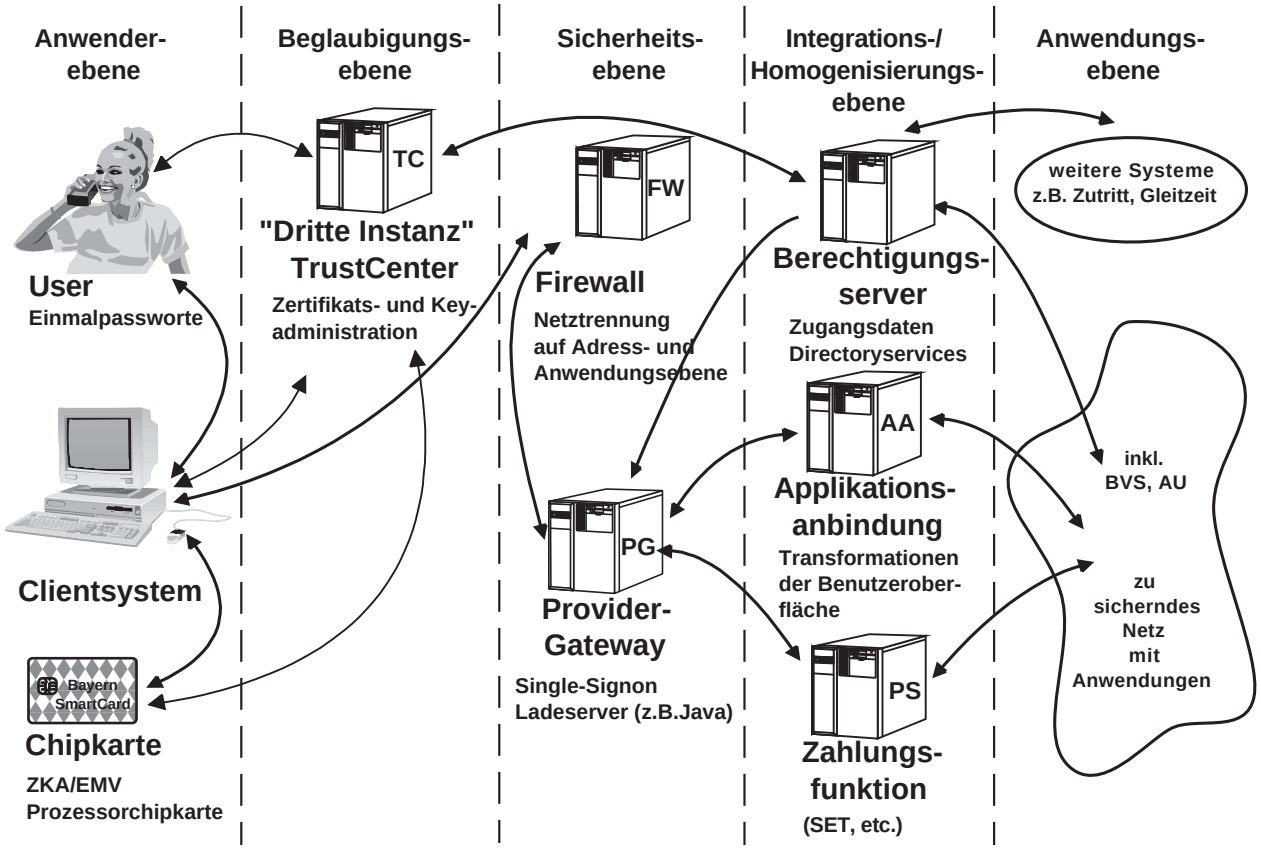


Abbildung 11.1: Berechtigungs- und Berechtigungsverwaltungsserver (BS und BVS)

Bei einer offenen Benutzergruppe mit theoretisch unbegrenzter Nutzerzahl, wie sie für BASILIKA im Vordergrund der Betrachtung steht, kann die Benutzerverwaltung nicht mehr nutzerspezifisch in den einzelnen Applikationen durchgeführt werden.

Die Nutzerprofile, d.h. die Zugriffsrechte zu Datenobjekten für bestimmte Nutzergruppen, werden nach wie vor auf der Applikations- oder auf Betriebssystemebene zu pflegen und zu definieren sein.

Die Zuordnung eines individuellen Nutzers zu einer Nutzergruppe im Sinne der jeweiligen Applikation jedoch muss an einer Stelle zentralisiert werden. Dies ist ein Gebot der Reduktion des Verwaltungsaufwands und der Erhöhung der Sicherheit gleichermaßen (siehe administrative Maßnahmen).

Zentralisierte Berechtigungsverwaltung ist auch für andere Berechtigungsobjekte wie Zutritt zu Räumen, Laboren, Rechner-Einrichtungen etc. erforderlich, je mehr Personen direkten Zutritt zu schützenswerten Objekten erhalten sollen, bzw. die Zahl der schützenswerten und schützensnotwendigen Einrichtungen (Genlabore etc.) zunimmt.

Bei einer hohen Zahl potentiell Berechtigter muss die Berechtigungsverwaltung teilautomatisiert und in Selbstbedienung durch den Nutzer überführt werden.

Unter Selbstbedienung und Automation ist hier zu verstehen:

- Berechtigungswunschanmeldung durch den „Kunden“,
- Freigabe der Berechtigung durch einen Spezialisten der verwaltenden Organisationseinheit (z.B. einer Fakultät in einer Hochschule) auf elektronischem Wege,
- Mitteilung der (Nicht-)Durchführung an den Antragsteller per E-Mail,
- automatische Übermittlung des neuen Berechtigungsprofils an das betroffene System (Rechnersystem, DV-Anwendung, Zutrittskontrollsystem, externer Datenbankanbieter etc.),
- automatische Steuerung des Single-Signon im Provider-Gateway (PG),
- Ausgabe von Berechtigungslisten und -profilen,
- automatische Bereinigung bei Exmatrikel bzw. Ende eines Arbeitsverhältnisses.

Während der sog. Berechtigungsverwaltungsserver (BVS) die vorstehenden Selbstbedienungsfunktionen übernimmt und in diesem Sinn eine schützenswerte Applikation mit Selbstbedienung durch den Kunden und den Berechtigungsbearbeiter darstellt, ist der Berechtigungsserver (BS) eine Art Directory-Server, der die Berechtigungsobjekte und deren zeitlich befristete Zuordnung (Sperrlistenverwaltung) zu einem individuellen Nutzer zentral speichert und damit online das Provider-Gateway (PG) bedient oder online oder offline die Benutzerverwaltung nachgelagerter Betriebssysteme oder Applikationen direkt oder die Berechtigungsdaten an einen externen Berechtigungsserver (im Slave-Modus) abgibt und damit Betriebssysteme und Applikationen steuert (siehe die aktuellen Entwicklungen von Directory Servern von Novell und Microsoft).

Auditserver (AU)

Eine wichtige Sicherheitsfunktion des Application-Gateways ist die lückenlose **Protokollierung** sämtlicher Vorgänge. Dabei muss beachtet werden, dass der Zugriff auf diese Komponente nur berechtigten Personen gestattet werden darf. Unter Umständen sollten die Audit-Informationen verschlüsselt abgelegt werden, so dass sie nur von dem Besitzer des Schlüssels ausgewertet werden können.

Application-Adapter (AA)

Der Application-Adapter ist das Modul, das die Umsetzung anwendungsspezifischer Oberflächen auf eine Standard-GUI (z.B. HTML, JAVA) vornimmt, um im Rahmen von Single-Signon den sporadischen Nutzer mit vertrauter Oberfläche zu versorgen, auf dem Client nur Standard-Software voraussetzen zu müssen (weltweite Wartbarkeit) und die Nutzerakzeptanz zu erhöhen.

Beglaubigungsinstanz

Es wurde oben ausgeführt, dass es in zweifacher Hinsicht unabhängige Beglaubigungsinstanzen geben muss/sollte.

Das TrustCenter (TC) erfüllt folgende Funktionen:

- Schlüsselverwaltung für asymmetrische Kryptoverfahren,
- physische Ausstellung von Chipkarten, einschließlich der RSA-Schlüssel,
- gegebenenfalls Onlinebeglaubigung von public keys.
- Daneben ist beglaubigte Software für Client und Provider-Gateway (PG) vorzuhalten, die über das offene Netz sicher zugeladen werden kann.
- Diese Instanz ist eventuell auch zuständig, dem Nutzer an einem Client nicht nur vertrauenswürdige Software für seinen Client (temporär) zu liefern, sondern auch als Dritter dem Nutzer die Authentizität des Partners zu bestätigen sowie zu beglaubigen, dass das Provider-Gateway (PG) vertrauenswürdige Software geladen hat.
- Diese Instanz ist eventuell auch zuständig, zertifizierte und vorinstallierte Sicherheitskomponenten (PG, BS, etc.) an einen Provider auszuliefern und dies gegenüber dem Nutzer am Client auf Wunsch zu bestätigen.

Die Beglaubigungsinstanz könnte auch die zentrale Dienstleistung eines elektronischen Signier- und Zeitstempeldienstes (ESTS) anbieten, der über das offene Netz angesprochen werden kann, und damit dedizierte Signatur-Clients (SC) überflüssig machen.

Es ist nicht davon auszugehen, dass der Normalbürger seinen PC mit einer zwangsläufig teuren Signatur-Clientsoftware oder -hardware ausstatten wird, um rechtsverbindlich mit Behörden kommunizieren zu können. Die Nutzerakzeptanz durch den Bürger wird sehr gering bleiben, wenn nicht durch Angebote einer solchen Dienstleistung im Netz sichergestellt wird, dass der sporadische Nutzer mit nur geringen Kosten belastet wird.

In allen genannten Fällen handelt es sich um Notariatsfunktionen. Diese Funktionen stellen besonders schützenswerte Applikationen dar und müssen deshalb einer vertrauenswürdigen Certification Authority (CA) als Aufgabe zugewiesen werden, falls eine gewisse Stufe der Sicherheit und des gegenseitigen Vertrauens erreicht werden soll/muss.

Welche Instanzen solche Dienste anbieten werden, ob dies privatwirtschaftlich oder behördlich geschieht, ist eine gesonderte Frage, die sich im Zusammenhang mit dem Signaturgesetz herausstellen wird. Die BASILIKA-Lösung muss zu dieser Entwicklung kompatibel bleiben.

Signatur-Client (SC)

Für hohe Sicherheitsanforderungen, insbesondere für rechtsverbindliche Geschäftsvorgänge im Sinne des Signaturgesetzes, wird es erforderlich sein, besondere Maßnahmen zu ergreifen, die nur mit Hardwareeinrichtungen auf Client/Nutzerseite zu erfüllen sein werden. Wie vorstehend bereits ausgeführt, wird diese Hochsicherheitslösung in der Regel nur geschlossenen Benutzergruppen, die Wirtschaftsinteressen haben, vorbehalten bleiben.

Das BASILIKA-Projekt wird so gestaltet werden, dass diese Bedingungen durch Zusatzeinrichtungen auf dem Provider-Gateway (PG) oder/und Clientseite erfüllt werden können. Sie werden aber nicht obligatorisch sein, um eine Skalierung der Sicherheitsstufen und der Kosten zu ermöglichen.

Payment-Server (PS)

Für die Abwicklung kostenpflichtiger, elektronischer Geschäftsvorgänge ist eine Zahlungsfunktion zu integrieren. Hier gibt es internationale Marktentwicklung unter dem Kürzel SET (Visa, MasterCard, Microsoft, IBM) und deutsche Entwicklungen im Zusammenhang mit der ZKA-Geldkarte (Firmen IKOSS, Gieseke & Devrient, Brokat).

Der Payment-Server wird von der zahlungsanfordernden Applikation angesprochen und nimmt die Zahlung im Zusammenspiel mit dem PG vor.

11.4.2 Administrierung

Es ist besonders wichtig, den manuellen Aufwand zur Verwaltung der vorstehend skizzierten Sicherheitsstrukturen und der schützenswerten Applikationen weitestgehend durch Verwendung von Automatismen zu reduzieren, da die Gefahr von Nachlässigkeiten beim Administrierungsspersonal, das in der Regel vor Ort in ausreichender Menge und Qualität nicht verfügbar sein wird, groß ist und die Auswirkungen von Fahrlässigkeiten enorm sind.

Die Systeme, die IT-Sicherheit gewährleisten, müssen so konzipiert sein, dass sie sich auch in Störungsfällen automatisch rekonfigurieren können, denn diese Einrichtungen müssen in einem 24-Stunden-Betrieb verfügbar gehalten werden, was manuelle Eingriffe in Störungsfällen verhindern würde, und jeder manuelle Eingriff zum Restart eines Systems kann ein sicherheitsrelevanter Eingriff sein.

Die Module AA, BVS, BS, PS etc. sind unter dem Aspekt der Sicherheit schützenswerte Applikationen und unterscheiden sich hinsichtlich der Administrierung nicht von anderen Applikationen im geschützten Netzbereich. Die schlechte Wartung der genannten Module kann das Gesamtsystem stilllegen oder fehlerhafte Funktionen bewirken, sie dienen aber nicht primär der Abwehr von Eindringlingen.

Die Module FW und PG allerdings sind die eigentlichen sicherheitskritischen Komponenten, die gegebenenfalls einer Zertifizierung unterliegen müssen.

Alle nachfolgenden administrativen Maßnahmen dienen der Sicherheit, sind aber auch Maßnahmen zur Reduktion des Personalbedarfs und damit zur Handhabbarkeit des Systems.

Konzept der Administrierung von technischen Sicherheitseinrichtungen

FW, PG und BS sollten so konzipiert sein, dass neue Versionen von einer unabhängigen Entwicklungsmannschaft getestet und installiert werden und die Übernahme auf die Produktionsrechner von gänzlich anderem Personal wahrgenommen wird. Die Betreiber vor

Ort sollten nur gezielte Stammdatenpflege durchführen können. Für den BS sollte dies nur über den BVS möglich sein.

Alle sicherheitsrelevanten Systeme enthalten eine Export- und Importschnittstelle, die dem Betreiber zugänglich ist. Damit kann er vor einem Versionswechsel den Datenbestand exportieren (verschlüsselt; dem Betreiber ist der Schlüssel nicht bekannt, sondern nur dem TrustCenter) und nach dem Versionswechsel die Daten wieder importieren.

Für den Auditingteil des PG wird eine ähnliche Struktur vorgeschlagen. Die Daten werden lokal verschlüsselt gespeichert. Dies ist eine Standardfunktion des vorkonfektionierten PG. Der Schlüssel wird vom TrustCenter verwaltet. Dazu gibt es die Standardauswertungslisten des AU für die Routineüberwachung, die keine Personenprofile zu erzeugen gestatten. Für Sonderauswertungen bei Missbrauchsverdacht, die über die Standardlisten hinausgehen, stellt das TrustCenter auf einer Chipkarte eine Zugangsmöglichkeit zur Datenbank des AU zur Verfügung, damit mit Datenbankkommandos und unter Beachtung des Vier-Augen-Prinzips Auswertungen vor Ort gefahren werden können.

Weitgehende Automatisierung der Pflege des zentralen Berechtigungsservers

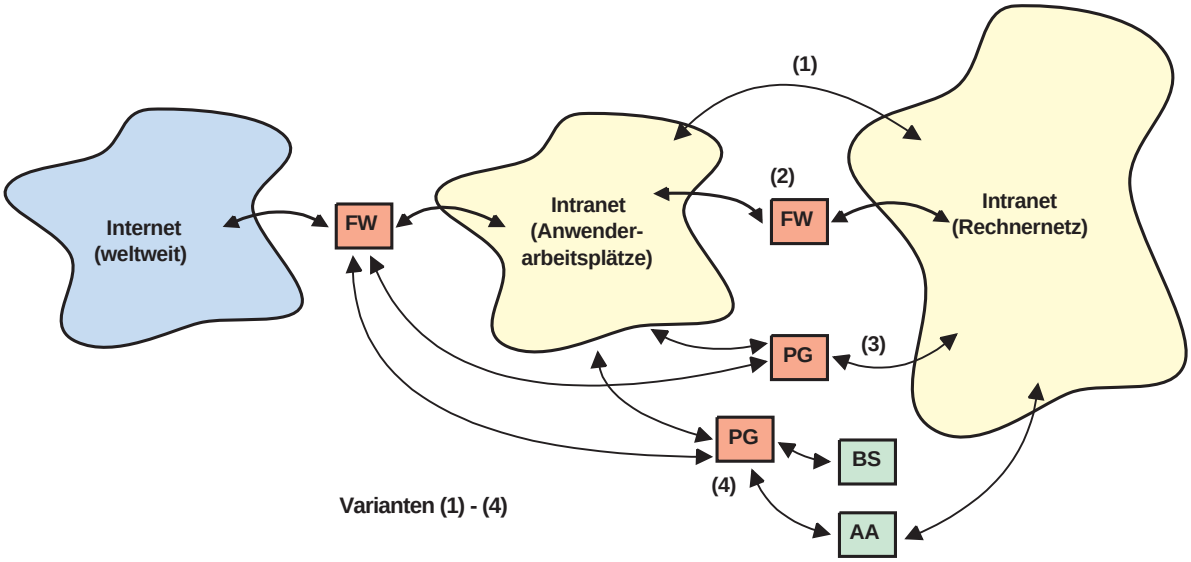
Insbesondere die Pflege der Berechtigungsobjekte im Rahmen der Homogenisierung der Anwendungslandschaft darf nicht einer manuellen Organisation unterworfen werden. Denn damit wird die Gefahr eröffnet, dass wegen Personalengpass entweder die „Kunden“ unzufrieden oder/und die Administratoren nervös und nachlässig werden. Beide Aspekte können die Sicherheit eines Systems erheblich schwächen, weil die Sicherheitsmaßnahmen nicht mehr oder nur noch halbherzig durchgeführt werden.

Bekannt gewordene Einbrüche in DV-Systeme hatten in der Regel nachlässige Administrierung der DV-Systeme als Ursache. Deshalb kommt den in den Kapiteln 9 und 10 formulierten organisatorischen und administrativen Maßnahmen zusammen mit den hier geforderten Automatismen besondere Bedeutung zu.

11.4.3 Sicherheitsstufen

Ein wesentlicher Aspekt einer Sicherheitsphilosophie ist die Möglichkeit des inkrementellen Ausbaus der Sicherheit.

Netzstrukturierung kann auch mit zu einem stufenweisen Aufbau einer Sicherheitsarchitektur herangezogen werden. Die verschiedenen Stufen unterscheiden sich nur in der Art des Übergangs zwischen Internet–Intranet und Intranet–Servernetz.



FW = Firewall, AA = Applikationsanbindung, PG = Provider-Gateway, FW + PG = IT-Sicherheitsserver

Abbildung 11.2: Sicherheitsstufenmodelle

(Die nachfolgend benutzten Nummern (n) beziehen sich auf das obige Diagramm)

- Der Einsatz einer Firewall (FW) am Übergang Internet–Intranet ist unverzichtbar.
- Die einfachste Variante (1) ist eine physische Kopplung zwischen Intranet und dem Servernetz. Dies ist heute üblicherweise der Fall.
- Am Übergang beider Netze wird ein zusätzlicher Firewall-Rechner verwendet (2), der z.B. dafür sorgen soll, dass RPC, UDP oder ähnliche Dienste, die die Applikationen im Servernetz untereinander verwenden, von den Endgeräten aus dem Intranet her nicht erreichbar sind. Ferner könnte in dieser Sicherheitsstufe bereits die Verwendung von vertrauenswürdigen GUIs zum Einsatz kommen.
- Anstelle einer Standard-Firewall könnte eine erweiterte Firewall (Application-Gateway) eingesetzt werden (3), um Funktionen wie sichere Authentifizierung, Vertrauenswürdigkeit der Verbindung (Private Virtual Channel (PVC)), TimeOut-Überwachung und Identifikationsmedienüberwachung bei Sitzungen für Nutzer aus dem Internet und/oder Intranet zu erzwingen.
- Die Absicherung kann weiter getrieben werden (4), indem zusätzlich das PG zusammen mit einem (zentralen) Berechtigungsserver die Funktion des Single-Signon (SSO) wahrnimmt und ein Application-Adapter AA für die heterogenen Anwendungen

im Verwaltungsservernetz gegenüber den Nutzern eine einheitliche Oberfläche was Zugang und GUI betrifft gewährleistet.

- Die Gewährleistung einer Rechtsverbindlichkeit elektronischer Vorgänge kann nur durch eine weitere Stufe (5) erreicht werden. Das gesamte beschriebene System muss zertifiziert werden, sowohl, was das Konzept betrifft, als auch einzelne Module wie Client, Chipkarten, Provider-Gateway (PG) etc., und muss in die Funktionen eines TrustCenters eingebunden sein.

Es ist wesentlicher Teil des BASILIKA-Projekts, solche Sicherheitsstufenmodelle vorzuschlagen, zu begründen, zu testen und zu validieren.

Kapitel 12

Zertifizierung von Sicherheitslösungen

12.1 Grundsätzliches zur Zertifizierung

Während die Betreiber von IT-Ressourcen meist selbst geeignete administrative Maßnahmen treffen und deren Einhaltung überwachen können (Revision), trifft dies für die Analyse und Bewertung der Sicherheitseigenschaften der eingesetzten Technik nur in Ausnahmefällen zu.

Es bedarf deshalb in Ergänzung der konzeptionellen und administrativen Vorkehrungen einer angemessenen **Überprüfung der technischen Sicherheitsvorkehrungen** sowie einer **Abnahmeprozedur**, bei der die sicherheitsgerechte Anwendung dieser Technik festgestellt wird.

Prüfverfahren der genannten Art sind Gegenstand von **Zertifizierungssystemen**, in denen Eigenschaften von Produkten und Prozessen untersucht werden: Beispiele hierzu sind die Bestätigung der Interoperabilität von „offenen“ Systemen bei X/Open und die Abnahme von Qualitätsmanagement-Systemen nach ISO 9000.

Diese Verfahren haben das Ziel, nachzuweisen, dass bestimmte Produkte oder Verfahren im Einklang mit (international akzeptierten) Normen stehen, d.h. es handelt sich um sogenannte Konformitätsprüfungen. Die meist privatwirtschaftlichen Träger solcher Prüfungen sind in Deutschland im Deutschen Akkreditierungsrat (DAR) vertreten.

12.1.1 Die Sicherheitszertifizierung

Die in diesem Bericht betrachtete Situation der missbräuchlichen Nutzung von IT-Ressourcen wird durch die herkömmlichen Zertifizierungssysteme nicht erfasst: Sie bestätigen letztlich nur die Eignung für den bestimmungsgemäßen Gebrauch, betrachten aber nicht oder nur sehr begrenzt die unsachgemäße, rechtswidrige, unkontrollierte, (vorsätzlich) missbräuchliche Verwendung (hier: von IT-Ressourcen).

Aus dieser Situation heraus sind in den 80er Jahren in den westlichen Industrie-Staaten **staatliche Zertifizierungssysteme** entstanden, die auf die **Sicherheit vor missbräuchlicher Nutzung von IT-Ressourcen** ausgerichtet sind[1].

Solche meist in internationale Anerkennungsvereinbarungen eingebundene Zertifizierungssysteme werden in Europa in einer Mischung aus privatwirtschaftlicher Prüfung und staatlicher Aufsicht und Zertifizierung durchgeführt[2].

12.1.2 Basis der Sicherheitszertifizierung für IT: ITSEC

Als technische Prüfgrundlage dient das international anerkannte und durch die Europäische Union zur Anwendung empfohlene Werk /ITSEC91/, mit dem das Sicherheitsniveau von IT-Systemen (Rechner, Netze, SmartCard-Anwendungen, u.v.m.) gegenüber potentieller missbräuchlicher Nutzung analysiert und bewertet werden kann.

Besonderes Anliegen bei der Konzeption dieser Prüfkriterien war es, keine Maximalforderungen an die Sicherheit zu stellen, sondern stets das **Angemessenheitsprinzip** zu beachten: In Abhängigkeit von

- den zu erreichenden Sicherheitszielen,
- der Bedeutung der zu prüfenden IT-Anwendung (und ihrer Daten) und
- dem als relevant erachteten Missbrauchspotential

werden technische und technisch-administrative Sicherheitsmaßnahmen in ihrer Wirkung analysiert und bewertet. Erkannte Schwachstellen können im Rahmen eines solchen Püfverfahrens behoben werden. Schlussendlich wird durch ein **amtliches Zeugnis (Zertifizierungsreport)** das erreichte Sicherheitsniveau bestätigt[3].

Je nach Sicherheitsstufe werden in /ITSEC91/ unterschiedliche Prüfmethoden definiert und in konkreten Zertifizierungen angewendet[4]. Die Spanne reicht dabei von ingenieurmäßigen Tests bis hin zur formalen Verifikation von Sicherheitseigenschaften.

---

[1] In Deutschland wird diese Aufgabe durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) wahrgenommen, das Träger des deutschen Zertifizierungssystems für IT-Sicherheit ist. Das BSI gehört zum Geschäftsbereich des Bundesministers des Innern; seine Aufgaben sind durch das BSI-Gesetz /BSIG/ geregelt.

[2] Je nach Rechtslage gelten in den beteiligten Staaten unterschiedliche Gewährleistungsbestimmungen. Für die Zertifizierungsergebnisse des BSI gilt das Prinzip der Staatshaftung.

[3] Das so skizzierte Verfahren wird heute in Großbritannien, Frankreich, Deutschland, USA und Kanada angewendet; die Ergebnisse werden de facto von vielen anderen Staaten anerkannt.

[4] Für tiefer gehende Informationen vgl. /ITSEC91/ und /ITSEM92/.

12.2 Zertifizierung von Unix und WindowsNT

12.2.1 Die Betriebssysteme Unix und WindowsNT

Allgemeines zu Unix

UNIX hatte vor ca. 25 Jahren seinen Ursprung im Forschungsbereich. Konzipiert als herstellerunabhängiges, portierbares Multiuser-Betriebssystem mit dem Schwerpunkt einer für die damalige Zeit hervorragenden Programmierunterstützung, war es ursprünglich weder für den kommerziellen Einsatz noch für Realzeitanforderungen vorgesehen.

Seinen heutigen hohen Reifegrad verdankt UNIX der Verbreitung im universitären und auch wissenschaftlichen Bereich und der Verfügbarkeit des Sourcecodes. Die öffentlich ausgetragenen Diskussionen aller Vor- und Nachteile, aller Schwachstellen und Fehler von UNIX wirkten sich anfangs imageschädigend aus, führten aber andererseits zu einem hohen Stabilitäts- und Reifegrad.

Als reines Multiuser-/Multitaskingsystem war es anfangs nur zum direkten Anschluss von Bildschirmen über serielle Schnittstellen (VT100 o.Ä.) konzipiert. Mit weiteren Entwicklungen wie X-Window und dem Internetprotokoll sowie den darauf basierenden Diensten wie NFS wurden die Grundlagen für die heutige Client/Server-Architektur geschaffen. Dadurch wurde UNIX für den kommerziellen Bereich so attraktiv, dass mit einer Fülle von Zusätzen wie Transaktionsmonitoren, Realzeitvarianten, Hochverfügbarkeitsvarianten, Management- und Security-Tools heute eine Vielzahl von Einsatzbereichen abgedeckt werden kann. Eine zwar langwierige doch erfolgreiche Arbeit von Normierungs- und Standardisierungsgremien verhalf den verschiedenen UNIX-Varianten zu zunehmender Übereinstimmung mit dem Ziel der Interoperabilität und der besseren Portierbarkeit von Applikationen — auch wenn immer noch ein großer Standardisierungsbedarf besteht.

Eine Unterscheidung in eine Client- und Serverarchitektur ist bei UNIX nicht vorhanden. Diese Beziehung wird durch die aktuelle Benutzung der Systeme bestimmt (wer fordert eine Dienstleistung, wie z.B. einen Zugriff auf eine entfernte Datei an, wer führt diese Dienstleistung aus). Trotzdem unterscheiden UNIX-Hersteller zwischen ihren Workstation- und Serverkonzepten, da typische UNIX-Server mit Funktionalitäten zur Erhöhung der Verfügbarkeit, der Verwaltung großer Datenmengen oder der Steigerung der Leistungsfähigkeit von Dateizugriffen über das Netz versehen sind und ihre Administrierung der Server trendgemäß mittels graphischer Tools ermöglicht wird.

Unix-Sicherheit unter dem Aspekt der Variantenvielfalt

Aussagen zur UNIX-Sicherheit sind durch die Variantenvielfalt wesentlich differenzierter zu betrachten als bei WINDOWSNT. Unter dem Sicherheitsaspekt wird im Folgenden nach drei prinzipiellen UNIX-Varianten unterschieden:

- dem Standard-UNIX mit einer Basissicherheit, die den aktuellen X/Open-Richtlinien entspricht,

- dem C2-UNIX, das den X/Open-Standard um einige Sicherheitsfunktionen zur Erreichung der C2-Funktionalität (vor allem die Protokollierung aller sicherheitsrelevanten Ereignisse sowie eine erweiterte Zugriffskontrolle, in der Regel durch Zugriffskontrolllisten) erweitert und
- den hochsicheren UNIX-Varianten, die den B-Klassen der Sicherheitskriterien[5], welche im Wesentlichen die Regeln der staatlichen Verschlusssachenanordnungen nachbilden, entsprechen. Dazu zählen die Version UNIX-ES (Enhanced Security) für B2 oder UNIX-MLS (Multi-Level-Security) für B1 oder UNIX-CMW (Compartmented Mode Workstation = MLS + Netzsicherheit[6] + sichere Windows-Oberfläche).

Allgemeines zu WindowsNT

Die Entstehung von WINDOWSNT hat den klassischen proprietären Hintergrund. Die Entwicklung liegt ausschließlich bei Microsoft. Sie begann im Jahre 1988 und war im Jahre 1993 in der Version WINDOWSNT 3.1 erstmals am Markt. Die Nichtverfügbarkeit des Sourcecodes und die Geheimhaltung interner Strukturen, wie der des NTFS-Dateisystems, machen den proprietären Charakter dieses Systems deutlich. Die wesentlichen Randbedingungen für die Entwicklung waren die Aufwärtskompatibilität der bisherigen WINDOWS-Applikationen, die Unterstützung von DOS-Applikationen, die Portierbarkeit des Systems auf andere Hardwareplattformen, die Erfüllung des C2-Sicherheitsstandards, der im rein kommerziellen Umfeld häufig gefordert wird, und die Unterstützung von Posix-Standards.

Für WINDOWSNT war von Anfang an der kommerzielle Kunde als Zielgruppe definiert und weder der technisch/wissenschaftliche Bereich noch der Homecomputerbereich. Wohl deshalb war das für den Transaktionsbetrieb erforderliche Realzeitverhalten durch das präemptive Multitaskingkonzept bereits berücksichtigt.

WINDOWSNT kennt zwar eine Unterscheidung in eine Client- und eine Servervariante, jedoch lediglich durch Zusätze bei der Servervariante zur Netzadministrierung, zur Unterstützung von bis zu 4 Prozessoren (Clientvariante maximal 2 Prozessoren) und in Mechanismen zur Unterstützung der Fehlertoleranz.

Eine Benutzung als reines Multiusersystem durch den direkten Anschluss mehrerer Bildschirme war nicht Bestandteil des Entwicklungskonzepts für WINDOWSNT. Stattdessen war es von Anfang an für die Einbindung in Netze konzipiert, wobei sich Microsoft an dem bewährten IP-Standard als Basisprotokoll orientierte.

[5] Die Sicherheitsstufen im Bereich der B-Klassen der Sicherheitskriterien beinhalten die Forderung, dass die Einstufung der Daten gemäß ihrer Vertraulichkeit nicht mehr benutzerabhängig sondern obligatorisch geschieht.

[6] Die Netzsicherheit umfasst üblicherweise MAC, DAC und Information-Labels, Secure-TCP/IP-Protocol, zentrales Facility-Management, vertrauenswürdiges Newsprint, Diskless-Client-Support, netzweites Audit und Multi-Level-Mail.

WindowsNT und seine Beziehung zur Hardware

Die in der UNIX-Welt vorhandene Variantenvielfalt spielt bei WINDOWSNT keine Rolle, da Microsoft als einziger Hersteller für die Entwicklung und Vermarktung verantwortlich zeichnet. Während jedoch im UNIX-Markt der Hardwarelieferant bisher identisch mit dem Betriebssystemlieferanten war und somit eine genau bekannte Hardware zugrunde lag[7], kann WINDOWSNT unabhängig vom Rechnersystem erworben werden und muss unterschiedliches Hardwaredesign der Motherboards sowie eine Vielzahl sonstiger Hardware berücksichtigen, die in der Intel-Rechner-Welt anzutreffen ist. Dieses Problem wurde durch eine zusätzliche Schicht zur Mikrokernelebene, die *Hardware Abstraction Layer (HAL)* gelöst, die das unterschiedliche Hardwaredesign bei gleichem Prozessortyp berücksichtigt.

Daneben gibt es Portierungen von WINDOWSNT auf andere Prozessorarchitekturen (wie den im Evaluierungsreport angeführten DEC Alpha-Chip). Diese Systeme werden üblicherweise wieder als eine Einheit direkt vom Rechnerhersteller angeboten.

Zusammenfassung

Beide Betriebssysteme sind Multitaskingsysteme mit integrierter Netzkomponente und graphischer Benutzeroberfläche. Jedoch ist WINDOWSNT im Gegensatz zu UNIX nicht als Multiusersystem konzipiert. WINDOWSNT unterstützt zu einem Zeitpunkt lediglich eine aktive Windowssitzung, so dass es eher als multitaskingfähiges Single-User-System zu bezeichnen ist, das den Benutzern des Netzes zusätzliche Netzserverdienste parallel zur Verfügung stellt.

Dagegen ist UNIX ein echtes Multiusersystem, das die gleichzeitige Sitzung mehrerer Benutzer ermöglicht. Damit die nachfolgend angeführten Sicherheitsfunktionen wirksam sind und nicht umgangen werden können, ist prinzipiell eine Unterstützung durch die Rechnerhardware erforderlich, die jedoch bei den heutigen Rechnerarchitekturen als gegeben vorausgesetzt werden kann.

12.2.2 Vergleich der Sicherheitsfunktion von Unix und WindowsNT

Identifikation/Authentifizierung

WINDOWSNT und die hier diskutierten UNIX-Varianten können die Forderungen nach C2 bezüglich der Identifikation/Authentifizierung erfüllen. Dazu sind entsprechende Auflagen zu berücksichtigen[8]. Eine Ergänzung der Zugangskontrolle zum Rechner durch Chipkarten oder biometrische Verfahren, wie sie der Markt in unterschiedlicher Leistungsbandbreite

[7] Diese Aussage trifft nicht mehr auf PC-UNIX-Varianten wie die verschiedenen Public-Domain-UNIX-Versionen (LINUX, FreeBSD etc.) zu, die wie WINDOWSNT eine Fülle an Motherboarddesigns und sonstigen Hardwarevarianten berücksichtigen müssen.

[8] Diese Aussage stimmt unter der Voraussetzung, dass durch die Administrierung die Login-Informationen in einer gesondert verborgenen Shadow-Datei liegen und die Vorgaben für Passwort-Mindestlänge, Passwort-Alterung und Vermeidung von Trivialpasswörtern eingestellt wurden. Detaillierte Angaben dazu enthalten die Zertifizierungsreports.

anbietet, kann den Zugangsschutz gerade unter dem Aspekt des Komforts erheblich verbessern.

WINDOWSNT erfüllt die die Trusted-Path-Anforderung (vertrauenswürdiger Pfad beim Login-Vorgang) aus der B2-Klasse der TCSEC[9]. Der vertrauenswürdige Pfad muss vom Benutzer zum Zeitpunkt des Logins durch Drücken von STRG-ALT-DEL initiiert werden. Die Standard-UNIX-Varianten erfüllen diese Forderung nicht, sehr wohl dagegen einige um die C2-Funktionalität erweiterte UNIX-Varianten sowie die CMW-, MLS- und ES-Varianten. Diese Systeme können den vertrauenswürdigen Pfad zusätzlich selbst initialisieren, z.B. nach einer Timeout-Bedingung.

Zugriffskontrolle

Bei WindowsNT kann zu jedem Zeitpunkt die Identität des Benutzers festgestellt werden, um eine korrekte Auswertung der Zugriffsrechte zu ermöglichen. Die Zugriffskontrolle ist nur wirksam bei Benutzung des WINDOWSNT File Systems (NTFS). Auf alle anderen Filesysteme — wie FAT und HPFS — ist diese Zugriffskontrolle nicht möglich. Die Zugriffsrechte werden auch unter der Windowsoberfläche bei Cut&Paste beachtet. Die Zugriffsrechte werden in Form diskreter Access-Control-Listen (ACLs) vergeben, wie es in der Stufe B2 explizit gefordert wird. Damit ist eine beliebig feine Granularität ermöglicht worden, deren Nutzung in der Verantwortung des Anwenders liegt. Rollenbasierte Zugriffsrechte zur Trennung verschiedener Funktionen, die in B2 ebenfalls gefordert werden, werden von WINDOWSNT zwar für die Rollentrennung des Operators vom Administrator aber nicht umgekehrt unterstützt (z.B. zur Durchführung des Backups).

Ebenso können bei Standard-UNIX zu jedem Zeitpunkt die Identitäten der Benutzer festgestellt werden und damit die Zugriffsrechte korrekt ausgewertet werden. Die Zugriffsrechte wirken auf alle Objekte des UNIX-Systems, auch auf Geräte. Ferner kann der Zugriff auf ganze Dateisysteme durch den Administrator bereits beim Mount generell auf Lesen eingeschränkt werden. X-Window basierende graphische Oberflächen wie Motif berücksichtigen jedoch bei Cut&Paste die Zugriffsrechte nicht. Die Zugriffsrechtegranularität besteht beim Standard-UNIX lediglich aus den Lese-, Schreib- und Ausführrechten für den Eigentümer, eine Gruppe und den Rest der Welt. Diese Granularität, die den C2-Forderungen der TCSEC nicht ganz gerecht wird, ist relativ grob, und es ist im Einzelfall zu prüfen, inwieweit diese Rechtestruktur dem eigenen Sicherheitsbedarf genügt.

Die C2-Anforderungen des amerikanischen *Orange Book* an die Granularität der Rechteverwaltung haben dazu geführt, dass viele UNIX-Varianten eine Rechtevergabe auf Basis von ACLs zusätzlich zur UNIX-Rechtestruktur anbieten, die eine beliebig feine Granularität der Zugriffsrechte ermöglichen und damit der WINDOWSNT-Lösung entsprechen. Um die UNIX-Kompatibilität zu wahren, wurden die Standard-UNIX-Rechte zusätzlich beibehalten, was sich leicht verwirrend auswirken kann.

Bei den B1/B2-UNIX-Varianten existiert zusätzlich zur benutzergesteuerten Zugriffskontrolle eine *Mandatory Access Control (MAC)* mit einer obligatorischen Einstufung in eine

[9] TCSEC = Trusted Computer Security Evaluation Criteria, auch bekannt unter dem Namen *Orange Book*, nationale Sicherheitskriterien der USA für Rechner

Ermächtigungsstufe für die eingeloggten Personen und einer erzwungenen Einstufung der Daten. Zur Unterstützung des „need-to-know“-Prinzips gehört das Konzept der Abschottung verschiedener Bereiche durch eine Kategorisierung. MLS- und CMW-UNIX genügen der B1- und UNIX-ES der B2-Sicherheitsklasse. Der in diesen Klassen nicht umgehbare Zugriffsschutz ist nicht nur für den VS-Bereich interessant, sondern kann gerade im Bereich des Persönlichkeitsschutzes (BDSG) sinnvoll zum Tragen kommen.[10] UNIX-ES bietet darüber hinaus frei konfigurierbare rollenbasierte Zugriffsrechte für die sicherheitsrelevanten Funktionsaufrufe an. Dadurch ist eine exakte Anpassung der verschiedenen Rollen an die administrativen Aufgabenbereiche möglich. Außerdem ist dem Systemadministrator der Zugriff auf eingestufte Daten verwehrt, da er seine Systemarbeiten mit der niedrigsten Ermächtigungsstufe durchführen muss (Systemparameter sind offen eingestuft und unterliegen den klassischen Schutzmechanismen von UNIX). Damit werden sogar Anforderungen aus der B3-Klasse erfüllt, die unter den Aspekten Revision und Datenschutz im kommerziellen Umfeld durchaus Sinn machen.

Wiederaufbereitung und Protokollierung

Unter der Wiederaufbereitung versteht man den Schutz der Informationen auf wiederverwendbaren Medien. Wird beispielsweise eine Datei neu angelegt, so darf kein Rückschluss auf den früheren Inhalt des zugeordneten Massenspeichers möglich sein. Es muss eine Initialisierung erzwungen werden. Diese Anforderungen werden von allen hier genannten Systemen gemäß C2 erfüllt, sowohl für den Massenspeicherbereich als auch für den Arbeitsspeicher.

Standard-UNIX bietet keine einheitliche Protokollierungskomponente. Es können eine Reihe verschiedener Audit-Einträge des Systems und Audit-Einträge durch Programme vorgenommen werden. Eine Zuordnung der Protokolleinträge zu einem Benutzer wird erschwert, da mehrere Logins mit derselben Benutzer-ID möglich sind und zusätzlich die Identität verändert werden kann[11]. Eine Kontrolle der Aktivitäten zur Laufzeit ist wegen des damit verbundenen Aufwands nur in Einzelfällen sinnvoll. Die übrigen UNIX-Varianten erfüllen ebenso wie WINDOWSNT die C2-Anforderungen der TCSEC und sind sehr fein konfigurierbar, um die Datenmenge auf den erforderlichen Informationsbedarf einzuschränken. Die B-Varianten protokollieren auch alle Veränderungen an den Einstufungen der Daten und den Ermächtigungen der Personen. Um die Eindeutigkeit bei Veränderung der Benutzer-ID zu gewährleisten, wurde bei diesen Systemen eine weitere Benutzerkennung eingeführt, die nicht veränderbar ist. Durch die im ES-System mögliche Rollentrennung (Sicherheitsbeauftragter, Operator usw.) kann dem Systemadministrator der Zugriff auf die Protokolldaten verwehrt werden.

[10] Beispiel: Der Schutzbedarf von Patientendaten kann im Krankenhaus durchaus in mehrere Bereiche unterteilt werden: Daten, die nur dem behandelnden Arzt zur Verfügung stehen, Daten, die dem Pflegepersonal der Station zur Verfügung stehen und Daten, die auch der Verwaltung zur Verfügung stehen. Die Daten stehen anderen Stationen nicht zur Verfügung.

[11] z. B. durch das SU-Kommando oder S-Bit-Programme.

Administrierungssunterstützung

Die Administrierung von WINDOWSNT geschieht mit den in der PC-Welt üblichen graphischen Benutzeroberflächen. Für den UNIX-Administrator gibt es inzwischen eine Fülle an Administrierungstools, jedoch von unterschiedlicher Qualität. Die am Markt verfügbaren Managementtools können vor allem dem Administrierungsneuling die Arbeit erleichtern, zumal gerade für das Sicherheitsmanagement ausgeklügelte zertifizierte Produkte erhältlich sind. Der versierte Administrator dagegen wird in vielen Fällen auf eigene, zusätzliche Shellskripts, vor allem wegen der Mächtigkeit dieser Werkzeuge, nicht mehr verzichten wollen.

Echtzeitverhalten

WINDOWSNT ist im Kern für Echtzeitanforderungen vorbereitet. Da WINDOWSNT im kommerziellen Markt angesiedelt war, wurden die Anforderungen von Transaktionsmonitoren berücksichtigt. Als präemptives Multitaskingsystem ist es bereits im Design für diese Einsatzgebiete vorbereitet und sollte mit diesen Anforderungen keine Probleme haben. Die Skalierbarkeit zur Abdeckung unterschiedlicher Leistungsanforderungen reicht in der Serverversion bis zu maximal 4 Prozessoren und wird durch die Verfügbarkeit des Systems auf leistungsfähigen RISC-Architekturen noch erhöht. Für kleine bis mittlere Abteilungen reicht diese Leistungsbandbreite durchaus aus.

Dagegen war die Gewähr der Bereitstellung einer angeforderten Dienstleistung in einem vorgegebenen Zeitrahmen für die UNIX-Entwickler ursprünglich kein Thema. Dies vereinfachte die Kernelprogrammierung von UNIX, da das System non-präemptiv konzipiert werden konnte, erschwerte aber den Einsatz in Umgebungen mit Realtime- oder Transaktionsanforderungen. Spezialvarianten und Zusatzprodukte tragen diesem Bedarf Rechnung, angefangen von neu entwickelten UNIX-Varianten mit präemptivem Multitasking über Systeme mit vielen Unterbrechungspunkten bis hin zu einer Vielfalt an Transaktionsmonitoren. Mit den inzwischen vorliegenden Posix-Standards (Posix 1003.1 und 1003.2), denen bereits mehrere UNIX-Varianten genügen[12], wie entsprechende ITSEC-Zertifikate nachweisen, ist heute vom Betriebssystem her auch der kommerzielle Bedarf mit UNIX-Servern abdeckbar. Auch die zweite Voraussetzung für die Gewähr kurzer Antwortzeiten, nämlich die Leistungsanpassung der Hardware an den erwarteten Transaktionsdurchsatz, ist mit der bei den heutigen UNIX-Serverarchitekturen skalierbaren Leistung vom Einzel-PC bis zur Mainframeklasse mit Kanal- und Multiprozessorarchitekturen im Leistungsbereich von Vektorrechnern ebenfalls erfüllt.

Ausfallsicherheit

Gerade im kommerziellen Bereich gewinnen Aspekte der Ausfallsicherheit eine immer größere Bedeutung. Es ist naheliegend, dass zur Erreichung einer hohen Ausfallsicherheit ein erhebliches Maß an Hardwareunterstützung bereitgestellt werden muss (z.B. Erfassung

[12] Ein entsprechender Nachweis wurde mittels ITSEC-Zertifikat für die Produkte MAXION/OS und HP/UX 10 erbracht.

von Messdaten wie Wärmeentwicklung, Zeitmessungen des I/O-Verhaltens und unterbrechungsfreies Abschalten von defekten Komponenten). Zusätzlich muss die Software in der Lage sein, alle Daten auszuwerten und sinnvolle Aktionen durchzuführen. Die Ausstattung mit ausfallsicheren Massenspeichern (wie RAID-Systemen) bis hin zur Schaffung von Redundanzen (wie komplett gespiegelten Rechnersystemen) erfordert eine aufwendige softwaretechnische Überwachung, die weit über das hinausgeht, was Standard-UNIX-Betriebssysteme leisten können. Hier muss also auf spezielle Lösungen der UNIX-Hersteller oder Third-Party-Produkte zurückgegriffen werden, die allerdings Verfügbarkeiten von über 99,9% garantieren können. Eine zuverlässige Aussage zur Ausfallsicherheit ist auf Basis der europäischen Sicherheitskriterien durchaus in Form eines Zertifikates zu erbringen und liegt für mehrere UNIX-Produkte vor[13]. WINDOWSNT bietet in der Servervariante Mechanismen zur Fehlertoleranz an, diese waren jedoch nicht Gegenstand der US-Evaluierung.

12.2.3 Verbesserung der Sicherheit im Netz

Angriffe auf das Netz sind mit den originären Mechanismen der Betriebssysteme nicht abzuwehren. Daher sind alle bisherigen C2-Sicherheitszertifikate — sowohl für UNIX als auch für WINDOWSNT — nicht für den Betrieb in einem inhomogenen Netz gültig. Lösungen zeichnen sich durch den Einsatz von LAN-Verschlüsselungskomponenten oder neuen Netzdiensten (wie DCE oder dem neuen Internet-Protokollstandard IPv6) ab.

Aufbau eines homogenen LAN

Durch einheitliche Plattformen im LAN, ergänzt durch eine zentrale Administrierung und einen physischen oder kryptologischen Schutz der Netzkomponenten kann sowohl für WINDOWSNT als auch für die C2-UNIX-Varianten ein Lösungsansatz geschaffen werden, der ein verbessertes Maß an Netzsicherheit ermöglicht. Unter dieser Voraussetzung und weiteren Auflagen behalten sogar einige C2-Zertifikate im Netz ihre Gültigkeit, wie das in Großbritannien erteilte WINDOWSNT-Zertifikat und einige UNIX-Zertifikate zeigen. Unter der Voraussetzung eines homogenen Netzes gibt es einen weiteren Zugewinn an Sicherheit durch UNIX-CMW und durch die Netz-Ergänzung *Enhanced Administration and Networking (EAN)* zu UNIX-ES. Diese Erweiterung, die auf der *Network Access Architecture (NAA)* basiert, ermöglicht jedoch nur dann eine erhebliche Verbesserung der Sicherheitseigenschaften im LAN, wenn die Sicherheitseigenschaften von allen Partnern im Netz unterstützt werden. Bei diesen Sicherheitsfunktionen in Netzen besteht i. Allg. nur die Wahl zwischen Einigung auf einer Minimalbasis oder dem Abbruch der Beziehungen, je nachdem, ob in der Anwendungsumgebung Kommunikation oder Sicherheit als vorrangig bewertet wird.

Einsatz von X11-Terminals im Unix-LAN

Werden im LAN ausschließlich X11-Terminals angeschlossen, so erreicht man einen Sicherheitsgrad, der Mehrplatzanlagen nahe kommt. Die direkte Bedrohung der Netz-

[13] Dazu gehören GUARDIAN 90 von Tandem Computer, DG/UX B2 SO von Data General und DYNIX PTX von Sequent Computer.

infrastruktur kann aber auch damit nicht gelöst werden. Durch CMW-konforme X11-Implementierungen konnte die fehlende Zugriffskontrolle der X-Window-Oberfläche nicht nur ausgeglichen werden, sie genügt sogar den Regeln des obligatorischen Zugriffsschutzes. Dieser Lösungsansatz wurde an einigen Stellen erprobt und hat sich bewährt, konnte sich aber trotz der sicherheitstechnischen und administrativen Vorteile kaum durchsetzen, wohl dadurch bedingt, dass er in der Konkurrenzsituation zum PC als zu teuer empfunden wurde.

Eine sichere Alternative zum LAN: Unix als Multiusersystem

Wird UNIX gemäß seiner ursprünglichen Konzeption als reines, unvernetztes Multiusersystem mit mehreren VT100-konformen Bildschirmen ausgestattet, kommt die UNIX-Sicherheit voll zum Tragen. Dies wird durch die bisher zertifizierten C2- und B1/B2-konformen UNIX-Varianten bestätigt, für die das Zertifikat genau in dieser Einsatzumgebung gilt. Aus Sicht des Anwenders mag der Verzicht auf eine graphische Oberfläche vorsintflutlich wirken, aber für Applikationen, die vorwiegend eine maskenorientierte Eingabe erfordern — wie im Transaktionsbetrieb üblich — genügt diese Darstellung durchaus. Bedenkt man den Ressourcenbedarf, den die graphischen Oberflächen gerade hinsichtlich der Rechenleistung und des Arbeitsspeichers verbrauchen, kann man üblicherweise sowohl mit geringeren Prozessorleistungen auskommen als auch mit besseren Antwortzeiten rechnen. Die Störanfälligkeit und die Komplexität der Fehlersuche reduzieren sich bei fehlendem LAN nicht unerheblich. Auch wenn UNIX-Workstations mit ihren graphischen Oberflächen brillieren, ist der hier vorgestellte Lösungsansatz unter mehreren Aspekten und besonders unter denen der Sicherheit, der Kosten und der Administrierbarkeit für kommerzielle Nutzer nicht uninteressant.

12.2.4 Zertifizierungen von WindowsNT

In den USA erzwingen die TCSEC des Department of Defense die Definition und Prüfung der „Trusted Computing Base“, das heißt, aller Teile des Systems, die sicherheitsrelevant sind. Diese müssen geprüft werden. Das hat bei Betriebssystemen immer zur Folge, dass die sicherheitsrelevanten Teile der Hardware und Firmware mitgeprüft werden müssen und die Aussagen des Evaluierungsreports auf exakt diese Hardware einzuschränken sind. Im Fall von WINDOWSNT wird gemäß dieser Strategie der Prozessor, das Motherboard, das BIOS und weitere unterstützende Hardware wie die Konfigurationsdatenbank des Rechners mit einbezogen.

Die ITSEC dagegen lassen die Prüfung eines Produkts zu, ohne sicherheitsrelevante Teile anderer Komponenten in gleicher Prüftiefe zu evaluieren. Im Zertifizierungsreport werden dann die Anforderungen an unterstützende Mechanismen der Hard- und Firmware oder sonstiger Komponenten zur Gewährleistung der beschriebenen Sicherheit als Anforderungskatalog an diese Komponenten aufgeführt. Diese Anforderungen können einerseits als Vorgabe für die Zertifizierung dieser Komponenten dienen, andererseits werden aber konkrete Installationen im Rahmen der ITSEC-Tests geprüft, für die das Zertifikat dann tatsächlich gilt.

Vorteil der europäischen Vorgehensweise ist eine größere Flexibilität der Einsatzumgebung des Produkts und ein geringerer Prüfaufwand für das entsprechende Produkt. Als Nachteil muss die größere Unsicherheit angesehen werden, wenn das Produkt nicht exakt in der zertifizierten Einsatzumgebung genutzt wird. Die Systemzertifizierung ermöglicht die passende Lösung dieses Problems, wie später noch erläutert wird.

Im Folgenden werden die Voraussetzungen für die Evaluierung bzw. Zertifizierung von WINDOWSNT in den USA und in Großbritannien näher beschrieben. Es wird jedoch ausdrücklich darauf hingewiesen, dass die hier aufgeführten Aspekte einen Auszug aus den Reports darstellen und eine erste Orientierungshilfe geben sollen. Für den sicheren Betrieb ist es unbedingt erforderlich, den Report beim Hersteller direkt anzufordern, damit die beschriebene Sicherheitsleistung tatsächlich zum Tragen kommt.

C2-Evaluierung von WindowsNT 3.5 mit U.S. Service Pack 3 in den USA

In den USA wurde die Evaluierung von WINDOWSNT nach den TCSEC gemäß C2 am 14. Februar 1996 abgeschlossen. Die Evaluierung bezog sich sowohl auf die Client- als auch auf die Serverversion. Die Sicherheitsaussagen gelten ausschließlich für die Version 3.5 mit den im Service Pack 3 enthaltenen Korrekturen[14]. Die Posix- und OS/2-Subsysteme müssen „disabled“ sein. Die Sicherheitsaussagen gelten nur für die Standalone-Versionen folgender Hardware:

- Compaq Proliant 2000 und 4000
- DECpc AXP/150

Die Aussagen zur Sicherheit gelten nicht für den Betrieb auf anderen Hardwareplattformen als den oben genannten und nicht für den Betrieb im Netz.

Der direkte Zugriff auf das System darf für Unbefugte nicht möglich sein. Die beiden hier geprüften Rechnertypen

- besitzen dazu ein physisch abschließbares Gehäuse;
- haben einen Bootschutz durch das Power-On-Password;
- können das Booten von externen Medien — wie vom Floppy-Laufwerk — konfigurierbar abschalten; diese Konfiguration (im Non-Volatile Random Access Memory (NVRAM)) ist durch ein Passwort geschützt[15];
- bieten Schutz des Systemdatums und der Systemzeit; diese Daten müssen durch den *Hardware Configuration Editor* nach dem Booten von MS-DOS durch einen speziellen Hardware-Editor gesetzt werden; die Daten sind nur dann geschützt, wenn die Konfiguration das Booten über Floppy-Laufwerke verhindert und keine MS-DOS-Partition auf der Festplatte angelegt wurde; im MS-DOS-Emulationsmode unter WINDOWSNT hat der User keinen Zugriff auf diese Daten, die im NVRAM abgelegt sind.

[14] Die aktuelle Version 4.x ist nicht zertifiziert.

[15] Bei Zugriff auf das System kann das Passwort zurückgesetzt werden.

F-C2/E3-Zertifizierung von WindowsNT 3.51 in Großbritannien mit Netzeinbindung

Das Zertifikat wurde gemäß den ITSEC-Kriterien erteilt. Die Funktionalität entspricht der F-C2 Klasse, die Korrektheit wurde gemäß E3 geprüft[16]. Die exakte Bezeichnung des zertifizierten Produkts ist WINDOWSNT Version 3.51 Build 1057. Von den vier verfügbaren Protokollen wurden NetBEUI und TCP/IP getestet.

Das Zertifikat gilt für folgende Hardware, wobei jedoch das BIOS und sonstige Firmware nicht Bestandteile der Zertifizierung waren:

- Compaq Proliant 4500 5/100, als Server mit 1 und 2 Prozessoren;
- Compaq Deskpro 5/90, als Server und Workstation;
- Compaq Proliant 2000, als Server;
- Compaq Deskpro XL 5/66 und 5/133, als Server und Workstation;
- Compaq Prosignia 300 5/90, als Workstation.

Dabei müssen die Compaq-Konfigurationssoftware und die FAT-Diskpartition entfernt werden und außerdem als Ersatz für die existierenden Files die Patch-Files LSASS.EXE und LSASRV.DLL zur Standard-Installation angefordert werden.

Die Gültigkeit der Sicherheitsaussagen wird auch auf das Netz ausgedehnt unter folgenden Voraussetzungen:

- Es dürfen nur Clients und Server benutzt werden, die dem Zertifikat entsprechen.
- Zentrale Security- und Netzadministration.
- Jeder Benutzer innerhalb des Netzes hat eine eindeutige Benutzer-ID und ein geheimes Passwort.
- Die vom Benutzer abhängige Qualität des Passworts muss ausreichend hoch sein. (Motivation!)
- Die Audit-Daten sind regelmäßig zu prüfen — auch um einen Überlauf zu vermeiden.
- Der Gast-Account ist zu außer Kraft zu setzen.
- Prozeduren zum Schutz des Exports und der exportierten Informationen (wie auf removable Medien oder Drucker) müssen existieren.
- Passwort-Cache darf im gesamten Netz nicht konfiguriert sein.
- Benutzer sind zur Nutzung der *Trusted-Path-Feature* anzuhalten (Einloggen, Locking und Shutdown).
- Die Benutzer bekommen nur die unbedingt erforderlichen Rechte (least privilege).
- Jede Domain und jeder Computer erhält einen eindeutigen Namen.
- Wenigstens ein Administrator unterliegt nicht dem Account Lockout.
- Das Booten von externen Medien darf für Benutzer nicht möglich sein.
- Der physische Zugang zum Computersystem und den Netzkomponenten einschließlich dem Kabel ist auf den erforderlichen Personenkreis zu beschränken.

[16] Die aktuelle Version 4.x ist nicht zertifiziert.

- Es darf nur autorisierte Software eingespielt werden.
- Zur Gewährleistung der Auswertbarkeit der Audit-Informationen über einen größeren Zeitraum sind alle Änderungen der User-Accounts in einer externen Audit-Datei mit zu protokollieren.

12.2.5 Auszug aus den Unix-Zertifizierungslisten (D, GB und USA)

Wegen der Fülle der Zertifikate für UNIX-Produkte wird auf eine detaillierte Betrachtung verzichtet. Die folgende Liste soll jedoch eine erste Orientierungshilfe bieten. Bei näherem Interesse ist auch hier der entsprechende Report von der Zertifizierungsstelle oder dem Hersteller anzufordern.

Produkt	**E-Stufe**	**Hersteller/Vertreiber**	**Zertifiziert am:**
UTS/MLS, Version 2.1.5+	B1 UNIX	Amdahl	Completed 01/07/94
Argus B1/CMW and C2/TMW (on Solaris 2.4)	F-B1, E3 / F-C2, E3	Argus Systems Group	in Evaluierung
System V/MLS, Release 1.2.0u	B1 UNIX	AT&T	Completed 09/01/92
Assurix C2 3.2	F-C2, E2	Bull Information Systems	Mai 1995
DPX/20 CMW	F-B1, E3	Bull Information Systems	November 1994
Securics V. 7.7.0.1	F-C2, E3	Bull Information Systems	September 1994
Securics B1+ V. 6.5.4	F-B1, UKL3	Bull Information Systems	März 1992
BEST-X/C2	F-C2, E3	Bull Information Systems	in Evaluierung
MAXION/OS 1.2	F-C2, E3	Concurrent Computer	in Evaluierung
Power SX	F-B1, -B2, E3	Cyber Guard Europe LtD	in Evaluierung
DG/UX B2 S0	F-B2, E4	Data General	in Evaluierung
DG/UX	B2 UNIX	Data General	Completed 03/09/93
DEC MLS+CMW V3.1A	F-B1, E3	DEC	Oktober 1996
ULTRIX MLS+	B1 CMW	DEC	Entered VAP 04/21/93
Trusted EDI on Solaris Security Features	X435	EDS	in Evaluierung
UTX/32S Release 1.0	C2 UNIX	Encore Computer	Completed 12/31/86
Fujitsu-ICL-Security Ext. for SCO UNIXWARE	Zusätze zu F-C2, E2	Fujitsu-ICL Computers	in Evaluierung

Produkt	E-Stufe	Hersteller/Vertreiber	Zertifiziert am:
CX/SX 6.1.1 with LAN/SX 6.1.1	B1	Harris	Completed 09/15/93
CX/SX 6.1.1	B1 UNIX	Harris Corporation	Completed 09/15/93
HP-UX V10	F-C2, E3	Hewlett Packard	in Evaluierung
CMW Plus	B1 CMW	Hewlett Packard	Entered VAP 05/14/93
HP-UX BLS release 9.0.9+	B1 UNIX	Hewlett Packard	RAMP Completed 12/01/94
AIX CMW	B1 CMW	IBM	Entered DAP 06/01/91
AIX V 4.2	F-C2, E3	IBM Deutschland	in Evaluierung
IBM E3/CMW for AIX	F-B1, E3	IBM United Kingdom	April 1996
IBM Shield	F-C2, E2	IBM United Kingdom	April 1996
ICL UNIX Version 7 level 2	F-C2, E2	International Computers	April 1995
ICL UNIX Version 7 level 5	F-C2, E2	International Computers	April 1995
Best-X/B1	F-B1, E3	International Computers	April 1996
SECUREPAK Security Admin.Tool	Subsystem	Openvision	Completed 11/22/91
SCO UNIX Ware 2.1	F-C2, E2	SCO	in Evaluierung
SCO CMW+ R. 3.0	F-B1, E3	SCO	in Evaluierung
CMW+ for Open Desktop	C2 UNIX	SecureWare	Entered VAP 03/10/93
CMW+ for Open Desktop	B1 UNIX	SecureWare	Entered VAP 03/10/93
Sequent DYNIX PTX UNIX	F-C2, E3	Sequent Computer	in Evaluierung
Sequent Trusted PTX UNIX	F-B1, E3	Sequent Computer	in Evaluierung
DYNIX/PTX	C2 UNIX	Sequent Computer	Entered Advice 09/08/94
Trusted PTX	B1 UNIX	Sequent Computer	Entered Advice 09/08/94
Reliant UNIX 5.43 / AUDIT 2.0	F-C2, E3	Siemens Nixdorf	in Re-Evaluierung
SINIX V5.42/AUDIT V1.0	F-C2, E2	Siemens Nixdorf	1995
Trusted IRIX/B release 4.0.5EPL	B1 UNIX	Silicon Graphics	Completed 02/06/95
Sun Solaris 2.4 SE	F-C2, E2	Sun Microsystems	November 1995
Sun Trusted Solaris 1.2	F-B1, E3	Sun Microsystems	November 1995
Trusted Solaris Version 1.1	B1 CMW	Sun Microsystems	Entered Formal 10/07/94
Trusted XENIX 4.0	B2 UNIX	Trusted Information Systems	RAMP Completed 09/17/93

Tabelle 12.1: Zertifikate für UNIX*-Produkte*

12.2.6 Das Systemzertifikat — die passende Lösung

Anwender haben die Möglichkeit, die reale Sicherheit ihrer konkreten Installation mit allen tatsächlich vor Ort existierenden Bedrohungen in Form einer Systemzertifizierung vom BSI nachweisen zu lassen. So kann beispielsweise eine Institution ihre Sicherheitsanforderungen als Sollvorgabe für eine Systemzertifizierung entwickeln und damit schlussendlich ein Ergebnis bekommen, das alle sicherheitsrelevanten Rahmenbedingungen und Arbeitsanweisungen beinhaltet. Werden Produkte eingesetzt, die bereits ein Zertifikat haben, reduziert sich der Zertifizierungsaufwand beträchtlich, da dann nur die Einsatzumgebung zu prüfen ist.

12.2.7 Internationale Anerkennung der Zertifizierungsergebnisse

Intensive Bemühungen der verschiedenen Staaten in Europa haben zu den harmonisierten europäischen Sicherheitskriterien ITSEC geführt und einigen daraus resultierenden Abkommen zur gegenseitigen Anerkennung der Zertifikate (wie mit der Schweiz und Großbritannien). Eine weitere Anerkennung der Zertifikate im gesamten EU-Bereich ist demnächst zu erwarten.

Das Bestreben, auch mit den USA zu einer gegenseitigen Anerkennung der Zertifikate zu kommen, hat inzwischen zu den *Common Criteria (CC)* /CC98/ geführt, die derzeit im Rahmen von Probeevaluierungen ihre Praktikabilität unter Beweis stellen müssen.

Bis zum Abschluss der Verhandlungen über die gegenseitige Anerkennung der Zertifikate mit den USA ist ein Vergleich der Evaluierungsergebnisse nur eingeschränkt möglich. So gibt es keine Gewähr, dass das in Deutschland erworbene Produkt tatsächlich dem in den USA geprüften entspricht — ganz zu schweigen von der Möglichkeit, dass Exportvarianten des Produkts gezielte Unsicherheiten beinhalten können (Beispiel: verkürzte Schlüssel in kryptographischen Algorithmen). Eine Zertifizierung in Deutschland beinhaltet durch das festgelegte Auslieferungsverfahren für den Anwender die Gewähr, das zertifizierte Produkt tatsächlich zu erhalten.

Trotzdem ist mit Hilfe des in den USA veröffentlichten Evaluierungsreports eine verbesserte Nutzung der Sicherheitsleistung für den europäischen Anwender möglich, wie die hier wiedergegebenen Informationen aus dem WINDOWSNT-Report eindeutig zeigen.

12.3 Sicherheitsvorgaben für die Zertifizierung von Firewalls

Zum Zwecke der Zertifizierung einzelner Firewalls (Sache der Anbieter) oder konkreter Firewall-Installationen (Sache des Betreibers) ist es sinnvoll, Sicherheitsziele, Bedrohungen und Sicherheitsfunktionen einander gegenüberzustellen und in der nachfolgenden

Form zu beschreiben. Das entsprechende Dokument trägt gemäß /ITSEC91/ die Bezeichnung *Sicherheitsvorgaben.* Zur Darstellung wird entsprechend der dortigen Vorlage folgende Gliederung gewählt:

- Festlegung des Evaluationsgegenstands (EVG) und Beschreibung der Art der Nutzung;
- Beschreibung der administrativen und technischen Einsatzumgebung;
- Definition der Objekte, Subjekte und Zugriffsarten;
- Sicherheitsziele und Bedrohungen;
- Beschreibung der Sicherheitsfunktionen;
- Beschreibung der Mechanismen (optional);
- Evaluierungsstufe und Mechanismenstärke.

12.3.1 Festlegung des Evaluationsgegenstands und Beschreibung der Art der Nutzung

Der Evaluationsgegenstand (EVG) ist eine Internet-Firewall, die aus Software-, Firmware- und Hardwareanteilen und der zugehörigen Dokumentation besteht.

Anmerkung: Für ein reales Produkt müssen vollständige Angaben geliefert werden, die natürlich produktspezifisch sind. Zum Beispiel sind Angaben darüber notwendig, ob der EVG einer bestimmten Plattform (z.B. eines spezifischen Betriebssystems) bedarf. Dies ist insbesondere dann notwendig, wenn durch solche Teile sicherheitsrelevante oder gar sicherheitsspezifische Funktionen des EVG unterstützt werden.

Die Art der Nutzung der Internet-Firewall wird wie folgt beschrieben:

Der EVG ist eine Anordnung aus Soft-, Firm- und Hardware zum Anschluss eines Netzes an das Internet unter Beachtung von Sicherheitsauflagen. Er ermöglicht den Abruf von Informationen für Nutzer aus dem Internet und stellt für interne Nutzer Internet-Dienste zur Verfügung. Insbesondere verfügt der EVG über Funktionen, die unbefugte Änderungen am EVG verhindern. Für ein konkretes Produkt sind detailliertere Informationen nötig.

12.3.2 Beschreibung der administrativen und technischen Einsatzumgebung

Administrative Einsatzumgebung: Es wird davon ausgegangen, dass der EVG so aufgestellt wird, dass er für Unbefugte nicht frei zugänglich ist. Das zu schützende Netz besitzt außer der Schnittstelle zum EVG keine weitere Schnittstelle, über die eine Verbindung zum Internet zustande kommen kann.

Technische Einsatzumgebung: Der EVG verfügt über mindestens zwei externe Schnittstellen: zum Internet und zum zu schützenden Netz. Weitere externe Schnittstellen werden u.U. für Wartungszwecke und zur Administration bereitgestellt. Der Info-Server, der Administrations-PC und das Application-Gateway können über die Konsole gewartet und administriert werden. Für ein konkretes Produkt sind detailliertere Informationen nötig: z.B. Schnittstellen zu einem Betriebssystem.

12.3.3 Definition der Objekte, Subjekte und Zugriffsarten

Durch die Definition von Objekten, Subjekten und Zugriffsarten kann beschrieben werden, welche Art Schutz der EVG bietet. Schutzbedürftig können z.B. Dateien und Devices, Arbeitsspeicherinhalte, laufende Prozesse, technische Funktionen und Komponenten usw. sein. Man spricht in diesem Zusammenhang von den schutzbedürftigen Objekten.

Diesen stehen Subjekte (Personen und Rollen, die von ihnen gestarteten Prozesse, technische Funktionseinheiten) gegenüber, die potentiell Objekte bedrohen können — etwa in manipulativer Absicht oder ähnlich wirkender Weise.

Mit diesen Begriffen können die Sicherheitseigenschaften typischerweise etwa wie folgt beschrieben werden:

Der EVG kennt folgende Subjekte, Objekte und Zugriffsarten:

Subjekte sind

- S1: authentifizierte Teilnehmer und die von ihnen initiierten Prozesse,
- S2: nicht authentifizierte Teilnehmer,
- S3: der System-Verwalter,
- S4: der Revisor (optional).

Objekte sind

- D1: Daten zur Konfiguration des EVG (Dateien, Inhalte nichtflüchtiger Speicher),
- D2: Daten des EVG, die als Programm ausführbar sind,
- D3: Datenpakete, die sich innerhalb des EVG befinden,
- D4: alle Daten des EVG, soweit sie nicht zu D1, D2 oder D3 gehören,
- D5: Daten im zu schützenden Netz,
- D6: Datenpakete im Internet.

Zugriffsarten sind

- A1: Lesen,
- A2: Schreiben,
- A3: Ausführen.

Subjekte sollen nur in definierter und erlaubter Weise auf Objekte zugreifen. Daher ist manche mögliche Kombination eines Subjekts, einer Zugriffsart und eines Objekts durch den EVG zu unterbinden. Der EVG muss z.B. wirksam verhindern, dass ein nicht authentifizierter Teilnehmer (S2) ein Programm (D2) ausführt (A3), mit dem Konfigurationsdaten (D1) geschrieben (A2) werden können.

Welche Objekte, Subjekte und Zugriffsarten betrachtet werden, ist im Einzelfall festzulegen.

12.3.4 Sicherheitsziele und Bedrohungen

Nach den zuvor genannten Grundlagen kann nun beschrieben werden, welche Sicherheitsziele verfolgt werden und welche Bedrohungen abgewehrt werden sollen.

Die in den ITSEC betrachteten Sicherheitsziele sind

- Vertraulichkeit,
- Unversehrtheit / Integrität,
- Verfügbarkeit.

Die ITSEC bewerten einen EVG im Hinblick darauf, ob die in den Sicherheitsvorgaben genannte Kombination von Vertraulichkeit, Verfügbarkeit und Integrität verlässlich bereitgestellt wird. In der o. g. technischen Einsatzumgebung könnte der EVG folgende Ziele verfolgen:

Z1: Teilnehmer aus dem Internet können nur solche Verbindungen zum zu schützenden Computernetz aufnehmen, die durch den EVG vermittelt werden.

Z2: Teilnehmer erhalten bei Vermittlung durch den EVG nur Kenntnis solcher Informationen, die über sichere Internet-Dienste zur Verfügung gestellt werden.

Z3: Alle vom EVG vermittelten Verbindungen werden nachgewiesen.

Z4: Der EVG schützt sich selbst vor unbefugter Änderung.

Der EVG wehrt damit folgende Bedrohungen ab:

B1: Subjekte S2 greifen vermittels der Zugriffsart A2 auf sensitive Daten D1, D2, D3 oder D5 zu, wodurch die Sicherheit entweder direkt oder indirekt verletzt wird.

B2: Subjekte S1, die nicht ein Subjekt S3 sind, greifen vermittels A2 auf Daten D1, D2 oder D3 zu.

B3: Ein Subjekt S4 greift vermittels A2 auf Daten D1, D2, D3, D4 oder D5 zu. Die Protokollierung der Aktionen von S4 ist keine Bedrohung!

B4: Subjekte S1 oder S2, die nicht Subjekte S3 und nicht Subjekte S4 sind, greifen vermittels A1 auf Daten D1, D2 oder D3 zu.

B5: Subjekte S2 führen Daten D2 aus (A3).

Es fällt auf, dass kein Kriterium für die Unterscheidung zwischen authentifizierten und nicht authentifizierten Teilnehmern genannt wird. Der Grund ist, dass erst zukünftige Internet-Dienste und einige wenige Implementationen verfügbarer Internet-Dienste eine Authentifizierung von Personen ermöglichen (werden). Ferner kann diese Unterscheidung auch ein mehrstufiger Prozess sein, weshalb ein Internet-Teilnehmer sowohl als Subjekt S1 wie auch als Subjekt S2 auftreten kann. Es können weitere Sicherheitsziele und abgewehrte Bedrohungen genannt werden.

12.3.5 Beschreibung der Sicherheitsfunktionen

Der EVG bietet Sicherheitsfunktionen in unterschiedlicher Zahl und Ausprägung, um den genannten Bedrohungen entgegenzuwirken. Die gängigen Sicherheitsfunktionen in der ITSEC-Bezeichnungsweise sind[17]: Identifizierung und Authentifizierung, Zugriffskontrolle, Beweissicherung, Protokollauswertung, Wiederaufbereitung, Unverfälschtheit, Zuverlässigkeit der Dienstleistung und Übertragungssicherung.

Ein EVG *kann* solche Sicherheitsfunktionen beinhalten. Im Falle einer Firewall werden in Übereinstimmung mit den o. g. Sicherheitszielen und Bedrohungen folgende Sicherheitsfunktionen bereitgestellt:

Identifizierung und Authentifizierung:

SF1: Internet-Teilnehmer werden durch Auswertung der Internet-Quellenadresse identifiziert.

SF2: Internet-Teilnehmer werden durch Auswertung des gewünschten Internet-Dienstes identifiziert.

SF3: System-Verwalter und Revisor werden identifiziert und authentifiziert.

SF4: Identifizierte (im Sinne von SF1 und SF2) Internet-Teilnehmer können authentifiziert werden.

Zugriffskontrolle:

SF5: Der Zugriffskontrolle unterliegen alle Objekte D1 und D2.

[17] Die Liste ist keine vollständige Aufzählung sondern beschreibt eher typische Sicherheitsfunktionen.

Beweissicherung:

SF6: Die Beweissicherung erfolgt durch Protokollierung, wobei Art und Umfang der protokollierten Daten von folgenden Kriterien abhängen:

- versuchter Verbindungsaufbau gescheitert;
- versuchter Verbindungsaufbau erfolgreich durchgeführt;
- gewünschter Internet-Dienst;
- IT-Komponente, in der die SF6 (ggf. in Teilen) implementiert ist.

SF7: Aktionen der Subjekte S3 und S4 werden protokolliert, wobei Login (einschließlich des Versuchs) und anschließend mindestens alle Zugriffe A3 dieser Subjekte protokolliert werden.

Protokollauswertung:

SF8: Die während der Beweissicherung anfallenden Informationen können ausgewertet werden. Es gibt protokollierbare Ereignisse, deren Eintreffen zwangsweise weitere Ereignisse auslöst (z.B. nicht unterdrückbares Einblenden einer Nachricht für ein Subjekt S3 an der Konsole).

Wiederaufbereitung:

Obwohl die Bereitstellung einer Wiederaufbereitung für spezielle Objekte (z.B. Arbeitsspeicher, Plattenbereiche, aber auch Bildschirme) als sehr vorteilhaft anzusehen ist, wird eine Sicherheitsfunktion hierzu nicht vorgeschrieben.

Unverfälschtheit:

SF9: Alle Objekte D1 werden vor Verfälschung durch Manipulation geschützt. Der schreibende Zugriff A2 von Subjekten S1 auf diese ist keine Manipulation.

Zuverlässigkeit der Dienstleistung:

SF10: Es gibt Ereignisse, deren Eintreffen zur Abweisung aller weiteren Verbindungsversuche führt. Dieser Zustand kann nur durch Aktionen eines Subjekts S3 oder S4 verändert (verlassen) werden.

Übertragungssicherung:

Zur Übertragungssicherung werden alle Möglichkeiten genutzt, die in den Kommunikationsprotokollen verankert sind. Weitere Anforderungen bestehen nur in solchen Fällen, wo eine Authentifizierung als Komponente eines Internet-Dienstes gegeben ist.

12.3.6 Beschreibung der Mechanismen der Sicherheitsfunktionen

Sicherheitsfunktionen werden realisiert durch bestimmte technische Prinzipien (z.B. redundante Hardwareauslegung) und mathematische Algorithmen (z.B. mathematische Signaturverfahren). Im Bedarfsfall können solche Mechanismen Bestandteil der Sicherheitsvorgaben[18] sein. Hierauf soll jedoch in diesen (generischen) Vorgaben nicht eingegangen werden.

12.3.7 Evaluierungsstufe und Mechanismenstärke

Eine Firewall erfüllt eine für das zu schützende, interne Computernetz lebenswichtige Aufgabe. Der Anwender vertraut der von ihr ausgehenden Schutzwirkung in hohem Maße. Daher sollte eine Firewall mindestens nach der Evaluationsstufe E3 der ITSEC geprüft werden. Die in ihr zur Anwendung gelangenden Sicherheitsmechanismen sollten mindestens die Stärke „hoch“ aufweisen.

12.4 Sicherheitsvorgaben für die Zertifizierung von Chipkartenlesern

Bei der Umsetzung einer Sicherheitspolitik kommen vielfach Chipkartenlösungen in Betracht, da nach dem heutigen Stand der Technik, hier im Sinne von SmartCards[19], ein hohes Sicherheitsniveau realisiert werden kann.

Dabei ist jedoch nicht nur die Chipkarte selbst zu betrachten; auch Kartenleser und Applikationsprogramme auf einem Hostrechner, der über den Kartenleser mit der Chipkarte verbunden ist, sind sicherheitsrelevant. Nur gemeinsam können diese Komponenten die Sicherheitspolitik realisieren.

Der Kartenherausgeber legt die Sicherheitskriterien im Kontext der geplanten Anwendungen fest. Die Anforderungen an die einzelnen Komponenten sind abhängig vom Bedrohungspotential und den möglichen Manipulationen im konkreten Einsatzumfeld.

Typische Szenarien, in denen Chipkartenapplikationen von Bedeutung sind, können u.a. die Unterstützung einer sicheren Übertragung von Daten über ein Netz sein, die Benutzerauthentifizierung, die Zugriffskontrolle auf gespeicherte Daten oder Geldbörsentransaktionen. Solche Anwendungen können parallel auf **einer** SmartCard vorhanden sein.

[18] Eine Regulierungsbehörde könnte z.B. fordern, dass bestimmte Signatur-Mechanismen verwendet werden. Dies ist aktuell etwa im IuK-Dienstleistungsgesetz vorgesehen.

[19] Als SmartCards werden Chipkarten mit eingebettetem Mikroprozessor und ggf. einem Coprozessor verstanden. Alle Interaktionen mit der Karte werden von einem darauf befindlichen Betriebssystem kontrolliert.

12.4.1 Eine Einführung in die Technik der Kartenterminals

Der Chipkartenleser, auch (Karten-)Terminal genannt, ist ein technisches Gerät, um Daten von einer Chipkarte zu lesen oder auf sie zu schreiben und gegebenenfalls eine Verbindung zu einem Host herzustellen. Als Terminal wird nicht nur die Kontaktiereinheit (physische Verbindung zur Chipkarte) mit der unmittelbar dahinter liegenden Schaltlogik gesehen, sondern auch das im Terminal integrierte Anwendungsprogramm. Die Funktionsweise der Chipkartenlesegeräte ist je nach Anwendung, Art des Einsatzes und der informationstechnischen Sicherheitsleistungen, die die Geräte erbringen sollen, sehr vielfältig. Ein einheitliches Anforderungsprofil hinsichtlich der Sicherheitsleistungen von Terminals kann daher nicht aufgestellt werden.

Die Terminals, die heute in den Anwendungsbereichen zum Einsatz kommen, können in zwei Grundversionen eingeteilt werden:

- Stand-alone-Terminal:
  Es gibt Terminals, die ohne weitere IT-Anbindung (z.B. Anschluss an einen PC) auskommen, z.B. bei Zugangskontrollen in Gebäuden.
- Terminal in Verbindung mit einem Host:
  Hier unterschiedet man zwischen Online- und Offline-Terminals. Die Online-Terminals dienen oft nur als Koppler zwischen Chipkarte und Host. Die Kommunikation wird direkt zwischen dem Host und der Chipkarte durchgeführt. Die Sicherheitsleistungen werden vom Host und der Chipkarte erbracht, das Terminal hat nur eine durchreichende Wirkung.

  Bei offline-geschalteten Terminals übernimmt das Terminal selbst eine Vielzahl von Funktionen und Sicherheitsleistungen. Zunächst besteht nur eine Kommunikation zwischen Chipkarte und Terminal. Später werden Daten mit dem Host ausgetauscht. Diese Terminals sind aufwendiger in ihrer technischen Ausstattung, besitzen einen eigenen Prozessor und können komplexe Sicherheitsfunktionen zur Verfügung stellen.

Das multifunktionale Kartenterminal

Ein Gerätetyp, der in zunehmendem Maße Anwendung findet, ist das multifunktionale Terminal. Es kann die verschiedensten Gerätetypen mit vielfältigen Funktionen und Anwendungen gleichermaßen bedienen.

Beispiele für Anwendungsbereiche:

- Digitale Signatur: Das Terminal hat die Funktion der Signierung und kann online oder offline zum Host geschaltet sein.
- Elektronische Geldbörse: Das Terminal (Händlergerät/Bankgerät) hat die Funktion, Wert-Beträge von der Chipkarte abzubuchen oder aufzubuchen, und kann online oder offline zum Host geschaltet sein.
- Chipkarte im Gesundheitswesen: Die Chipkarte als Versicherungsnachweis für die Mitglieder der gesetzlichen Krankenkassen (reine Speicherchipkarte) ist bereits seit

Januar 1995 im Einsatz. In verschiedenen Projekten wird bereits die SmartCard als Patientenchipkarte getestet. Weitere Anwendungen, die in Feldversuchen zur Zeit entwickelt werden, sind die DiabCard, ApothekerCard, NotfallCard usw.

- Chipkarte als Zugangskontrolle.
- Chipkarte als sicherer Schlüsselspeicher (im Rahmen von Verschlüsselungen), ggf. mit kryptographischen Coprozessoren zur symmetrischen/asymmetrischen Verschlüsselung.

Das folgende Beispiel kann als Grundlage und Leitfaden für die Erstellung von Sicherheitsvorgaben im Sinne der /ITSEC91/ dienen. Wegen der geringen Komplexität wurden die Vorgaben für portable Lesegeräte im Krankenversicherungsbereich ausgewählt.

12.4.2 Festlegung des Evaluierungsgegenstandes

Das portable Terminal ist ein Gerät ausschließlich zum Lesen und Speichern von Versichertendaten der Krankenversichertenkarten (KVK) der Krankenkassen in Deutschland. Das Terminal ist für den Einsatz bei Hausbesuchen und in Arztpraxen konzipiert. Der Funktionsumfang des Gerätes richtet sich nach der technischen Spezifikation der Kassenärztlichen Bundesvereinigung (KBV).

Der Evaluierungsgegenstand (EVG) besteht aus den Hardwarekomponenten und der Software, die als Firmware im EEPROM abgelegt wird.

12.4.3 Angenommene Einsatzumgebung und Definition der Objekte, Subjekte und Zugriffsarten

technische Einsatzumgebung:

Der EVG kann beim Einlesen der Versichertendaten stand-alone betrieben werden *(Speichermodus)*. Im *Direktmodus* können die Versichertendaten bei gesteckter Versichertenkarte unmittelbar an einen angeschlossenen PC oder Drucker übertragen werden. Dazu sind ein PC mit einer entsprechenden Applikationssoftware, die das T=1-Protokoll und den Befehlssatz der KBV-Spezifikation unterstützt, und ein Drucker erforderlich.

administrative Einsatzumgebung:

Es gibt keine besonderen Anforderungen hinsichtlich der administrativen Einsatzumgebung.

Definition der Objekte, Subjekte und Zugriffsarten:

Subjekte sind autorisierte und nicht-autorisierte Benutzer.

Objekte sind die Daten der Versichertenkarten im Datenspeicher des Terminals.

Zugriffsarten sind das Auslesen und das Löschen von Daten im Datenspeicher des Terminals.

12.4.4 Sicherheitsziele und Bedrohungen

Die grundsätzlichen **Sicherheitsziele** sind:

1. Der Datensatz einer gültigen Versichertenkarte soll unverfälscht von der Versichertenkarte zum Terminal übertragen werden **(Wahrung der Integrität).**
2. Der im Terminal zwischengespeicherte Datensatz darf durch unbefugte Benutzer nicht ausgelesen werden können. Eine Änderung des Datensatzes darf keinesfalls möglich sein **(Wahrung der Integrität und der Vertraulichkeit).**
3. Die im Terminal zwischengespeicherten Daten sollen unverfälscht an den PC übertragen werden **(Wahrung der Integrität).**

In stärkerer Differenzierung:

- Das portable Terminal soll nur gültige, d.h. mit der KBV-Spezifikation konforme Versichertenkarten auslesen und deren Daten speichern.
- Ungültige, d.h. nicht zur KBV-Spezifikation konforme Versichertenkarten sollen vom Terminal für den Anwender sichtbar abgewiesen werden.
- Eine fehlerhafte Übertragung der Daten von der Versichertenkarte zum Terminal und aus dem Terminalspeicher zum angeschlossenen Endgerät soll erkannt werden.
- Die Daten auf der Versichertenkarte sollen durch das Terminal nicht verändert oder gelöscht, die Daten im Terminalspeicher nicht verändert werden können.
- Das Auslesen der Daten aus dem Terminalspeicher soll nur nach erfolgreicher Identifikation und Authentifizierung und mit den in der KBV-Spezifikation aufgeführten Kommandos (über die normalen Schnittstellen) möglich sein.
- Die Daten sollen nach erfolgreicher Übertragung im Terminal gelöscht werden.
- Die im Terminal gespeicherten Daten sollen vor unbefugtem Lesen und/oder Löschen geschützt werden.

Angenommene Bedrohungen:

B1: Verwendung von Krankenversichertenkarten, die nicht der technischen Spezifikation entsprechen, ohne dass diese durch das Terminal abgewiesen werden.

B2: Fehlerhafte Übertragung der Daten von der Versichertenkarte zum Terminal, ohne dass dies erkannt und die Versichertenkarte durch das Terminal abgewiesen wird.

B3: Veränderung von Daten auf der Versichertenkarte während des Verbleibs der Versichertenkarte im Terminal.

B4: Veränderung von Daten im Terminalspeicher durch Zugang über die Schnittstellen oder durch fehlerhafte Bedienung des Terminals.

B5: Fehlerhafte Übertragung der Versichertendaten vom Terminal zum PC, ohne dass dies erkannt und der Vorgang abgebrochen wird.

B6: Unbefugtes Auslesen aus dem Terminal oder Manipulation von Versichertendaten über Schnittstellen, die nicht in der technischen Spezifikation vorgesehen sind.

B7: Unbefugtes Sichtbarmachen oder Abrufen der im Terminalspeicher abgelegten Krankenversichertendaten.

B8: Unbefugtes Sichtbarmachen oder Abrufen von bereits übertragenen Krankenversichertendaten bei Verlust des Terminals und der dazugehörenden Arztkarte.

12.4.5 Sicherheitsfunktionen

SF1: Die eingelesenen Versichertendaten werden durch das Terminal auf Konformität mit der technischen Spezifikation geprüft. Ungültige Versichertenkarten werden abgewiesen, es erfolgt keine Weiterverarbeitung der Daten. Eine Fehlermeldung wird angezeigt.

SF2: Es wird durch ein Prüfsummenverfahren sichergestellt, dass eine Verfälschung der Daten bei der Übertragung von der Versichertenkarte zum Terminal erkannt und die Versichertenkarte abgewiesen wird.

SF3: Nach erfolgreicher Übertragung der Versichertendaten aus dem Terminalspeicher zum PC oder Drucker wird der interne Speicherbereich im Terminal automatisch oder per Tastendruck wiederaufbereitet.

SF4: Bei der Übertragung der im Terminal gespeicherten Versichertendaten zum PC wird durch ein Prüfsummenverfahren eine Verfälschung der Daten erkannt und die Übertragung abgebrochen.

SF5: Fehlerhafte oder ungültige Kommandos, die über externe und interne Schnittstellen übermittelt werden, werden erkannt und abgewiesen.

SF6: Das Auslesen der im Terminal gespeicherten Daten über die angegebenen Schnittstellen oder das Display erfolgt nur nach erfolgreicher Identifizierung und Authentifizierung des Bedieners durch die Arztkarte.

12.4.6 Technische Sicherheitsmaßnahmen

Die an dieser Stelle geforderte Beschreibung der Sicherheitsmechanismen soll hier nicht ausgeführt werden.

Stattdessen werden einige weitere Sicherheitsmaßnahmen genannt, die zwar keine Sicherheitsfunktionen im Sinne der ITSEC sind, hier aber in Bezug auf die Bedrohungen als solche behandelt werden.

SM1: Es sind nur die Schnittstellen vorhanden, die in der technischen Spezifikation angegeben sind.

SM2: Das portable Terminal enthält keine Funktionen zum Beschreiben der (im Terminal steckenden) Versichertenkarte.

SM3: Eine Möglichkeit zum Beschreiben des Terminalspeichers durch externen Programmaufruf oder durch die äußeren Bedienelemente oder Schnittstellen ist nicht vorhanden.

12.4.7 Evaluierungsstufe und Mechanismenstärke

Die angestrebte Evaluierungsstufe ist E2; die Mindeststärke der Mechanismen „niedrig“. Für die Sicherheitsfunktion SF6 ‘Identifizierung und Authentifizierung’ gibt der Antragsteller die Mechanismenstärke „mittel“ an.

12.5 Erfahrungsbericht aus der bisherigen Zertifizierung von Chipkarten

12.5.1 Kurze Einführung in die Chipkartentechnologie

In den verschiedenen Anwendungsbereichen kommen unterschiedliche Chipkartentypen zum Einsatz.

- **Speicherchipkarte:** Es handelt sich hier um eine reine Speicherchipkarte, die im Kommunikationsprozess nicht aktiv wird. Es können Daten auf die Karte geschrieben und von der Karte gelesen werden. Je nach Ausstattung der Karte können Schreib- und Leseschutzfunktionen genutzt werden.
- **SmartCard oder Prozessorchipkarte:** Dieser Kartentyp ist mit einem Mikroprozessor ausgestattet. Neben einer reinen Speicherfunktion können auch eigene Prozesse von der Chipkarte ausgeführt werden. In den Kommunikationsprozess kann die Chipkarte aktiv eingreifen. Es können Sicherheitsfunktionen mit hohem Schutzwert implementiert und genutzt werden.

Eine SmartCard kann unter Kontrolle ihres Betriebssystems als sicherer Datenspeicher (Vertraulichkeit und Integrität) angesehen werden. Objekte sind die auf der Karte vorhandenen Dateien: personenbezogene Applikationsdaten, Transaktions- und Valutadaten einer elektronischen Geldbörse oder geheime Schlüssel oder PINs für die Authentifizierung.

Als Subjekte im Lebenszyklus der Karte werden der Anwendungsanbieter, der Anwendungsadministrator, der Kartenhalter und der Außenstehende unterschieden. Die Rollenunterscheidung der Subjekte erfolgt implizit durch das Wissen einer Authentifizierungsinformation (PIN oder Schlüssel). Dabei übernimmt das Terminal die Mittlerfunktion zur Karte. Es kann sich auch selbst gegenüber der Karte authentifizieren.

12.5.2 Sicherheitsziele des Chipkartenbetriebssystems

Als Zugriffe auf die Objekte werden das Erzeugen von Dateien oder Verzeichnissen, das Lesen, Schreiben und Löschen von Daten oder Parametern und PIN-Änderungen unterschieden. Für elektronische Geldbörsen gibt es weitere Zugriffsmöglichkeiten z.B. zum Auf- und Abbuchen.

Zur Unterstützung einer vertraulichen und authentischen Datenübertragung zwischen einzelnen Systemkomponenten, z.B. eines Krankenhausnetzes, können Chipkarten einer Hostapplikation bestimmte Dienstleistungen zur Verfügung stellen, die auf der Karte in einer sicheren Betriebsumgebung ablaufen. Dazu zählen beispielsweise das Erzeugen und Verschlüsseln von Sitzungsschlüsseln für eine Datenverschlüsselung und das Erzeugen und Verifizieren digitaler Signaturen.

Die nicht autorisierte Nutzung dieser Dienstleistungen sowie nicht autorisierte Zugriffe auf die Objekte müssen durch die Sicherheitsfunktionalität der Chipkarte verhindert werden. Außenstehende dürfen keine Daten lesen oder modifizieren, für die sie keine expliziten Rechte besitzen. Ebenso sollten die Kenntnisnahme und mögliche Manipulationen wichtiger Daten auf dem Weg über die Kommandoschnittstelle zum Betriebssystem der Karte abgewehrt werden können.

12.5.3 Typische Sicherheitsfunktionen einer Chipkarte und Voraussetzungen für ihre Wirksamkeit

Auf einer Chipkarte werden typischerweise folgende Sicherheitsfunktionen realisiert:

- die Authentifizierung von Benutzer und Terminal gegenüber der Karte, meist bezogen auf bestimmte Dateien oder Dateistrukturen,
- die Zugriffskontrolle auf Dateien auf der Karte,
- die Übertragungssicherung von Kommandos, Daten und Meldungen zwischen Chipkarte, Kartenleser und Host und
- die Wiederaufbereitung von Speicherplatz.

Dabei kann unterschieden werden zwischen den Sicherheitseigenschaften des Betriebssystems und denen der Hardwareplattform der Karte.

Die Hardwareplattform muss im Kontext möglicher Bedrohungen über ausreichende, dem Stand der Technik entsprechende Sicherheitsmechanismen verfügen. Im Einzelnen wären beispielsweise möglich: Sensoren, Passivierungsschichten, Fuses, Busscrambling, verdeckte Speicher sowie Fehlererkennungs- und Fehlerkorrekturmechanismen.

Das Betriebssystem muss derart aufgebaut sein, dass es ab dem Zeitpunkt der Übergabe der Karte vom Kartenherausgeber (Supplier) an den Anwendungsanbieter nicht manipuliert werden kann und sich nicht selbst verändern oder neu laden kann. Die Kartenvorbereitungsphase darf nur einmal durchlaufen werden können.

Außerdem muss gewährleistet sein, dass die Sicherheitsfunktionen nicht durch andere Funktionen des Betriebssystems umgangen werden können. Trace- bzw. Debug-Funktionen dürfen nicht enthalten sein. Bei allen Interaktionen zwischen Chipkarte und Terminal oder Host reagiert das Betriebssystem der Karte jeweils nur auf ein Kommando, das von außen über die einzige Schnittstelle an es herangetragen wird. Das Betriebssystem speichert Informationen über den Authentifizierungszustand, der im Betrieb aktuell gültig ist. Werden bei einem Zugriff die Zugriffs- oder Authentifizierungsbedingungen nicht erfüllt, so reagiert die Karte mit einer Abweisung des Kommandos in Form einer Fehlermeldung.

Bezogen auf die o.g. Subjekte wird meist ein hierarchisches Zugriffskonzept realisiert, das dem Anwendungsanbieter die umfassendsten Rechte und dem Außenstehenden die geringsten Rechte zubilligt. Realisierbar sind diese Anforderungen beispielsweise durch einen objektorientierten Ansatz für die Dateistruktur. Bei diesem Ansatz werden auf Datei- bzw. Verzeichnisebene die jeweilige Forderung nach einer bestimmten Authentifizierung und die für den Dateizugriff eingestellten Rechte abgelegt und vom Betriebssystem vor dem jeweiligen Zugriff geprüft.

Anforderungen an die Programmierung einer Chipkartenapplikation

Der Programmierer einer Applikation ist für die korrekte Interaktion mit der Karte verantwortlich. Ebenso hängt auch die Verwendung der Sicherheitsfunktionen selbst wie z.B. die Forderung nach einer bestimmten Form der Authentifizierung und die Festlegung bestimmter Zugriffsrechte für eine Datei auf der Karte von der Initialisierung der Datenstruktur auf der Karte ab, da beim Erzeugen einer Datei die für den Zugriff notwendige Authentifizierung und die Zugriffsrechte definiert werden müssen. Die Regeln, die hierbei durch einen Anwendungsprogrammierer zu beachten sind, müssen vom Kartenherausgeber präzise dokumentiert sein. In der Anwendungsphase ist die Hostapplikation bzw. der agierende Benutzer dann gezwungen, die eingestellten Anforderungen an die Authentifizierung und Zugriffskontrolle zu erfüllen, um auf eine bestimmte Datei zugreifen zu können.

Ergänzung der Sicherheitsleistung durch die Hostapplikation

Wird die Abwehr von Bedrohungen wie beispielsweise der Kenntnisnahme oder Manipulation von übertragenen Daten in einem lokalen Netz oder der Vortäuschung falscher Identitäten gefordert, so kann die Hostapplikation Daten und Dienstleistungen der Chipkarte nutzen, um eine bestimmte Sicherheitsleistung im System zu erbringen.

Die Chipkarte bietet der Hostapplikation dazu Verschlüsselungs- und Signaturfunktionen an oder wird als sicherer Datenspeicher für Authentifizierungs-, Schlüssel- und Anwendungsdaten verwendet. Die Hostapplikation selbst bzw. deren Programmierer bestimmt, wie die vorgegebene Sicherheitspolitik unter Verwendung der Sicherheitsfunktionen der Karte umgesetzt wird.

12.6 Revisionssicherheit von Betriebssystemen und Anwendungen

Bei der Revision geht es um die Fragestellung, anhand geeigneter Aufzeichnungen (Protokolle) erfolgte Transaktionen nachträglich nachvollziehen zu können. Ziel ist es,

- die Ordnungsmäßigkeit der Transaktionen belegen zu können,
- qualitätsmindernde Faktoren erkennen zu können und auszumerzen,
- sicherheitsrelevante Ereignisse zu analysieren und zukünftig verhindern zu können.

Um diese Ziele erreichen zu können, ist es erforderlich, dass die Aufzeichnungen

1. alle relevanten Ereignisse und Vorgänge erfassen,
2. einen angemessenen Detaillierungsgrad haben,
3. prinzipiell Beweiskraft besitzen, d.h. lückenlos, untäuschbar und nicht-manipulierbar sind[20] und
4. in vernünftiger Zeit mit akzeptablen Werkzeugen ausgewertet werden können.

Die unter 3. aufgeführte Eigenschaft „lückenlos“ meint, dass es keine für die Revision relevanten Aktionen gibt, die von der Protokollierung nicht erfasst werden; „untäuschbar“ bezeichnet die Eigenschaft, dass die aufgezeichneten Aktionen tatsächlich stattgefunden haben und definitiv den betreffenden Personen zugeordnet werden können. Letzteres setzt voraus, dass Personen ausreichend sicher identifiziert und authentifiziert wurden. „Nicht-manipulierbar“ ist die Protokollierung dann, wenn sie nicht unbefugt temporär abgeschaltet, die Ereignisfilter nicht während der Aufzeichnung unbefugt geändert und insgesamt die Aufzeichnung nicht nachträglich verändert oder gelöscht werden kann.

In der IT-Praxis trifft man zwei grundsätzliche Aufzeichnungsebenen an:

- Protokolle der zugrunde liegenden Betriebssysteme: Die Aufzeichnungen beinhalten Vorgänge wie das An- und Abmelden von Benutzern, den Zugriff auf Datenobjekte und andere Ressourcen (z.B. Übertragungsdienstleistungen).
- Protokolle der Anwendungen: Anfang / Ende der Nutzung der Anwendung durch einen Benutzer; Zugriff zu den der Anwendung unterstehenden Datenstrukturen, aber auch z.B. die betriebsbedingt notwendige Transaktionssicherung bei Datenbanken.

Je nach Art des Betriebssystems bzw. der Anwendung kann ein Systemverwalter oder auch ein spezieller Accounting-Manager oder Audit-Verwalter dabei einstellen, welche Ereignisse mit welchen Daten aufgezeichnet und für welche Benutzer und für welche Zeiträume Protokolle erzeugt werden sollen. Damit kann zumeist den o.g. Forderungen 1 und 2 genüge getan werden.

Ob und bis zu welchem Grad der Forderung 3 entsprochen werden kann, hängt von dem konkreten Betriebssystem bzw. der konkreten Anwendung ab. Dabei ist diese Forderung

[20] Die Frage der Rechtsgültigkeit bzw. der gerichtlichen Verwertbarkeit wie auch das Problem der datenschutzrechtlichen / arbeitsrechtlichen Zulässigkeit solcher Aufzeichnungen sollen hier nicht diskutiert werden.

kaum durch den Nutzer selbst verifizierbar. Er muss sich hier vielmehr auf die Aussagen des Herstellers bzw. neutraler Gutachter stützen. Deshalb ist es sinnvoll, dort, wo Revisionssicherheit verlangt wird, Systeme und Anwendungen zu nutzen, die zumindest zertifizierte Protokoll- bzw. Audit-Komponenten besitzen.

Revisionssicherheit setzt weiterhin voraus (Forderung 4), dass man prinzipiell und praktisch in der Lage ist, die Aufzeichnungen auswerten zu können. Die normale Praxis ist aber eher, dass die Protokolle wegen ihres Umfangs nicht ausgewertet werden oder sogar die Protokollierung abgeschaltet wird, letzteres oft auch aus Performance-Gründen. Um diesen Mängeln abzuhelfen, ist es erforderlich, von vornherein die Protokollfilter so detailliert wie nötig aber so grob wie möglich einzustellen.

Um sich vor einer provozierten Überlastung des Aufzeichnungssystems (neben dem Erschleichen ausreichend hoher Privilegien für das Abschalten oder nachträgliche Abändern der Aufzeichnungen eine weitere klassische Manipulationsmethode) zu schützen, sind organisatorisch-technische Maßnahmen zu treffen, die einen undefinierten Systemzustand — z.B. durch Überlauf des Protokollspeichers — vermeiden.

Da die Aufzeichnungen z.T. längerfristig aufbewahrt werden müssen, sind außerdem Fragen der Auslagerung auf geeignete Datenträger, deren Aufbewahrung und ggf. Vernichtung bzw. Wiederaufbereitung zu klären.

Anbieter von Betriebssystemen und Anwendungen haben teilweise für ihre Produkte nach eingehender Prüfung Sicherheitszertifikate bekommen, denen entnommen werden kann, ob und inwieweit die Forderungen 1–4 erfüllt sind.

12.7 Empfehlungen zur Zertifizierung von Sicherheitslösungen

- **Prototypisches Vorgehen für den Erhalt eines zertifizierten Produkts**

  Im Kontext der Hochschulverwaltungen und Universitätskliniken und des Schutzes ihrer Netze und Systeme vor missbräuchlicher Nutzung wird empfohlen, die zuvor skizzierte Dienstleistung der Sicherheitszertifizierung für einige ausgewählte Sicherheitskomponenten (Firewalls, SmartCards, Betriebssysteme) in Anspruch zu nehmen bzw. bei der Auswahl und Beschaffung zertifizierten Komponenten den Vorzug zu geben. Dies folgt dem allgemein anerkannten Leitsatz, dass Sicherheit immer **geprüfte Sicherheit** ist.

  In noch festzulegenden Pilotfällen könnte das nachfolgend skizzierte Schema angewendet werden. Nachdem entsprechende Anwendungserfahrungen vorliegen, sollte es für vergleichbare Situationen — je nach Sensibilität — als Empfehlung oder als Richtlinie zur Anwendung kommen:

  1. In enger Abstimmung mit dem Betreiber von IT-Ressourcen wird ein detailliertes technisches Sicherheitskonzept entwickelt, in dem das Sicherheitsziel (hier: die

Verhinderung missbräuchlicher Nutzung), die konkreten Einzelbedrohungen, die vorhandenen / noch einzurichtenden Maßnahmen und das angestrebte Sicherheitsniveau festgehalten werden.

2. Soweit in diesem Konzept beispielsweise Firewalls auftauchen, werden die technischen Anforderungen an solche Firewalls soweit präzisiert, dass sie bei einer Ausschreibung / Beschaffung entsprechender Geräte zugrunde gelegt werden können. Das gleiche gilt sinngemäß für andere, sicherheitsrelevante Komponenten im Gesamtsystem.
3. Unter Nutzung der Resultate aus 1. und 2. wird eine Systemzertifizierung durchgeführt.
4. Soweit die Zertifizierungsverfahren im Ergebnis bestimmte Hinweise und Auflagen für die sicherheitsgerechte Anwendung von IT-Ressourcen geben, sind diese durch die einzelnen Betreiber in der Praxis zukünftig zu berücksichtigen.
5. Als Ergebnis der Zertifizierungsverfahren werden Revisionsverfahren definiert, durch die die **Aufrechterhaltung der Sicherheit** vor missbräuchlicher Nutzung im laufenden Betrieb auch nach Änderungen der technischen Einstellungen gewährleistet werden kann.

Durch die zuvor beschriebene Vorgehensweise kann den konkreten Sicherheitsbedürfnissen nach dem Stand der Technik Rechnung getragen werden.

Für die Durchführung dieser Verfahren sind dabei folgende Aufwände erforderlich:

- Soweit kommerzielle Produkte eingesetzt werden sollen, die bereits als solche zertifiziert wurden[21], kann auf diese Ergebnisse zurückgegriffen werden, so dass hierfür keine Kosten anfallen.
- Soweit dies nicht der Fall ist, kann den Anbietern im Rahmen von Beschaffungen eine (Produkt-)Zertifizierung aufgegeben werden. Die Kosten hierfür sind zunächst durch den Anbieter zu tragen; ein Durchschlagen der Kosten auf die konkrete Beschaffung ist aller Erfahrung nach nicht oder nur in sehr untergeordnetem Maße zu erwarten[22].
- Die Systemzertifizierung dagegen ist kostenmäßig durch den Betreiber der IT-Ressourcen zu tragen. Mit der vorgeschlagenen pilothaften Vorgehensweise wird dies jedoch nur für einige wenige typische Einsatzfälle durchzuführen sein; alle anderen Installationen können auf diese Ergebnisse als Referenzfall zurückgreifen. Unter den geschilderten Prämissen sind für einen Pilotfall externe Ressourcen in der Größenordnung weniger Personenmonate (bis zu max. 3) erfor-

[21] Listen solcher zertifizierter Produkte sind bei den staatlichen Zertifizierungsstellen erhältlich /BSI97/, für Deutschland: BSI, Postfach 20 03 63, 53133 Bonn. Das BSI bietet auch einen Auskunftsdienst bezüglich der Produkte, die durch entsprechende Stellen anderer Staaten zertifiziert wurden.

[22] Die Gründe hierfür sind, dass das Zertifizierungsergebnis für ein Produkt des Anbieters von diesem in anderen Beschaffungen (auch im internationalen Umfeld) vorgelegt werden kann bzw. generell als Qualitätsnachweis gilt, die Kosten andererseits erfahrungsgemäß max. 5 % der Entwicklungskosten für das Produkt ausmachen. Bisher ist deshalb kein Produkt durch die Sicherheitszertifizierung nennenswert verteuert worden.

derlich. Notwendige interne Ressourcen eines Betreibers sind pro Verfahren auf weniger als ein Personenmonat beschränkt.

- **Sicherheitsprüfungen/-zertifizierungen unter Verwendung von Chipkarten**

  Um ein vertrauenswürdiges IT-System unter Verwendung von Chipkarten zu erhalten, sollte bei der Erstellung des System-Sicherheitskonzepts beachtet werden, dass die Anforderungen an die Funktionalität und an die Prüfung (E-Stufe, Mindeststärke der Sicherheitsmechanismen) entsprechend dem Schutzbedarf oder der rechtlichen Anforderungen (u.a. BDSG) festgelegt werden.

  Anwendungsszenarien auf der für den Einsatz geplanten Plattform sind genau zu beschreiben. Die System-Sicherheitspolitik ist möglichst präzise zu formulieren und zu dokumentieren. Die Definitionen von im System agierenden Subjekten und Prozessen, den zu schützenden Objekten, den Zugriffsmöglichkeiten und Beschränkungen sowie die Formulierung von Bedrohungen auf Systemebene sollten eine Abbildung auf die einzelnen Produktkomponenten Chipkarte, Kartenleser und Hostapplikation ermöglichen. Danach können die einzelnen Komponenten dahingehend bewertet werden, ob und in welchen Stufen sie zertifiziert werden müssen. In Anbetracht der Sensibilität der Daten und der möglichen Schadensauswirkungen dürften dabei die Stufen E3/E4 mit mindestens mittlerer Mechanismenstärke vorzusehen sein.

12.8 Literatur

/BSIG/ Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz — BSIG)
17. Dezember 1990, Bundesgesetzblatt I 1990 S. 2834

/BSI96/ Bundesamt für Sicherheit in der Informationstechnik:
„Sicherheitsanforderungen an Internet-Firewalls“, 1996

/BSI97/ BSI-Zertifikate:
„Sicherheit von IT-Produkten und -Systemen“,
Druckschrift BSI 7148, jeweils aktuelle Fassung

/CC98/ *„Common Criteria Project“*
`http://csrc.nist.gov/nistpubs/cc/index.html`

/ITSEC91/ *„Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)“,*
Version 1.2, Juni 1991, Bundesanzeiger-Verlag Köln 1991,
ISBN 92-826-3003-X

/ITSEM92/ Commission of the European Communities:
„Information Technology Security Evaluation Manual (ITSEM)“,
Version 1.0, ECSC-EEC-EAEC, Brussels-Luxembourg, 1992/93

/TDI91/ National Computer Security Center:
„Trusted Database Management System Interpretation of the Trusted Computer Security Evaluation Criteria, (Draft)“,
1991

/TNI87/ National Computer Security Center:
„Trusted Network Interpretation of the Trusted Computer Security Evaluation Criteria“,
NCSC-TG-005, Library No. S228,526 (1987)

/UNIX-ES/ Bundesamt für Sicherheit in der Informationstechnik:
„Sicherheitseigenschaften von UNIX *System V Rel. 4 und* UNIX-ES*“,*
Studien des BSI
Oldenbourg Verlag

Glossar

ABR — *Siehe* Available Bit Rate.

Access-Listen — Access Control Lists (ACL). Geben Auskunft, wer Zugriffsrechte für bestimmte Objekte, wie Dateien oder Verzeichnisse, besitzt.

Access-Server — Dedizierter Rechner, der über integrierte analoge oder digitale Schnittstellen den Zugang vom Telefon- zum Hochschulnetz vermittelt.

Account — Nutzungsgenehmigung für einen Rechner oder für einzelne Dienste auf einem Rechner.
Siehe auch Benutzerkennung.

Accounting — Zuordnung von DV-Leistungen (etwa von CPU-Zeit bei Rechnern oder übertragenem Datenvolumen bei Netzen) zu den Verursachern, z.B. zu Abrechnungszwecken.

Accounting-Box — Vom Regionalen Rechenzentrum Erlangen im Rahmen eines DFN-Projekts entwickeltes System zur Netzüberwachung; beschränkt auf X.25-basierte Protokolle.

ActiveX — Unter der Federführung von Microsoft entwickelte Produktfamilie, die es ermöglicht, Programme wie Applets vom Server zu laden und auszuführen. ActiveX ist nicht betriebssystemunabhängig.

Adresse — *Siehe* IP-Adresse.

AFS — *Siehe* Andrew File System.

aFTP — *Siehe* anonymous FTP.

AH — *Siehe* Authentication Header.

AIX — Herstellerabhängiges UNIX-Betriebssystem von IBM.

Andrew File System (AFS) — Dateiverwaltungssystem ähnlich wie NFS. AFS verfügt über zusätzliche Möglichkeiten wie Kerberos-Authentifizierung, lokales Zwischenspeichern von Daten und verfeinerte Zugriffskontrolle auf Dateisysteme.

anonymous FTP (aFTP) Spezielle Form des FTP-Dienstes, der einem Benutzer ohne eigenen Account „anonymen“ Zugang zu entsprechenden FTP-Servern gewährt.

Apache-SSL Sicherer WWW-Server, der auf dem für Hochschulen frei verfügbaren WWW-Server Apache und SSLeay aufsetzt.

API *Siehe* Application Programming Interface.

Application-Gateway Rechnersystem zur Kopplung von Netzen mit Vermittlungsfunktion auf der Anwendungsschicht. Diese Funktion wird i.Allg. durch Proxies erbracht. Wird als Firewallkomponente eingesetzt. *Siehe auch* Proxy, Firewall.

Application Programming Interface (API) Schnittstelle für Anwendungsprogramme, um bereits definierte Routinen einbinden zu können.

Archie Internet-Dienst, mit dem in Datenbanken nach Inhaltsverzeichnissen von anonymous-FTP-Servern recherchiert werden kann.

Archiv-Server Dedizierter Rechner, der – in der Regel in Verbindung mit einem Robotersystem für Magnetbandkassetten – Daten langfristig archiviert.

Asymmetrische Verschlüsselung Kryptographisches Verfahren, welches mit zwei verschiedenen Schlüsseln arbeitet. Jeder Benutzer hat zur Verschlüsselung der an ihn gerichteten Nachrichten einen öffentlichen Schlüssel (Public Key), der allen Kommunikationspartnern bekannt sein muss, und zur Entschlüsselung der Nachrichten einen geheimen Schlüssel (Private Key), der nur ihm selbst bekannt sein darf. Beispiel: PGP.

Asynchronous Transfer Mode (ATM) Verfahren zur Datenübermittlung, das insbesondere auch Sprach- und Bewegtbildübermittlung mit hoher Übertragungsgeschwindigkeit unterstützt.

ATM *Siehe* Asynchronous Transfer Mode.

ATM Forum Internationale Organisation, die das Ziel hat, durch das Definieren von Interoperabilitätskriterien die Verbreitung von ATM zu fördern.

Audit-Dateien Protokolldateien.

Auditing Registrierung der Identität eines Nutzers, der von ihm verbrauchten Ressourcen und der von ihm ausgelösten Aktivitäten.

Authentication Header (AH) Bestandteil von IPv6 zur Authentifizierung und Überprüfung der Datenintegrität.

Authentifizierung auch: Authentisierung, Authentifikation. Mechanismus, mit dem die Identität eines Dienstenutzers bzw. eines Absenders von Daten überprüft wird, im einfachsten Fall anhand von Benutzerkennung und Passwort.
Siehe auch Kryptographische Verfahren.

Available Bit Rate (ABR) ATM-Service-Klasse, die Flusskontrollmechanismen definiert, die eine möglichst hohe Auslastung des Netzes verbunden mit einer möglichst geringen Zellverlustrate zum Ziel haben.

Backbone-Netz Hochschulweites oder überregionales Hochgeschwindigkeitsnetz (meist in FDDI- oder ATM-Technologie), das der Verbindung eigenständiger Teilnetze dient.

Backup
(a) Sammelbezeichnung für Ausweich- und Ersatz-Verfahren bzw. -Ressourcen.
(b) Gesamtheit der gesicherten Dateien.

BASILIKA „Bayerische Sicherheitslösung für Dienstangebote in offenen Kommunikationsnetzen". BayernOnline-Pilotprojekt der Bayerischen Staatsregierung, das einen integrierenden, umfassenden Lösungsansatz für IT-Sicherheit vorstellt.

Bastion Application-Gateway, das als einziges Rechnersystem eines lokalen Netzes vom unsicheren Netz aus angesprochen werden kann.

BayDSG Bayerisches Datenschutzgesetz.

Bayernnetz (BayNet) Datennetz im Rahmen von BayernOnline.

BayernOnline Initiative der Bayerischen Staatsregierung zum Aufbau eines Datenhochgeschwindigkeitsnetzes und zur Förderung neuer Kommunikationstechnologien in Bayern.

BayHSchG Bayerisches Hochschulgesetz.

BayKrG Bayerisches Krankenhausgesetz.

BDSG Bundesdatenschutzgesetz.

Behördennetz (im Rahmen von BayernOnline) Teil des Bayernnetzes, jedoch logisch und physisch vom Hochschulnetz und vom Bürgernetz getrennt.

Benutzerkennung Name, unter dem sich ein Benutzer auf einem Rechner oder im Netz anmeldet. *Siehe auch* Account, Login.

Berechtigungs-Server System zur Verwaltung verschiedenster Berechtigungsobjekte (z.B. Logins, Ressourcen, Zutritt zu Räumen).

Betreiber *Siehe* Systembetreiber.

BHN Bayerisches Hochschulnetz.

Billing Zuordnen der Kosten von DV-Leistungen zum Konto des Verursachers.

bit Binärzeichen, kleinste Informationseinheit.

bit/s Bit pro Sekunde; Maßeinheit für die Übertragungsrate in Datennetzen.
Abgeleitete Einheiten:
1 kbit/s = 1 Kilobit pro Sekunde = 1.024 bit/s
1 Mbit/s = 1 Megabit pro Sekunde = 1.024 kbit/s

BMBF Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie.

Breitband-WiN (B-WiN) Deutschlandweites Hochgeschwindigkeitsnetz für die Wissenschaft, das auf ATM-Übermittlungstechnik basiert und Anschlussraten für Einzel- und Gemeinschaftsanschlüsse von derzeit 34 Mbit/s und 155 Mbit/s bietet.
Siehe Wissenschaftsnetz.

Bridge Gerät zur Kopplung lokaler Netze (auf ISO/OSI-Schicht 2).

Broadcast and Unknown Server (BUS) Zuständig für die Übertragung aller Broad- und Multicasts und des unknown Unicast-Verkehrs innerhalb eines emulierten LANs.
Siehe auch LAN Emulation (LANE).

Broadcast-Paket Paket einer bestimmten Protokollschicht, das allen zugehörigen Stationen zugeteilt wird (Einer-an-Alle-Nachricht); z.B. Medienbroadcast (Schicht 2) wird allen am Medium z.B. Ethernet-Subnetz befindlichen Stationen (auch über Bridges) zugestellt.

Broadcast-Sturm Lawinenartige Ausbreitung von Broadcast-Paketen.

Brute-Force-Attacke Brachialangriff; Versuch, ein System oder eine Verschlüsselung durch Ausprobieren aller Möglichkeiten aufzubrechen.

BSD Berkeley System Derivative. Variante des Betriebssystems UNIX.

BSI Bundesamt für Sicherheit in der Informationstechnik.

Bürgernetz (im Rahmen von BayernOnline) Einwählmöglichkeit in das Bayernnetz für nicht-kommerzielle Zwecke.

BUS *Siehe* Broadcast and Unknown Server.

B-WiN *Siehe* Breitband-WiN.

Byte
Informationseinheit, bestehend aus 8 Bit.
Abgeleitete Einheiten:
1 KB = 1.024 Byte
1 MB = 1.024 Kilobyte
1 GB = 1.024 Megabyte
1 TB = 1.024 Gigabyte

CA
Siehe Certification Authority.

Cache-Server
Dedizierter Rechner zum Zwischenspeichern von Daten (z.B. im WWW).

Caching
Schnelles Zwischenspeichern von Daten.

Campusnetz
Netz, das die verschiedenen Gebäude auf dem Gelände einer Einrichtung/Hochschule verbindet.

CBR
Siehe Constant Bit Rate.

CBT
Siehe Computer Based Training.

CC
Siehe Common Criteria.

CD-ROM
Compact Disk Read Only Memory.
Portable optische Speicherplatte mit einer Aufzeichnungskapazität von etwa 650 Megabyte. Einmal gespeicherte Daten sind nicht überschreibbar.

Cell-Oriented-Switch (CO-Switch)
Ein CO-Switch zerlegt ankommende Pakete in Zellen (48 Bytes) und transportiert sie sofort weiter. Der Einsatz von CO-Switches ist besonders bei ATM-Backbone-Netzen zu empfehlen.

CERT
Computer Emergency Response Team.
Siehe Computer-Notfall-Team, DFN-CERT.

Certification Authority (CA)
Eine CA ist eine vertrauenswürdige Institution, die nach der von der PCA festgelegten Policy zertifiziert ist und auf dieser Basis arbeitet. Ihre Aufgabe ist es, öffentliche Schlüssel zu beglaubigen, d.h. Benutzer zu zertifizieren.

Challenge-Response-Verfahren
Verfahren, bei dem Einmalpasswörter den Zugriff von einem externen System auf einen Server erlauben. Bei jedem Verbindungsaufbau schickt der Server eine Zahl (challenge). Das externe System errechnet mit Hilfe einer Identifikationszahl (PIN) oder eines geheimen Passworts des Benutzers einen Wert, den es an den Server schickt.

Chat-Dienst
Siehe IRC.

Chiffrat
Aus einem Klartext mittels Verschlüsselung gewonnener Datensatz.

Chipkarte Kreditkartengroße Speicherkarte – als intelligente Smart-Card mit Rechnersystem ausgestattet – mit Funktionen im Bereich der Authentifizierung und Autorisierung. Sie kann im DV-Bereich für mehrere Funktionen eingesetzt werden, z.B. Erhöhung der IT-Sicherheit, Einzug von Gebühren, Betriebsdatenerfassung, Zutrittskontrolle, Sicherung des Zugangs zu oder von externen Partnern.

CIP Computer-Investitionsprogramm im Rahmen des HBFG, das die Einrichtung von Pools vernetzter Arbeitsplatzrechner für Studierende zum Ziel hat.

Class A, B, C *Siehe* IP-Adresse.

Classical IP Classical IP over ATM (RFC 1577) definiert, wie ein ATM-Netz als logisches IP-Subnetz in eine geroutete Umgebung eingebunden werden kann. Es erlaubt eine weiche Migration zum ATM-Switching.

Client *Siehe* Client/Server-Modell.

Client/Server-Modell Modell einer Arbeitsteilung zwischen Rechnern, bei welcher bestimmte Rechner (Server) Dienstleistungen, wie beispielsweise Rechenleistung oder Netzdienste, für andere Rechner oder Prozesse (Clients) bereitstellen. Voraussetzung für die Realisierung des Client/Server-Modells ist ein leistungsfähiges Kommunikationsnetz.

Clipper Chip In den USA entwickeltes System zur Key-Escrow-Verschlüsselung von Telefongesprächen.

CN *Siehe* Corporate Network.

Common Criteria (CC) Gemeinsame, auf der Basis der ITSEC und TCSEC erarbeitete Kriterien für die Prüfung und Bewertung der IT-Sicherheit.

Common Object Request Broker Architecture (CORBA) Standard, der die Kommunikation zwischen Objekten und Programmen regelt.

Computer Based Training (CBT) Lehr- und Lernform unter Einsatz des Computers, bei der die Inhalte in elektronischer Form aufbereitet sind.

Computerdelikte Z.B. Computerbetrug, Computermanipulation und Computersabotage. Computerdelikte werden auf eine Anzeige oder einen Strafantrag hin strafrechtlich verfolgt. Bei Schäden muss der Täter zusätzlich mit zivilrechtlichen Regressansprüchen rechnen.

Computer-Notfall-Team Computer Emergency Response Team (CERT). Einrichtung, die die Verbesserung der Sicherheit von DV-Systemen zum Ziel hat, indem u.a. Informationen über Sicherheitsprobleme bei bestimmten Systemen verteilt und Lösungsmöglichkeiten aufgezeigt werden.
Siehe auch DFN-CERT.

Computerviren *Siehe* Viren.

Compute-Server Dedizierter Rechner für rechenintensive Anwendungen.

Constant Bit Rate (CBR) ATM-Service-Klasse, die eine konstante oder garantierte Übertragungsrate unterstützt. *Siehe auch* QoS.

Copycards Mit Magnetstreifen versehene Karten zur Bezahlung von Kopien, Ausdrucken und anderen Ressourcen ohne großen Verwaltungsaufwand. Die Abrechnungsbeträge werden von der Karte abgebucht, bis ein im voraus entrichteter Geldbetrag aufgebraucht ist.

CORBA *Siehe* Common Object Request Broker Architecture.

Corporate Network (CN) Ein von privatwirtschaftlichen Betreibern aufgebautes, standortübergreifendes Kommunikationsnetz für geschlossene Benutzergruppen.

CO-Switch *Siehe* Cell-Oriented-Switch.

CPU Central Processing Unit. Zentraleinheit eines Rechners.

Cracken „Knacken“ (Ausspähen) von Passwörtern.

Crack-Programme Programme, die bspw. durch das automatisierte „Ausprobieren“ von Wörtern aus elektronischen Wörterbüchern oder aus dem Umfeld eines Benutzers versuchen, das Passwort dieses Benutzers zu ermitteln.

CT-Switch *Siehe* Cut-Through-Switch.

Cut-Through-Switch (CT-Switch) Switch, der auf der Basis von Quellen- und Zieladressen arbeitet. Damit ist ein schnelles Weiterleiten von Paketen möglich.

DAR Deutscher Akkreditierungsrat.

Data Encryption Standard (DES) Symmetrisches Verschlüsselungsverfahren.
Siehe Kryptographische Verfahren.

Datagramm (datagram) Datenpaket, das verbindungslos, d.h. ohne fest geschaltete logische Kommunikationsverbindung, zwischen Sender und Empfänger im Netz übermittelt wird.

Datenbank-Server Dedizierter Rechner für Datenbanksysteme.

Datenschutzgesetze Landes- und Bundesgesetze zum Schutz personenbezogener Daten.

Datex-P Öffentliches Paketnetz der Deutschen Telekom AG.

DCE Siehe Distributed Computing Environment.

Denial-of-Service-(DoS)-Attacke Angriff, der zum Ziel hat, das angegriffene System durch starkes Anhäufen von Anfragen lahmzulegen.

DENIC Deutsches Network Information Center. Das DENIC betreibt den „Primary Name-Server“ für die deutsche Internet-Domain „de“ und vergibt Unterdomains zu „de“ sowie IP-Adressen.

DES *Siehe* Data Encryption Standard.

Desktop Management Interface (DMI) Gruppe betriebssystem- und protokollunabhängiger Programmierschnittstellen zum Management von PCs, Servern und anderer Hardware.

Desktop Management Task Force (DMTF) Arbeitsgemeinschaft, die das Entwickeln von Standards für das Management von PC-basierten Systemen (Einzelplatz, Netz) zum Ziel hat. *Siehe auch* DMI.

DFN-CERT Computer Emergency Response Team (Computer-Notfall-Team), das im Auftrag des DFN-Vereins Information und Beratung bei Sicherheitsproblemen im WiN leistet.

DFN-PCA Ein BMBF-gefördertes Projekt zum Aufbau einer Zertifizierungshierarchie in Deutschland. *Siehe auch* PCA.

DFN-Verein „Verein zur Förderung eines Deutschen Forschungsnetzes e.V.“ mit Sitz in Berlin, Betreiber des Wissenschaftsnetzes.

DFS *Siehe* Distributed File System.

DG/UX Herstellerabhängiges UNIX-Betriebssystem von Data General.

Dialog Nutzungsart für einen Rechner, bei der wechselweise Eingaben durch den Benutzer und Ausgaben durch den Rechner erfolgen.

Digitale Signatur Digitale Unterschrift. *Siehe* Kryptographische Verfahren.

Directory-Dienste Adressverzeichnisse von Netznutzern (E-Mail-Adressen) analog zu den Telefonbüchern (z.B. X.500, Whois, AMBIX-D des DFN-Vereins).

Directory-Server Dedizierter Rechner für Directory-Dienste.

Distributed Computing Environment (DCE) DCE, das von der OSF entwickelt wurde, dient der Realisierung vernetzter Client/Server-Umgebungen über Betriebssystemgrenzen hinweg.

Distributed File System (DFS) Teil von DCE. Wie beim Network File System (NFS) sind Daten im Netz auf verschiedenen Rechnern verfügbar. DFS bietet gegenüber NFS u.a. eine höhere Sicherheit durch Datenverschlüsselung beim Transport über das Netz.

DMI *Siehe* Desktop Management Interface.

DMTF *Siehe* Desktop Management Task Force.

DNS *Siehe* Domain Name Service.

DoD Department of Defense.

Domain (Domäne) Logischer Netzbereich (z.B. ein Hochschulnetz innerhalb des Wissenschaftsnetzes). Teilbereiche davon können ihrerseits Domains bilden (Subdomains), so dass sich ein hierarchischer Aufbau (bis herab zum einzelnen Host) ergibt. Die „Toplevel-Domain“ für alle deutschen Subdomains des Internet trägt den Namen „de“ und wird vom DENIC verwaltet.
Domains werden durch Angabe der zugehörigen IP-Adressen oder einen einprägsamen Domain-Namen charakterisiert. Domain-Namen haben folgende Struktur:
[hostname.[subdomain.[subdomain.[...]]]]domain.topleveldomain
Beispiel: rzux07.rz.uni-wuerzburg.de

Domain Name Service (DNS) Internet-Dienst, der dem Domain-Namen eines Rechners seine IP-Adresse zuordnet.

DOS Disk Operating System. *Siehe* MS-DOS.

DoS-Attacke *Siehe* Denial-of-Service-Attacke.

DTE Data Terminal Equipment. Gerät, das als Quelle oder Ziel von Daten den Datentransfer kontrolliert, z.B. Terminal oder PC.

DTE/DCE-Eigenschaft Accounting-Systeme, die mittels DTE/DCE-Eigenschaft aktiv in einen Datenstrom eingeschaltet werden, liefern exakte Messergebnisse, beeinflussen aber den Netzverkehr, z.B. Router, Firewall, Accounting-Box.

DV Datenverarbeitung.

DV-Ressourcen Datenverarbeitungsgeräte, Datenverarbeitungsmaterial, Datenleitungen und Netzkomponenten.

E/A-Server Dedizierter Rechner für den Betrieb von bestimmten Eingabe/Ausgabe-Geräten.

E-Basisdienste Dienste im Inneren des geschützten Netzes, die von Externen (z.B. Kunden der Klinik oder Verwaltung) genutzt werden.

EC *Siehe* Electronic Commerce.

EDI Electronic Data Interchange.

EDIFACT *Siehe* Electronic Data Interchange for Administration, Commerce, and Transport.

Einmal-Passwort Passwort, das nur einmal verwendet werden kann, so dass das Abhören durch Dritte keinen Missbrauch ermöglicht. *Siehe auch* S/Key.

Einwählknoten Wähleingänge zum Netz eines Online-Dienstes oder Internet-Providers.

Electronic Commerce (EC) Elektronischer Geschäftsverkehr.

Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT) Weltweites Regelwerk für den elektronischen Austausch von Geschäfts- und Handelsdaten.

Elektronische Post *Siehe* E-Mail.

E-Mail Electronic Mail, elektronische Post. E-Mail-Systeme unterstützen den Austausch von Nachrichten über Datennetze. Im Internet wird dafür das Protokoll SMTP verwendet. Daneben gibt es X.400-Mail-Systeme.

Encapsulating Security Payload Header (ESP) Sicherheitsoption in IPv6. Sie sichert durch Verschlüsselung die Integrität und Vertraulichkeit bei einer Rechner-Rechner-Kommunikation.

End to End Direkte Kommunikationsverbindung zwischen zwei Endgeräten im Netz.

EPHOS *Siehe* European Procurement Handbook for Open Systems.

ESP *Siehe* Encapsulating Security Payload Header.

Etagennetz Kommunikationsnetz, das die verschiedenen Räume innerhalb eines Stockwerks miteinander verbindet.

Ethernet Protokoll für lokale Netze mit einer Übertragungsrate von 10 Mbit/s. Als Übertragungsmedien werden Thick Wire Ethernet (Yellow Cable), Thin Wire Ethernet (Cheapernet), Twisted Pair (TP) Ethernet und Lichtwellenleiter verwendet.

European Procurement Handbook for Open Systems (EPHOS) Das Europäische Beschaffungshandbuch für offene Systeme enthält Richtlinien zur Beschaffung von Systemen der Informationstechnik (IT) und der Telekommunikation durch die öffentliche Hand.

EVG Evaluationsgegenstand.

Fast Ethernet Netzprotokoll für lokale Netze, das eine Datenübertragungsrate von 100 Mbit/s ermöglicht (Standard IEEE 802.3 und Standard IEEE 802.12).

FDDI *Siehe* Fiber Distributed Data Interface.

Fernzugriff Ortsunabhängiger Zugriff auf entfernte Systeme.

Fiber Distributed Data Interface (FDDI) Norm für die Struktur und Funktion von Glasfaserringnetzen mit einer Übertragungsrate von 100 Mbit/s.

File Datei.

File Transfer Protocol (FTP) Protokoll zur Übertragung von Dateien zwischen Rechnern im Internet.

File-Server Dedizierter Rechner, der Dateien für andere Rechner verwaltet. *Siehe auch* NFS, AFS, DFS.

File-Transfer *Siehe* File Transfer Protocol.

Filterregeln Regeln, die festlegen, welche Datenpakete von einer aktiven Netzkomponente weitergegeben bzw. ausgesondert werden.

Firewall System zur gegenseitigen Abschottung von Netzen unterschiedlichen Sicherheitsbedarfs. Mit Hilfe einer „Software-Brandschutzmauer“ werden dabei die Netze über Filterfunktionen und evtl. zusätzliche Authentifizierung mit einem Zugriffsschutz versehen.

Frame Datenpaket auf Schicht 2 des ISO/OSI-Modells.

Frame Tagging Herstellerabhängiges Verfahren zur Übermittlung von Paketen innerhalb und zwischen VLANs durch das Einfügen von ‚Tags‘.

Freeware Software, die kostenlos genutzt werden darf.
Siehe auch Public-Domain-Software, Shareware.

F-Secure Produktfamilie, die auf dem SSH-Protokoll basiert.
Siehe auch SSH.

FTP *Siehe* File Transfer Protocol.

FTP-Server Dedizierter Rechner, der frei verfügbare Software zur Übertragung bereithält. *Siehe auch* anonymous FTP.

Gast-Benutzerkennung Anonym zu nutzende Benutzerkennung, die nur für einige Grunddienste, wie Recherchen in Bibliothekskatalogen, gültig ist und nicht beantragt werden muss.

Gateway Netzkomponente (Kommunikationsrechner) zur Verbindung verschiedenartiger Rechnernetze.

Gebäudenetz Kommunikationsnetz innerhalb eines Gebäudes.

Global System for Mobile Communication (GSM) Internationaler Standard für digitale Funknetze.

Gopher Weltweit vernetztes Informationssystem im Internet, das auch über WWW zugänglich ist.

Graphical User Interface (GUI) Bezeichnung für eine grafisch aufgebaute Benutzeroberfläche.

GSM *Siehe* Global System for Mobile Communication.

GUI *Siehe* Graphical User Interface.

Hacking Unbefugtes Eindringen in ein Computersystem über dessen Verbindung zu einem Datennetz.

Hash-Komprimat Eine Art „Quersumme“ über eine Datei, an der Veränderungen der Daten zu erkennen sind.

HBFG Hochschulbauförderungsgesetz.

HDLC *Siehe* High Level Data Link Control.

Header *Siehe* Paketnetz.

High Level Data Link Control (HDLC) Herstellerneutrales, bitorientiertes, synchrones Übertragungsprotokoll. Es unterstützt Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-Verbindungen.

HIS Hochschul-Informations-System GmbH.
Gemeinsam von Bund und Ländern finanzierte Gesellschaft, die Software für den Verwaltungsbereich von Hochschulen anbietet.

Hochleistungsrechner Vektor- oder Parallelrechner (bzw. Kombination daraus).

Hochschulnetze Datennetze im Hochschulbereich. Zu unterscheiden sind hochschulinterne Rechnernetze und hochschulübergreifende Netze.

Höchstleistungsrechner Rechner der höchsten verfügbaren Leistungsklasse.

Host Rechner in einem Datennetz, insbesondere Rechner mit Leistungsfunktionen für andere Rechner im Netz, z.B. zur Bereitstellung von Datenbanken.

HP-UX Herstellerabhängiges UNIX-Betriebssystem von Hewlett Packard.

HTML *Siehe* Hypertext Markup Language.

HTTP *Siehe* Hypertext Transfer Protocol.

HTTPS *Siehe* Hypertext Transfer Protocol, Secure.

HyperLinks Verweise im WWW auf andere Dokumente und Daten; kodiert in URLs.

Hypertext Markup Language (HTML) Standardformat der Dokumente im WWW. HTML ist hard- und softwareunabhängig.

Hypertext Transfer Protocol (HTTP) Client/Server-Protokoll für den Zugriff auf Informationen im WWW.

Hypertext Transfer Protocol, Secure (HTTPS) Variante des HTTP-Protokolls, wird zur Herstellung von verschlüsselten Verbindungen (*siehe auch* SSL) benutzt.

I-Basisdienste Dienste, die vom Inneren des geschützten Netzes aus genutzt werden.

ICMP *Siehe* Internet Control Message Protocol.

ICMP-Redirect Nachricht eines Gateways an einen Host, für die Datenübertragung ein anderes (besseres) Gateway zu benutzen. *Siehe auch* ICMP.

IDEA *Siehe* International Data Encryption Algorithm.

IDENTD Identification Daemon. Dient bei „anonymen“ Diensten der Rückverfolgung von Verbindungen zur Identifikation des Nutzers.

IDS *Siehe* Intrusion-Detection-System.

IEEE Institute of Electrical and Electronic Engineers. Standardisierungsinstitution.

IETF *Siehe* Internet Engineering Task Force.

Information Highway „Datenautobahn“, Hochgeschwindigkeitsdatennetz für Multimedia-Anwendungen.

Informationsdienste Netzdienste, die dem Benutzer die Informationssuche erleichtern. Beispiele im Internet: Gopher, WorldWideWeb.

International Data Encryption Algorithm (IDEA) Blockorientierter Verschlüsselungsalgorithmus, der mit 64-Bit-Blöcken und einer Schlüssellänge von 128 Bit arbeitet.

International Telecommunication Union (ITU) Weltweit tätige Organisation, die den Aufbau und Betrieb von Telekommunikationsnetzen und -diensten koordiniert.

Internet Weltweiter Verbund von Netzen auf Basis der Protokollfamilie TCP/IP mit derzeit etwa 60 Mio. Teilnehmern.

Internet Control Message Protocol (ICMP) Ein Internet-Protokoll der Schicht 3, das Kontroll-, Fehlerkorrektur- und zusätzliche Informationsfunktionen enthält.

Internet Engineering Task Force (IETF) Teil des Internet Activities Board (IAB); ist verantwortlich für die technischen Entwicklungen des Internet, besteht aus etwa 40 Arbeitsgruppen.

Internet-(Service-)Provider Anbieter von Internet-Diensten.

Internet-Adresse *Siehe* IP-Adresse.

Internet-Dienst Netzdienst auf Grundlage der TCP/IP-Protokollfamilie, z.B. E-Mail nach SMTP, News, WWW.

Internet Protocol (IP) *Siehe* TCP/IP.

Internet Relay Chat (IRC) Internet-Dienst, der den Benutzern ermöglicht, per Tastatureingaben in Echtzeit miteinander zu kommunizieren (to chat = plaudern).

Intranet Technisch gesehen ist ein Intranet ein firmeninternes Netz, das auf der Internet-Technologie aufbaut. Es kann mit dem Internet verbunden sein, muss es aber nicht notwendigerweise sein.

Intrusion-Detection-System (IDS) System, das Angriffe und Angriffsversuche schon während ihres Ablaufens entdecken und Gegenmaßnahmen ermöglichen soll.

IP *Siehe* TCP/IP.

IP-Adresse Zahlenkombination, die einen Rechner im Internet eindeutig bezeichnet. IP-Adressen haben folgende Struktur: a.b.c.d (a, b, c, d sind natürliche Zahlen zwischen 0 und 255). In Deutschland werden IP-Adressbereiche vom DENIC vergeben. Es werden drei Größenklassen von IP-Adressbereichen unterschieden:

Class A:	1.b.c.d	bis	126.b.c.d
Class B:	128.1.c.d	bis	191.255.c.d
Class C:	192.1.1.d	bis	223.255.255.d

(Über die Variablen kann vom Inhaber eines Adressbereiches verfügt werden.)

IPng Internet Protocol next generation ist eine Arbeitsgruppe der IETF, die eine neue Version des IP-Protokolls (IPv6) entwickelt. Die neuen IP-Adressen sollen aus 6 Bytes bestehen und neben der Vergrößerung des Adressraumes auch noch zusätzliche Funktionalitäten bereitstellen.

IP-Spoofing Umgehen von Sicherheitskontrollen, die lediglich auf der Abfrage der IP-Adresse beruhen, durch Vortäuschen einer gefälschten IP-Adresse.

IPv6 *Siehe* IPng.

IPX *Siehe* SPX/IPX.

IRC *Siehe* Internet Relay Chat.

IRIX Herstellerabhängiges UNIX-Betriebssystem von Silicon Graphics.

ISDN Integrated Services Digital Network. International genormtes, öffentliches, digitales Wählnetz, das über einen einzigen Anschluss verschiedene Dienste der Sprach- und Datenkommunikation anbietet.

ISDN-Adapter Adaptierende Funktionseinheit für den Zugang von PCs zum ISDN. *Siehe auch* ISDN.

ISO/OSI-Modell International Organization for Standardization / Open Systems Interconnection-Modell. Universelles, hierarchisches 7-Schichten-Modell der Datenkommunikation.
Schicht 7: Anwendungsschicht
Schicht 6: Darstellungsschicht
Schicht 5: Kommunikationssteuerungsschicht
Schicht 4: Transportschicht
Schicht 3: Vermittlungsschicht
Schicht 2: Sicherungsschicht
Schicht 1: Bitübertragungsschicht
Die Kommunikation zwischen gleichen Schichten verschiedener Partner wird durch Protokolle geregelt.

IT Informationstechnik.

ITSEC Information Technology Security Evaluation Criteria. Europäische Kriterien für die Sicherheitszertifizierung von Produkten und Systemen.

ITU *Siehe* International Telecommunication Union.

IuKDG Informations- und Kommunikationsdienste-Gesetz.
Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste.

Java Von der Firma Sun entwickelte, rechner- und betriebssystemunabhängige Programmiersprache. Sie ist objektorientiert und besonders geeignet zur Gestaltung von WWW-Seiten. Dabei werden Quellentexte von Programmen in einen plattformunabhängigen Zwischencode übersetzt. Dieser kann dann durch geeignete Interpreter auf beliebigen Rechnersystemen abgearbeitet werden.

Java-Applet Programmteile, die kompiliert an einen Rechner übertragen und dort durch einen javafähigen Browser ausgeführt werden.

JavaScript Ein von der Firma Netscape eingeführter Quasi-Standard, um in HTML-Seiten ausführbare Scripte zu integrieren. Mit JavaScript können z.B. interaktive Formulare mit integrierten Plausibilitätsprüfungen realisiert werden.
JavaScript und Java sind zunächst zwei unterschiedliche Systeme.

Joint Editing Mit einem Joint Editing Tool (einem sog. „Whiteboard“) können Teilnehmer einer Multimedia-Konferenz gemeinsam an einem Grafik- oder Textdokument arbeiten.

KBV Kassenärztliche Bundesvereinigung.

Kerberos Das Programmsystem Kerberos dient der gesicherten Authentifizierung von Benutzern in Datennetzen. Dabei erhält der Client auf Anforderung von einem Kerberos-Server ein sog. „Ticket“ mit (verschlüsselter) Authentifizierungsinformation, das dem Client erlaubt, bestimmte Dienste auf einem anderen Rechner in Anspruch zu nehmen.

Key Management Verwaltung kryptographischer Schlüssel.

Key-Escrow-Verschlüsselung Kryptographisches Verfahren, bei dem die privaten Schlüssel bei einer staatlichen Stelle hinterlegt werden, um ggf. die Überwachung des Datenverkehrs zu ermöglichen.

Key-Recovery-Mechanismen Mechanismen, die die Hinterlegung sogenannter Ersatzschlüssel bei „vertrauenswürdigen Stellen“ vorsehen.

Key-Server Verfahren und Systeme zur Verwaltung und Verteilung öffentlicher Schlüssel.

Koaxialkabel Kabel zur Übertragung von Breitband-Signalen. Wichtige Ausführungsformen für LANs sind Cheapernet-Kabel (10Base2) und Yellow Cable (10Base5).

Kommunikationsprotokoll *Siehe* Protokoll.

Kryptanalyse Aktivitäten zur Dechiffrierung von verschlüsselten Texten.

Krypto-Box Spezielles Datenschutzsystem, das die zu übertragenden Daten verschlüsselt.

Kryptographische Verfahren Verschlüsselungsverfahren, die es ermöglichen, Daten abhörsicher an einen Empfänger zu versenden oder mit einer digitalen Signatur die Unversehrtheit einer Nachricht beim Transport über das Netz zu gewährleisten und den Absender sicher zu authentifizieren.

Krypto-Kanal Technische Möglichkeit des verdeckten Informationsaustausches durch den Einsatz von Krypto-Boxen und -Routern.

Krypto-Router Komponenten, die eine Verschlüsselung des gesamten Datenverkehrs zwischen zwei oder mehreren Standorten vornehmen.

KVK Krankenversichertenkarte.

LAN *Siehe* Local Area Network.

LAN Emulation (LANE) LAN Emulation erlaubt eine protokolltransparente Kopplung von LANs über ATM sowie die Kommunikation mit direkt an ATM angeschlossenen Endgeräten.
LAN Emulation ist in einer Client/Server-Architektur konzipiert. Es besteht aus LAN Emulation Client (LEC) und LAN Emulation Service. Der LAN Emulation Service wiederum zerfällt in drei Teile: LAN Emulation Configuration Server (LECS), LAN Emulation Server (LES) und Broadcast and Unknown Server (BUS).

LAN Emulation Client (LEC) Ein LEC befindet sich in jedem direkt angeschlossenen Endgerät oder Edge-Device (z.B. Bridge, Router).
Siehe auch LAN Emulation (LANE).

LAN Emulation Configuration Server (LECS) Kontrollinstanz für die gesamte Umgebung von LANE. Der LECS regelt die Zuordnung von einzelnen Clients zu verschiedenen emulierten LANs durch Vermitteln der ATM-Adressen der LES.
Siehe auch LAN Emulation (LANE).

LAN Emulation Server (LES) Kommando- und Kontrollzentrale innerhalb eines LANE. Der LES registriert MAC-Adressen und löst sie zu ATM-Adressen auf. *Siehe auch* LAN Emulation (LANE).

LAN Emulation Service Server-Komponente von LANE, besteht aus drei Teilen, die zentral oder verteilt über das Netz implementiert werden können. *Siehe auch* LAN Emulation (LANE).

LANE *Siehe* LAN Emulation.

LDAP *Siehe* Lightweight Directory Access Protocol.

LEC *Siehe* LAN Emulation Client.

LECS *Siehe* LAN Emulation Configuration Server.

LES *Siehe* LAN Emulation Server.

Lichtwellenleiter (LWL) Glasfaserkabel (fiber optic cable).

Lightweight Directory Access Protocol (LDAP) Offene, im Internet standardisierte Schnittstelle, die es erlaubt auf standardisierte Directory-Dienste (z.B. X.500, NDS) zuzugreifen.

Local Area Network (LAN) Nahverkehrsnetz.

Login Anmeldung (mit Benutzerkennung und Passwort) eines berechtigten Nutzers bei einem Rechner zu Beginn einer Arbeitssitzung.

Logout Abmeldung eines Nutzers bei einem Rechner am Ende einer Arbeitssitzung.

LWL *Siehe* Lichtwellenleiter.

MAC Medium Access Control auf Schicht 2 im ISO/OSI-Modell.

Mailbox DV-System bzw. Dateiverzeichnis für Empfang, Speicherung, Abruf und Versand elektronischer Post.

Mail-Server Dedizierter Rechner für das Speichern und Verarbeiten von E-Mails.

Mainframe Universalrechner mit proprietärem Betriebssystem.

Makroviren Ein Makrovirus nutzt die Makrosprache einer Applikation (z.B. MS-Word, MS-Excel), um sich zu verbreiten und eventuell weitere Wirkungen zu erzielen. *Siehe auch* Viren.

MAN *Siehe* Metropolitan Area Network.

Management Information Base (MIB) Datenbank, in der die im Netz angeschlossenen und zu verwaltenden Objekte und Funktionen beschrieben sind, die z.B. mittels SNMP gemanagt werden können.

Mbone Multicast Backbone. Internet-Dienst für multimediale Videokonferenzen mit der Möglichkeit des Joint Editing.

Metropolitan Area Network (MAN) Kommunikationsnetz zur Verbindung von Einrichtungen, die in einem Stadtbereich verteilt sind.

MIB *Siehe* Management Information Base.

Microsoft Network (MSN) Online-Dienst der Fa. Microsoft.

MIME *Siehe* Multipurpose Internet Mail Extensions.

Modem Modulator/Demodulator. Gerät, das einen digitalen Bitstrom in analoge Signale umwandelt und umgekehrt.

MO-Disk Magneto-optische Platte.

Moni-Box Vom Regionalen Rechenzentrum Erlangen entwickeltes Accounting-System zum Aufzeichnen von Kommunikationsvorgängen in lokalen Netzen.

Monitoring Aufzeichnung von Verkehrsdaten in Netzen zur Betriebsüberwachung.

MPEG Motion Picture Experts Group. Mit MPEG-Verfahren lassen sich Bewegtbilddaten komprimieren.

MPOA *Siehe* Multiprotocol over ATM.

MS Windows Familie von PC-Betriebssystemen der Fa. Microsoft (WINDOWS 3.1x, WINDOWS95, WINDOWSNT).

MS-DOS PC-Betriebssystem der Fa. Microsoft.

MSN *Siehe* Microsoft Network.

MUCK *Siehe* Multifunktionale Universitätschipkarte.

Multi User Host Zentraler Rechner mit Mehrbenutzersystem.

Multicast Backbone *Siehe* Mbone.

Multicast-Verfahren „Einer-an-Viele“-Verfahren. Damit kann eine ganze Gruppe von Rechnern adressiert werden.

Multifunktionale Universitätschipkarte (MUCK) Pilotprojekt zur Verbesserung von universitären Abläufen durch die Einführung einer Chipkarte für Mitarbeiter und Studenten.

Multimedia Integration von Informationen verschiedener Medien (Text, Grafik, Bild und Ton).

Multimedia-Konferenz Bei einer Multimedia-Konferenz steht den Teilnehmern neben Audio- und Videokommunikationsdiensten auch ein Joint-Editing-Dienst zur Verfügung. Beispiel: Mbone.

Multimediale Internet-Dienste *Siehe* Mbone, WWW.

Multiprotocol over ATM (MPOA) MPOA ist neben LANE ein weiterer Ansatz, eine protokolltransparente Kopplung von LANs über ATM sowie die Kommunikation mit direkt an ATM angeschlossenen Endgeräten zu ermöglichen. Es wurde im Herbst 1997 vom ATM Forum spezifiziert.

Multiprozessor-Systeme Rechnersysteme mit mehreren Prozessoren.

Multipurpose Internet Mail Extensions (MIME) Protokoll zur Identifikation empfangener Daten als Text, Grafik oder Audiodaten mit entsprechender Darstellung.

Name-Server Dedizierter Rechner für den Domain Name Service (DNS).

NDS *Siehe* Novell Directory Services.

Netiquette Guidelines Ratschläge zur verantwortungsvollen Nutzung des Internet (RFC 1855).

NetNews Internet-Dienst. Diskussionsforum in Form eines „elektronischen schwarzen Bretts“, bei dem auf speziellen News-Servern den Benutzern Artikel zu bestimmten Themengebieten, sogenannten News-Gruppen, zur Verfügung gestellt werden. Der Benutzer kann auch selbst Informationen einspeisen („posten“) und Diskussionspartner sein.

Network File System (NFS) Dateiverwaltungssystem der Firma Sun. Mit NFS können File-Systeme, die auf verschiedenen Rechnern liegen, zu einem einzigen logischen Verzeichnisbaum kombiniert werden. Alle gängigen UNIX-Systeme unterstützen NFS.

Network Information Service (NIS) Von der Firma Sun entwickelter Netzdienst, der Administrationsinformationen (z.B. Konfigurationsdaten, Benutzer-Accounts) zur Verfügung stellt. NIS wird über RPC realisiert.

Network News — *Siehe* NetNews.

Network News Transport Protocol (NNTP) — Die NetNews-Daten werden mit Hilfe von NNTP im Internet übertragen.

Netzdienst — Über ein Daten-/Sprachnetz verfügbarer Kommunikationsdienst.

Netzdurchsatz — Übertragene Datenmenge pro Zeiteinheit (in bit/s).

Netzkomponenten — „Passive“ Netzbestandteile (wie Leitungen, Verteiler, Anschlussdosen) und „aktive“ elektronische Geräte für den Netzbetrieb (wie Bridges, Gateways, Router, Modems).

Netzmanagement — Gesamtheit der Vorkehrungen und Aktivitäten zur Sicherstellung eines effektiven und effizienten Einsatzes eines Rechnernetzes.

Netzsegment — Physische Untereinheit eines Netzes.

Netztechnologien — *Siehe* ATM, Ethernet, Fast Ethernet, FDDI, ISDN.

Netz-File-System — *Siehe* Network File System.

News — *Siehe* NetNews.

News-Server — Dedizierter Rechner für die Speicherung und Verteilung von News-Artikeln.

NFS — *Siehe* Network File System.

NIP — Netz-Investitionsprogramm im Rahmen des HBFG, das den Aufbau hochschulinterner Rechnernetze zum Ziel hat.

NIS — *Siehe* Network Information Service.

NNTP — *Siehe* Network News Transport Protocol.

Notfallplan — Zusammenstellung von Regeln und Prozeduren, die bei einem Notfall befolgt werden sollen.

Novell Directory Services (NDS) — Die Novell Directory Services wurden für die Verwaltung von E-Mail-Adressen in Novell-Netzen entwickelt. Daraus ist mittlerweile eine dezentrale Datenbank zur Verwaltung von Benutzeraccounts, Zugriffsrechten, Netzressourcen, u.v.a.m. entstanden.

Novell NetWare — NetWare der Firma Novell ist eines der am weitesten verbreiteten Client/Server-Netz-Betriebssysteme.

nrt-VBR — *Siehe* Variable Bit Rate.

Offene Systeme — Kommunikationssysteme, die eine einfache Verknüpfung von Rechnern über Betriebssystem- und Herstellergrenzen hinweg ermöglichen sollen (open systems).

Offline-Erfassung Erfassung von Daten durch ein Erfassungssystem ohne unmittelbare Verbindung zu einem Datennetz.

One-Time-Passwort Passwort, das nur für eine Session Gültigkeit hat. *Siehe auch* Challenge-Response-Verfahren.

Online-Dienst(-Anbieter) Kommerzieller Anbieter proprietärer Netzdienste und meist auch von Internet-Diensten über Einwählknoten. Beispiele: AOL, CompuServe, MSN, T-Online.

Online-Erfassung Erfassung von Daten mit sofortiger Übertragung über das Netz zu einem Auswertungssystem.

Online-Wartung Fernwartung von DV-Systemen über das Datennetz.

OPAC Online Public Access Catalogue. System, das dem Benutzer den direkten Zugriff auf einen Bibliothekskatalog oder eine Datenbank ermöglicht.

Open Software Foundation (OSF) Vereinigung von fast allen wichtigen DV-Herstellern für gemeinsame Entwicklungen, z.B. einheitliches Betriebssystem auf der Basis von UNIX.

Packet-Screen Komponente (Hard- und Software), die sich an der Schnittstelle zweier Netze befindet. Mittels Filterregeln auf der Vermittlungs- bzw. Transportschicht werden die Zugriffe nach beiden Seiten kontrolliert.

Paketnetz In einem paketvermittelnden Netz werden die Daten in Blöcke (Pakete) eingeteilt, die unabhängig voneinander über das Netz geschickt werden. Jeder Block besteht aus einem Kopfteil (header), der insbesondere die Adressinformation enthält, und einem Datenteil.

Parallelrechner Hochleistungsrechner mit vielen Prozessoreinheiten.

Passwort Individuell gewählte, geheimzuhaltende Zeichenkette für die Authentifizierung eines Nutzers gegenüber einem Rechner, Zugangscode.

Passwortdatei Geschützte Datei auf einem Rechner, welche die Passwörter der Benutzer in verschlüsselter Form enthält.

Passwort-Scanner Verfahren, das es gestattet, Passwörter auf ihre Sicherheit hin zu überprüfen.

Patches Softwarekomponenten, die den Systemadministratoren von Firmen zur Verfügung gestellt werden, um fehlerhafte Funktionen von Betriebssystemen oder bereits im Einsatz befindlicher Software zu korrigieren.

PCA *Siehe* Policy Certification Authority.

PCL *Siehe* Printer Control Language.

PDU *Siehe* Protocol Data Unit.

PEM *Siehe* Privacy Enhanced Mail.

Performance Leistung eines Informationsverarbeitungssystems.

Permanent Virtual Circuit (PVC) Dauerhaft eingerichtete virtuelle Verbindung, die zwei Stationen fest miteinander verbindet. Ihre Aktivierung erfolgt durch eine zentrale Stelle.

Personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Beim Umgang mit personenbezogenen Daten sind die Datenschutzgesetze zu beachten.

PGP *Siehe* Pretty Good Privacy.

PIN Persönliche Identifikationsnummer.

Policy Certification Authority (PCA) Hauptaufgabe einer PCA ist das Erstellen von Sicherheitsrichtlinien für die Zertifizierung von Schlüsseln (Policy). Diese Policy bildet die Grundlage fast aller Aktionen einer PCA und legt zusätzlich Richtlinien fest, die von den in der Hierarchie unterhalb angesiedelten CAs und Benutzern einzuhalten sind.

Port Die Kommunikation zwischen Rechnern erfolgt auf der Transportschicht im ISO/OSI-Modell über sogenannte Portnummern. Für einige Standarddienste werden von der IANA (Internet Assigned Numbers Authority) sogenannte Well-Known-Portnummern vergeben. Beispiel: Port 21 gilt für FTP-Server.

Pretty Good Privacy (PGP) Ein im Internet frei verfügbares Programm, das mittels eines asymmetrischen Verfahrens das Verschlüsseln und elektronische Signieren von Dateien ermöglicht.

Postscript Seitenbeschreibungssprache mit flexiblen Schriftfunktionen und hochqualitativer Grafikausgabe.

Printer Control Language (PCL) Herstellerspezifische Sprache zur Steuerung von Druckern; entwickelt von Hewlett Packard (HP).

Privacy Enhanced Mail (PEM) Spezifikation zur Verschlüsselung von E-Mail-Nachrichten.

Private Key *Siehe* Asymmetrische Verschlüsselung.

Private Virtual Channel *Siehe* Virtual Channel (VC).

Produkt Kommerziell erhältliche Hardware und/oder Software.

Produkt-Zertifizierung *Siehe* Zertifizierung.

Proprietäres Betriebssystem Herstellerspezifisches Betriebssystem wie MVS (der Fa. IBM) oder VMS (der Fa. DEC).

Protocol Data Unit (PDU) Dateneinheit, die auf gleicher Schicht des ISO/OSI-Modells ausgetauscht wird.

Protokoll Satz von Vorschriften und Regeln für eine bestimmte Form des Informationsaustausches über ein Datennetz auf gleicher Schicht im ISO/OSI-Modell.
Siehe auch SPX/IPX, TCP/IP, X.25.

Protokollanalysator Gerät, das passiv an ein Datennetz angeschlossen wird, um den Netzverkehr zu beobachten und zu analysieren.

Provider *Siehe* Service-Provider.

Proxy Ein Proxy ist ein Stellvertreter des Servers gegenüber dem Client und ein Stellvertreter des Client gegenüber dem Server. Nach Authentifizierung des Clients bzw. des Servers gegenüber dem Proxy, arbeitet dieser transparent. Proxies existieren z.B. für HTTP, SMTP, FTP, Telnet, . . .

Prozessorchipkarte *Siehe* Chipkarte.

Public Key *Siehe* Asymmetrische Verschlüsselung.

Public-Domain-Software Software, bei welcher der Autor auf seine Urheberrechte (ggf. mit Einschränkungen) verzichtet hat.
Siehe auch Freeware, Shareware.

Punkt-zu-Punkt-Verbindung „Einer-an-Einen“-Verfahren. Es wird nur ein Rechner adressiert.

PVC *Siehe* Permanent Virtual Circuit.

QoS *Siehe* Quality of Service.

Quality of Service (QoS) Die Güte des Übertragungsdienstes wird bei einer Ende-zu-Ende-Beziehung an Hand von einigen Parametern definiert.

RA *Siehe* Registration Authority.

RADIUS *Siehe* Remote Authentication Dial-In User Service.

RAM-Disk Im Arbeitsspeicher (Random Access Memory, RAM) nachgebildetes Rechner-Laufwerk mit schnellem Zugriff.

Raubkopien Unrechtmäßig erstellte Softwarekopien.

Recovery-Maßnahmen Maßnahmen, die dem Wiederherstellen eines definierten Zustandes dienen sollen.

Referenzmonitor Im Sinne der Sicherheitstheorie ist es der Teil des Systems, der die sicherheitsrelevanten Funktionen enthält. Er ermöglicht es, sich bei der Umsetzung der Sicherheitspolitik ganz auf die Sicherheitsaspekte zu konzentrieren.

Registration Authority (RA) Optional in der PCA-Hierarchie zwischengeschaltete Instanz, die Teilnehmeridentitäten überprüft, aber keine Zertifikate ausstellt.

Remote Access *Siehe* Fernzugriff.

Remote Authentication Dial-In User Service (RADIUS) System mit einer Authentifizierungsdatenbank, das eine einfache Authentifizierung auf der Basis von Login-Kennungen und Passwörtern durchführt.

Remote Login Anmeldungsprozedur bei einem entfernten Rechner. *Siehe auch* Telnet.

Remote Procedure Call (RPC) Aufruf einer Prozedur in einem Modul oder einer Task, die möglicherweise auf einem entfernten Rechnersystem stattfindet.

Remote Shell (rsh) Protokoll, das die Ausführung von Kommandos auf entfernten Rechnersystemen ermöglicht.

Requests for Comments (RFCs) Durch fortlaufende Nummern gekennzeichnete Dokumente des IAB (Internet Architecture Board) mit technischen Mitteilungen, Standards und Nutzerinformationen zum Internet. Die RFCs sind im Netz z.B. unter `ftp://nis.nsf.net/documents/rfc/` frei verfügbar.

Revisionssicherheit Fähigkeit, Aktivitäten im Netz und auf den Rechnersystemen nachträglich nachvollziehen zu können (z.B. durch Aufzeichnung von Verbindungsdaten).

RISC-Technologie Prozessortechnologie für leistungsfähige Rechner (Reduced Instruction Set Computer).

rlogin *Siehe* Remote Login.

RMON-Client Spezielles Gerät, das passiv an ein Datennetz angeschlossen wird, um den Netzverkehr zu beobachten und zu analysieren.

root Spezieller Benutzerzugang auf UNIX-Systemen, der die Steuerung des Systems erlaubt.

root-Rechte Erweiterte Benutzerrechte für den root-Account, erforderlich zur Systemadministration.

Router Aktive Netzkomponente, die als Schnittstelle zwischen Netzen Funktionen bis zur Vermittlungsschicht (ISO/OSI-Schichten 1 – 3) erfüllt. Auf Schicht 3 sind dies u.a. die Wegewahl für Datenpakete und die Vermittlung zwischen verschiedenen Netzschichten. Router als Schicht-3-Komponenten können auf verschiedenen Medienprotokollen (wie z.B. Ethernet und FDDI) aufsetzen. Lokale Netze werden durch Router zur Lasttrennung in Subnetze aufgeteilt.
Im Internet, wo durchgehend IP als Netzprotokoll eingesetzt wird, wird statt der Protokollumsetzung auf Schicht 3 eine andere Methode zum Passieren von Netzen mit anderer Vermittlungsschicht (z.B. X.25), das sog. Tunneling, verwendet. Hierbei packen Router auf der einen Seite die Datenpakete (hier: IP) in Datenpakete einer anderen Vermittlungs- oder höheren Schicht (z.B. X.25) ein und auf der anderen Seite wieder aus. (Beispiele: IP über X.25; IP über ATM; X.25 über TCP).

Routing Wahl des Übertragungsweges für ein Datenpaket.

RPC *Siehe* Remote Procedure Call.

RSA Asymmetrisches Verschlüsselungsverfahren, benannt nach den Entwicklern Rivest, Shamir und Adleman, das auf großen Primzahlen basiert.

rsh *Siehe* Remote Shell.

rt-VBR *Siehe* Variable Bit Rate.

S/Key Verfahren zur Erzeugung von Einmalpasswörtern, basierend auf der Client/Server-Architektur.

S/MIME *Siehe* Secure Multipurpose Internet Mail Extensions.

SANUS Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmen auf der Basis internationaler Normen und Standards. Vom BMBF gefördertes Projekt, das die Bereitstellung in der Praxis erprobter Hilfsmittel und Leitlinien zur Umsetzung der EU-Richtlinie zum Arbeits- und Gesundheitsschutz an computerunterstützten Arbeitsplätzen zum Ziel hat.

SAP Systems, Applications, and Products in Data Processing.
Anbieter von Lösungen auf dem Gebiet der kommerziellen Client/Server-Anwendungen.

SATAN *Siehe* Security Administrator Tool for Analyzing Networks.

Scanner (a) Optisches Eingabegerät.
(b) Verfahren zur Überprüfung von Sicherheitsmaßnahmen.

SCO-Unix Weitgehend herstellerunabhängiges UNIX-Betriebssystem.

Screened Subnet Teilnetz, das sich zwischen zwei Packet-Screens befindet und in dem auch ein Application-Gateway als Bastion betrieben wird.

Secure Electronic Marketplace for Europe (SEMPER) Ein von der Europäischen Kommission gefördertes Projekt, das die Grundlagen für sichere elektronische Geschäfte über öffentliche Netze schaffen soll.

Secure Multipurpose Internet Mail Extensions (S/MIME) Verfahren zum Verschlüsseln und Signieren von E-Mail-Nachrichten nach dem MIME-Standard.

Secure Shell (SSH) Ermöglicht eine gesicherte Verbindung zwischen Rechnern.

Secure Sockets Layer (SSL) Protokoll für verschlüsselte Datenübertragung.

Security Administrator Tool for Analyzing Networks (SATAN) Programm, das über das Netz Sicherheitslücken in Computersystemen aufspürt und vom Systembetreiber zur Verbesserung der Sicherheit, aber auch von Hackern verwendet werden kann.

SEMPER *Siehe* Secure Electronic Marketplace for Europe.

Server *Siehe* Client/Server-Modell.

Service-Provider Anbieter von Netzdiensten. Beispiele: Mobilfunk-(Service-) Provider, Online-Dienste, Internet-Provider.

Session Key Schlüssel, der für jeweils genau einen Verschlüsselungsvorgang bzw. für ein begrenztes Zeitintervall gilt.

SF-Switch *Siehe* Store-and-Forward-Switch.

SGB Sozialgesetzbuch.

Shadow-Mechanismus Verfahren, das dafür Sorge trägt, dass die verschlüsselt gespeicherten Passwörter der Benutzer nur für den jeweiligen Systemverwalter „sichtbar“ sind; erschwert damit die üblichen Crack-Versuche.

Shareware Software, die kostenlos erprobt werden kann; bei dauerhafter Benutzung ist ein Unkostenbeitrag an den Autor zu entrichten.
Siehe auch Public-Domain-Software, Freeware.

S-HTTP *Siehe* HTTPS.

Sicherheitskonzept Festlegung relevanter Sicherheitsziele und der erforderlichen organisatorischen und technischen Maßnahmen.

Sicherheitsmanagement Verwaltung von sicherheitsrelevanten Komponenten und Funktionen entsprechend einer definierten Sicherheitspolitik.

Sicherheitspatches *Siehe* Patches.

Sicherheitsstufe Nach den ITSEC unterscheidet man sechs Sicherheitsstufen von DV-Systemen (E1 bis E6).

SigG Gesetz zur digitalen Signatur.

Signatur Digitale Unterschrift.

SigVO Verordnung zum Signaturgesetz.

Simple Mail Transport Protocol (SMTP) Protokoll für E-Mail im Internet.

Simple Network Management Protocol (SNMP) Herstellerunabhängiger Standard, vorwiegend eingesetzt zum Managen von TCP/IP-Netzen. Mit SNMP können gewisse Eigenschaften von Rechnern abgefragt und modifiziert werden. Es können in gewissen Situationen auch Alarmsignale (SNMP-Traps) an die Management-Station gesendet werden.

Single-Signon (SSO) Ein Benutzer besitzt nur eine Kennung innerhalb eines Netzes. Mit dieser Kennung kann er sich anmelden und auf alle Systeme und Anwendungen im Netz zugreifen, für die er berechtigt ist, wobei der Begriff „Netz“ sowohl für ein zusammenhängendes physisches Netz als auch für mehrere Netze stehen kann.

SmartCard *Siehe* Chipkarte.

SMTP *Siehe* Simple Mail Transport Protocol.

SNMP *Siehe* Simple Network Management Protocol.

Software Metering Überwachung von Software-Lizenzen, durch die sichergestellt wird, dass nur eine gewisse, von einem automatischen Zähler kontrollierte Anzahl von Nutzern die Software im Netz gleichzeitig verwenden kann.

Solaris Herstellerabhängiges UNIX-Betriebssystem von Sun.

Spoofing Eine Identität vortäuschen, sich als jemand anderes ausgeben. Beim IP-Spoofing konfiguriert ein Teilnehmer des Internet seinen Rechner so, dass dieser die IP-Adresse eines anderen Rechners verwendet.

SPX/IPX Netzprotokolle der Firma Novell analog zu TCP/IP.

SQL *Siehe* Structured Query Language.

SSH *Siehe* Secure Shell.

SSL *Siehe* Secure Sockets Layer.

SSLeay SSL-Implementierung von E. A. Young. Sie erlaubt es, Applikationen zu erstellen, die mit Schlüssellängen arbeiten, die nicht von Exportbeschränkungen betroffen sind.
Siehe auch Apache-SSL.

SSO *Siehe* Single-Signon.

Stadtnetz *Siehe* Metropolitan Area Network.

Stand-alone-System Rechner ohne Netzanschluss.

Standleitung Fest geschaltete Leitungsverbindung.

Steganographie Bezeichnung für Verfahren, die Nachrichten in größeren Trägerbotschaften verstecken. So kann z.B. das jeweils niedrigste Bit eines Pixels einer Grafikdatei eine verborgene Information enthalten.

StGB Strafgesetzbuch.

Store-and-Forward-Switch (SF-Switch) Ein SF-Switch empfängt und puffert ein gesamtes Paket und kann zusätzliche Fehlerprozeduren ausführen.

Structured Query Language (SQL) Standardisierte Sprache, mit der Datenbankanfragen an relationale Datenbanken plattformunabhängig formuliert werden können.

Subnetz Teilnetz eines Kommunikationsnetzes.

Supervisor Call (SVC) Mechanismus, der es nichtprivilegierten Prozessen ermöglicht, Leistungen privilegierter Funktionen zu erhalten.

SVC a) *Siehe* Switched Virtual Circuit.
b) *Siehe* Supervisor Call.

Switch Spezielle aktive Netzkomponente.

Switched Virtual Circuit (SVC) Gewählte virtuelle Verbindung, die mit Hilfe der Signalisierungsprotokolle aufgebaut wird. Die miteinander zu verbindenden Stationen werden bei der Verbindungsanforderung durch den Benutzer festgelegt.

Symmetrische Verschlüsselung Kryptographisches Verfahren, bei dem derselbe geheime Schlüssel (Private Key) für das Ver- und Entschlüsseln verwendet wird. Beispiel: DES.

System Kombination verschiedener Produkte in einer anwendungsspezifischen, realen Einsatzumgebung.

Systemadministrator Betreuer eines (dezentralen) Infomationsverarbeitungssystems innerhalb einer Hochschule.

Systembetreiber Betreiber von Informationsverarbeitungssystemen, wie z.B. das Hochschulrechenzentrum.

Systemmanagement Gesamtheit der Vorkehrungen und Aktivitäten zur Sicherstellung eines effektiven und effizienten Einsatzes von verteilten Systemen.

System-Zertifizierung *Siehe* Zertifizierung.

TACACS *Siehe* Terminal Access Controller Access Control System.

Tag Ein Tag ist ein kurzes zusätzliches Datenfeld, das die Information beinhaltet, zu welcher Verbindung ein Datenpaket gehört.

Talk Internet-Dienst, der analog zu IRC funktioniert, wobei hier allerdings nur zwei Partner miteinander kommunizieren.

TCB *Siehe* Trusted Computing Base.

TCP/IP Transmission Control Protocol / Internet Protocol. Übertragungsprotokolle auf Schicht 4/3 des ISO/OSI-Modells, auf denen die Internet-Dienste basieren.

TCPD *Siehe* TCP-Wrapper.

TCP-Wrapper Server-Programm, das die Namen und die IP-Adressen der anfragenden Rechner protokolliert und überprüft, ob diese berechtigt sind, den gewünschten Dienst in Anspruch zu nehmen; synonym: TCP-Daemon (TCPD).

TCSEC *Siehe* Trusted Computer System Evaluation Criteria.

Tele- Präfix für Netzanwendungen wie Telearbeit (Teleworking), Telebanking, Telefax, Telefonie, Telekonferenz, Telekooperation, Telelearning bzw. -teaching, Telemedizin, Teleshopping.

Telnet Internet-Dienst, der es ermöglicht, auf anderen Rechnern im Netz so zu arbeiten, als ob man direkt als Terminal angeschlossen wäre (Remote Login).

Terminal Access Controller Access Control System (TACACS) Authentifizierungsprotokoll, das für die Validierung bei Remote Access entwickelt wurde. Es erlaubt die zentrale Verwaltung von Benutzerkennungen und Passwörtern bei mehreren Einwählknoten.

Terminal-Adapter Umsetzeinrichtung zwischen Telefon- und Hochschulnetz.

Text Conferencing *Siehe* IRC, Talk.

TFTP *Siehe* Trivial File Transfer Protocol.

Ticket *Siehe* Kerberos.

Timeout Zeitspanne, nach der z.B. Versuche zur Verbindungsaufnahme im Netz oder inaktive Verbindungen automatisch abgebrochen werden.

TKG Telekommunikationsgesetz.

Tool Software-Werkzeug.

TP-Technik *Siehe* Twisted Pair.

Trivial File Transfer Protocol (TFTP) Sehr einfaches Protokoll zur Übertragung von Dateien, das auf einem unzuverlässigen Datagrammdienst von UDP basiert und bei dem keine Authentifizierung durchgeführt wird.

Trouble-Ticket-System (TT-System) Datenbankorientierte Verwaltung (Erstellen, Aktualisieren und Löschen) von Trouble-Tickets zu Netz- und Systemproblemen unter Verwendung allgemein verfügbarer Schnittstellen mit Auslösen von entsprechenden Aktionen (z.B. Versenden von E-Mail).

TrustCenter Ein TrustCenter ist ein Teil einer CA. Seine Hauptaufgaben sind die Erzeugung von Schlüsselpaaren und die sichere Übergabe an den Besitzer.

Trusted Computer System Evaluation Criteria (TCSEC) US-amerikanische Klasseneinteilung für Computersicherheit und Datenschutz im Internet; auch bekannt als „Orange Book“.

Trusted Computing Base (TCB) Zusammenfassung aller sicherheitsrelevanten Daten eines Systems zu einem Teilsystem, das von den restlichen Systemkomponenten abgeschottet ist.

TT-System *Siehe* Trouble-Ticket-System.

Tunnel Logischer Kanal zur Übertragung von Daten zwischen zwei Rechnern. *Siehe auch* Tunnelling.

Tunnelling Daten, die nach einem bestimmten Netzprotokoll zwischen zwei Rechnern ausgetauscht werden sollen, werden auf einem Teil des Verbindungswegs für die Übertragung in Pakete eines anderen Protokolls eingepackt.

Twisted Pair (TP) Art von Rechnervernetzung mit verdrillten Kupferkabeln.

Übertragungsprotokoll *Siehe* Protokoll.

Übertragungsrate Übertragene Datenmenge pro Zeiteinheit in bit/s oder Vielfachen davon.

UBR *Siehe* Unspecified Bit Rate.

UDP *Siehe* User Datagram Protocol.

Unautorisierter Zugang Zugang zu einem Rechner oder Netz ohne Benutzungsberechtigung.

Unicast-Paket Paket, das von einem Sender an einen Empfänger gesendet wird (Punkt-zu-Punkt-Nachricht).

Universalrechner Rechner, der im Gegensatz zu einem Server nicht spezialisiert ist und vielfältige Aufgaben bearbeiten kann.
Siehe auch Mainframe.

Unix Offenes Betriebssystem, für das Varianten aller gängigen Rechnerhersteller vorhanden sind, z.B. AIX (IBM), DG/UX (Data General), Digital UNIX (DEC), HP-UX (Hewlett Packard), Irix (SGI), Solaris (Sun), UNICOS (Cray).

Unix to Unix Copy Kommunikationsprogramm für den Austausch von Dateien und Aufträgen (Kommandos) zwischen UNIX-Systemen.

Unspecified Bit Rate (UBR) ATM-Service-Klasse, die für Dienste mit geringen Anforderungen an das Netz konzipiert ist. Es sind keine Flusskontrollmechanismen implementiert. Bei diesem Dienst dürfen Zellen ohne Einhaltung von bestimmten Bitraten gesendet werden. Das Netz garantiert nicht die Übertragung der Zellen und informiert auch nicht bei Zellverlusten.

URL Uniform Resource Locator. Einheitliche und eindeutige Bezeichnung von Dateien im WWW.

User Datagram Protocol (UDP) Übertragungsprotokoll auf Schicht 4 des ISO/OSI-Modells. UDP arbeitet verbindungslos auf Datagramm-Basis.
Siehe auch TCP/IP.

UUCP *Siehe* UNIX to UNIX Copy.

Variable Bit Rate (VBR) ATM-Service-Klasse, die eine variable Übertragungsrate mit Parametern für Durchschnitts- und Spitzenwerte unterstützt. Dabei wird unterschieden zwischen:
– Real-Time Variable Bit Rate (rt-VBR) für Sprache und Daten,
– Non-Real-Time Variable Bit Rate (nrt-VBR) für verbindungsorientierten Datenverkehr.

VBR *Siehe* Variable Bit Rate.

VC *Siehe* Virtual Channel.

Vektorrechner Spezieller Hochleistungsrechner.

Vermittlungsrechner *Siehe* Router.

Verschlüsselung *Siehe* Kryptographische Verfahren.

VEU Verordnung über Elektronische Unterschrift.

Video- und Audio-Kommunikation Kommunikation mit Bewegtbild und Ton.

Videokonferenz Im ISDN stehen bereits Videokonferenzdienste zur Verfügung. Für den späteren Einsatz eines Videokonferenzsystems in allen Arbeitskreisen der bayerischen Hochschulrechenzentren wurde 1996 das Projekt „Telekonferenz der Bayerischen Rechenzentrumsleiter“ gestartet.

Viren Bösartige Miniprogramme, die sich hinter harmlosen Dateien verbergen und die von einem portablen Datenträger oder dem Netz unbeabsichtigt geladen werden können. Sie können den Betrieb eines Computers erheblich beeinflussen oder ihn sogar lahmlegen.

Virenscanner Schutzprogramm, das Viren-Infektionen verhindert und/oder beseitigt.

Virenwächter Integriertes Schutzprogramm, das die aus dem Netz empfangenen Dateien automatisch auf Virenbefall untersucht.

Virtual Channel (VC) Ein virtueller Kanal ist eine logische, unidirektionale Übermittlungseinrichtung.

Virtual Local Area Network (VLAN) Virtuelle lokale Netze (VLANs) dienen zur logischen Verknüpfung von Netzteilnehmern zu dynamischen Arbeitsgruppen innerhalb eines physischen Netzes.

Virtual Path (VP) Ein virtueller Pfad ist eine logische, unidirektionale Übermittlungstrasse, auf der mehrere VCs definiert sein können.

Virtuelles Privates Netz (VPN) Zusammenschluss privater Netzinseln über verschlüsselte Verbindungen, die über ein öffentliches Netz geführt werden. *Siehe auch* CN.

VLAN *Siehe* Virtual Local Area Network.

VP *Siehe* Virtual Path.

VPN *Siehe* Virtuelles Privates Netz.

VT100 Terminaltyp, der von den meisten Servern und Kommunikationsprogrammen unterstützt wird.

Wähleingänge Zugangsleitungen von einem öffentlichen Netz z.B. in ein Hochschulnetz für die Nutzung von DV-Ressourcen vom häuslichen Arbeitsplatzrechner aus (digitaler Zugang über das ISDN-Netz oder analoger Zugang mittels Modem über das Telefonnetz).

WAIS *Siehe* Wide Area Information Service.

Wallet „Digitale Brieftasche“ z.B. für elektronische Form von Personalausweis, Führerschein, Geldbörse, Signierfunktion. Hier eingeschränkt auf portable Hardware (taschenrechnergroße Computer) mit virtuellen Realisierungen wichtiger Funktionen (z.B. Personalausweis, Geld, Kreditkarte, integriertem elektronischen Schlüssel für Challenge-Response-Verfahren).

WAN *Siehe* Wide Area Network.

WAP Wissenschaftler-Arbeitsplatzrechner-Programm im Rahmen des HBFG, das die Ausstattung der Wissenschaftler an den Hochschulen mit vernetzten Arbeitsplatzrechnern zum Ziel hat.

Whiteboard Elektronisches Zeichenbrett für das Joint Editing in Telekooperationssystemen.

Whois Internet-Dienst, der die Recherche nach Benutzer- und Rechnernamen ermöglicht, wobei pro Recherche nur innerhalb einer Domain gesucht werden kann, da ein Whois-Server nur eine Domain verwaltet.

Wide Area Information Service (WAIS) Mit dem Dienst WAIS kann im Internet in verschiedenen Datenbanken nach bestimmten Stichwörtern gesucht werden.

Wide Area Network (WAN) Weitverkehrsnetz.

WiN *Siehe* Wissenschaftsnetz.

Windows *Siehe* MS WINDOWS.

WiN-Shuttle Vom DFN-Verein betriebene Wähleingänge ins WiN bspw. für den Zugang von Schulen.

Wissenschaftsnetz (WiN) Datennetz für die Wissenschafts- und Bildungseinrichtungen in Deutschland, welches vom DFN-Verein organisiert wird. Das konventionelle („Schmalband-“)WiN basiert auf X.25, das neue Breitband-WiN auf ATM. Das Wissenschaftsnetz ist Teil des Internet.

Workflow-Management-System Methode, um Arbeitsabläufe und den Informationsfluss innerhalb eines Unternehmens durchgängig und flexibel zu steuern. Spezielle Netzsoftware unterstützt diese Form der Arbeitsorganisation.

WorldWideWeb (WWW) Verteilter, elektronischer Informationsdienst im Internet unter Verwendung von HyperLinks.

WWW *Siehe* WorldWideWeb.

WWW-Client Programm („Browser“), mit dem Dokumente im WWW gesichtet werden können, z.B. Mosaic, Netscape, Internet Explorer.

WWW-Server Dedizierter Rechner für den WWW-Dienst.

X.25 Protokoll zur paketvermittelnden Datenübertragung, das in Deutschland bei Datex-P und im (konventionellen) Wissenschaftsnetz verwendet wird.

X.400 Neben SMTP weiterer Standard für den Austausch von E-Mail-Nachrichten (Message Handling System).

X.500 Standard für einen verteilten Verzeichnis-Dienst in Netzen (X.500-Directory-Service oder X.500-DS).
Beispiel: AMBIX-D.

X/OPEN Vereinigung führender DV-Hersteller mit dem Ziel, eine einheitliche Anwendungsumgebung für portierbare, herstellerunabhängige Software zu definieren (z.B. durch Vereinheitlichung von UNIX).

X-Window Das X-Window-System ist eine grafische Benutzeroberfläche mit Fenstertechnik.

Yellow Pages (YP) Ursprünglicher Name des Network Information Service (NIS). Der Name wurde aus Urheberrechtsgründen geändert.

YP *Siehe* Yellow Pages.

Zertifizierung Technische Prüfung und Abnahme von technischen Einrichtungen und deren Anwendungen nach bestimmten Kriterien im Hinblick auf das Sicherheitsniveau, z.B. Zertifizierung eines Firewall-Systems. Man unterscheidet Produkt- und System-Zertifizierung.

ZSI Zentralstelle für Sicherheit in der Informationstechnik.

Zugangscode *Siehe* Passwort.

Stichwortverzeichnis

S