

5. Sicherheitsmechanismen im Universitäts-Netz (Stand und Ausblick)

5.1. Einleitung

Eine Studie der NCSA ergab, daß Unternehmen mit Internet-Zugang achtmal so stark durch Daten-Angriffe gefährdet sind wie Unternehmen, die das Internet nicht nutzen [Zapp]. Zudem ermittelt das CERT eine wachsende Zahl von Computerdelikten. Hinzu kommt die Dunkelziffer betroffener Unternehmen, die aus Image-Gründen auf eine Meldung des Schadens verzichten.

Universitäten müssen einen freien Zugang zum Internet gewähren. Tatsächlich gehen jedoch nach bisherigen Erfahrungen 90% der Hack-Versuche von solchen freien Gemeinschaften aus [CHE96]. Auch Universitäten nutzen Computer-Systeme, die definitiv schutzbedürftig sind, z.B. in der Verwaltung, und manche Studenten haben Zeit und Motivation genug, beispielsweise Zugang zu Gehalts-, Matrikel- und besonders zu Notenlisten zu suchen.

Daher muß die Frage nach geeigneten Sicherheitsmechanismen ganz besonders auch bei Universitäten gestellt werden.

In diesem Kapitel kann nur eine Grobanalyse der im Universitätsnetz vorhandenen Sicherheitsmechanismen vorgenommen werden, d.h. den Ist-Zustand zu untersuchen, diesen zu bewerten und daraus eine Folgerung für eine Soll-Konzeption abzuleiten.

Gründlicher als die klassische Ist-Soll-Analyse fällt jedoch eine Szenario-Studie aus, in der nicht nur technische sondern auch die weitaus kritischeren organisatorischen Mängel eingehender untersucht werden. Letztere nehmen internationalen Studien zufolge 85% aller auftretenden Sicherheitsmängel ein. Im Rahmen des DFN werden Sicherheitsprojekte an Universitäten unter Zusammenschluß von mehreren internen Wissensträgern und externen Sicherheitsfachleuten über eine Laufzeit von mehreren Jahren durchgeführt. Innerhalb dieser Projekte werden dann regelmäßig u.a. sog. Szenarien-Workshops durchgeführt. Dieses Beispiel soll die ganze Komplexität der IT-Sicherheit verdeutlichen.

Die Anforderungen der Nutzer der drei Teilnetze des RUN sind bezüglich der Performance und der Security unterschiedlich. Daher erfolgt die Analyse getrennt für alle drei Netze. Im Anschluß der jeweiligen Teilanalyse werden jeweils sinnvolle Lösungsansätze vermittelt. Den Abschluß bilden allgemeingültige Empfehlungen.

Dies soll jedoch nicht darüber hinwegtäuschen, daß alle drei Teilnetze sich gegenseitig bedingen und ergänzen. Werden notwendige Sicherheitsvorkehrungen im Hochschulnetz unterlassen, so hat dies gleichzeitig Einfluß auf die Sicherheitsgrad der anzuschließenden Teilnetze von Verwaltung und Medizin.

5.2. Hochschulnetz

5.2.1. Funktionalitäten und Sicherheitsanforderungen

Die Universität und speziell das Rechenzentrum sieht ihre primäre Aufgabe in der Offenheit gegenüber:

1. Studenten, Professoren und wissenschaftliche Mitarbeiter, die zum Zwecke des Studiums und der Forschung über Wählleitungen oder direkt auf die Ressourcen der Hochschule und speziell des Rechenzentrums zugreifen müssen
2. Firmen, Forschungs- und Bildungseinrichtungen, die über das Internet mit der Universität kommunizieren

Das heißt, sie muß vor allem eine hohe Verfügbarkeit gegenüber dem Nutzer gewährleisten, und dies bei größtmöglicher Performance. Die Sicherheitsanforderungen werden momentan noch als gering angesehen, da keine sicherheitsrelevanten Daten verwaltet werden, zumindest solange noch keine zentralen File-, Backup- und Archivserver im Einsatz sind.

Fazit: Die technischen Maßnahmen zur Erhöhung der Sicherheit gegenüber unbefugten Zugriffen dürfen die Performance (Reaktionszeiten, Durchsatz) des Datenverkehrs nicht wesentlich verschlechtern.

5.2.2. Realisierung der Funktionalitäten und Sicherheitsanalyse

Bild 5-1 zeigt die bereits zum Teil realisierte Netzstruktur des Hochschulnetzes.

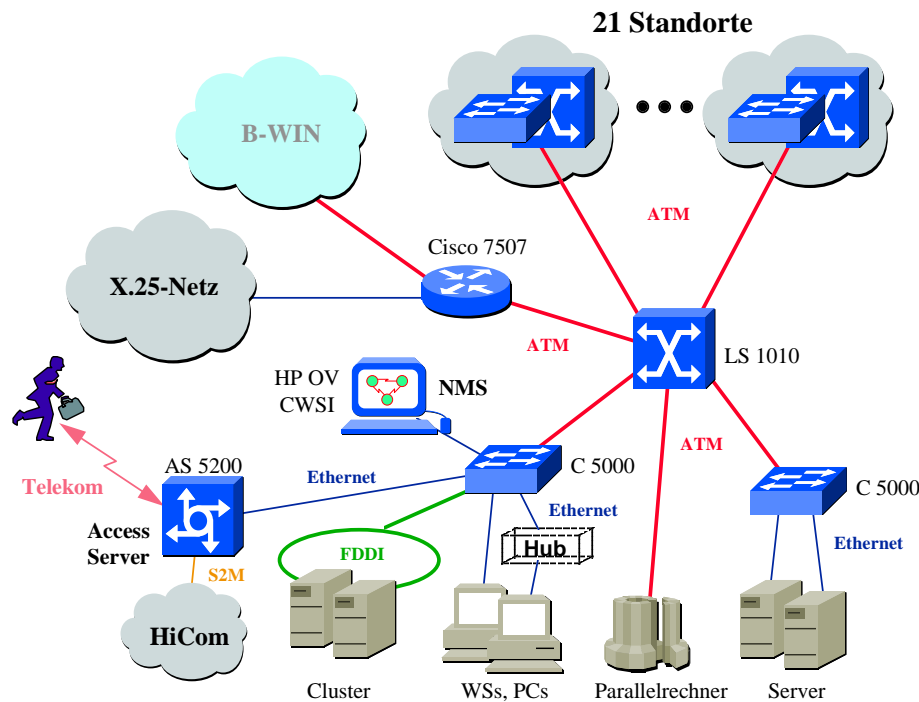


Bild 5-1 : Im Aufbau befindliche Struktur des Hochschulnetzes

Ein potentieller Angreifer hat damit gleich drei Zugangs-Schnittstellen:

1. Zugang über das Internet
2. Zugang über das Wählnetz
3. Direkter Zugang innerhalb des Netzes

Diesen Gefahren wird mit folgenden bereits verfügbaren Mitteln begegnet, wobei das für die Cisco-Komponenten Gesagte prinzipiell auch für die beiden anderen Teilnetze anzuwenden ist:

Die Überführung der bisherigen Subnetze in VLANs hat immense Sicherheitsvorteile. Die VLANs sind im eigentlichen Sinne geschlossene Benutzergruppen, d.h. die Teilnehmer eines VLANs können nur mit denen eines anderen VLANs kommunizieren, zu dem auch ein Verbindungsweg durch den Router definiert worden ist, diese Definition erfolgt auf Basis von Access Lists. Beispiel hierfür sind die Steuerinterfaces der Cisco-Komponenten, die alle ein- und demselben VLAN des Administrators zugeordnet werden können, dieses ist jedoch von anderen VLANs nicht zugänglich (Routing disabled).

Der zentrale Router Cisco 7507 am Ausgang zum B-WIN übernimmt bereits eine Filterungsfunktion per Access Lists. So sind die Dienste TFTP und SNMP nach außen verbarrikiert, da es erstens keinen Grund für eine globale Bereitstellung gibt und zweitens diese eine mangelhafte Sicherheitsfunktionen implementiert haben [Frisch].

TFTP wird hauptsächlich zum Booten von Workstations über das Netzwerk und zur Routerkonfiguration verwendet. Es enthält jedoch keinerlei Authentifikation, d.h. jeder erhält Zugriff, ohne Benutzername oder Paßwort anzugeben.

SNMP übernimmt den Transport von Management-Informationen. Es verfügt nur über eine geringe Authentifikation, die unverschlüsselt über das Netz übertragen wird (siehe Kapitel 4.3.2.).

Datenpakete, die von außen am Routerport ankommen, aber nicht an die Domäne „uni-rostock.de“ adressiert sind, werden ungelesen vom Router verworfen.

Nach außen hin erlaubt sind Dienste wie FTP, HTTP,SMTP, NNTP, Gopher, Telnet etc..

Der Zugang zu den verschiedenen Netzressourcen im Rechenzentrum ist nur den dafür befugten Personen per zentral vergebenem Account gestattet. Die Zugangsdaten aller Uni-Angehörigen werden dabei von einem zentralen UNIX-Server verwaltet. Dieser Account besteht üblicherweise aus einer Kennung und einem dauerhaften Paßwort. Diese können jedoch, gerade bei Studenten, leicht weitergegeben werden. Auf dieses Problem wurde in Kapitel 4.3. hingewiesen.

Die durch das Cisco-eigene Betriebssystem IOS auf den zentralen Netzkomponenten (ATM-Switches, LAN-Switches, Router) ermöglichte Sicherheit basiert in erster Linie auf der Steuerung der Paßwort-Vergabe. Dieser Paßwort-Schutz erfolgt auf zwei Ebenen:

1. Login-Paßwort zum Öffnen des Ports (LAN-, Konsolen- und AUX-Port) für Zugriffe über SNMP, FTP, Telnet u.ä.
2. Enable-Paßwort (MD5-verschlüsselt) für Zugriff auf Konfiguration etc. (diese Paßwörter können nach Lese- und Schreibrecht differenziert werden)

Der Zugriff ist nach Port und Zugriffsrecht differenzierbar.

Beispiel ist der Zugriff auf den SNMP-Agent eines Switches oder Routers, per entfernter NMS-Station (Remote) oder per an den Service-Port angeschlossenen Terminals (Local) über Telnet.

Weiterhin sind mit einem kommenden Upgrade für den LAN-Switch Catalyst 5000 zusätzliche Sicherheitsfunktionen pro Port integriert, wie dies bereits beim Catalyst 3000 vollzogen ist. Für jeden Ethernet-Port werden dann Listen von zugelassenen MAC-Adressen geführt. MAC-Adressen sind individuell und pro Hardwarekomponente weltweit einmalig.

Wird eine System mit unbekannter MAC-Adresse an den Port geschaltet, wird dieser Port des LAN-Switches innerhalb von wenigen Sekunden abgeschaltet sowie ein SNMP-Trap zur Alarmierung an die Netzmanagement-Station gesendet. Beim ATM-Switch LightStream 1010 ist dieser Schutzmechanismus bereits implementiert, auf der Basis von zugelassenen ATM-Adressen pro Port.

Für das herstellerübergreifende Netzmanagement mit HP-OpenView erfolgt der Zugriff auf das NMS über Paßwörter mit abgestufter Rechtevergabe:

- Read Only (Nur Lesen)
- Read/Write (Lesen und Schreiben)
- Supervisor (uneingeschränkt)

Ein zusätzlicher Schutz wird momentan geschaffen durch die physische Zugangskontrolle: so werden alle NMS-Stationen in einen abgetrennten Raum verlagert.

Momentan noch sicherheitskritisch sind die Einwahlpunkte am Annex-Server über das Netz der Deutschen Telekom AG. Hier wird neben dem relativ sicheren PPP-Protokoll noch das SLIP-Protokoll unterstützt, das über keinerlei Adreßinformationen verfügt. Die Paßwortübermittlung erfolgt über die Einwählleitung über ein unverschlüsseltes ASCII-File und wird erst bei der Weiterleitung zur Abfrage zwischen Annex- und UNIX-Server innerhalb des Uni-Netzes verschlüsselt.

Eine Ablösung des Annex-Servers durch einen Access-Server Cisco AS5200 ist bereits geplant (siehe [Anlage 5]). Neben der Erhöhung der Einwahlkapazität hat dies noch zusätzliche Vorteile bezüglich der Sicherheit. Der Access Server Cisco AS5200 ist eine Kombination aus Modems (analog u. digital) und einem Router. Hier wird neben einer starken Authentifikation auch die Rechtevergabe gesteuert, und zwar auf der Grundlage von Access Lists. Der sicheren Authentifikation dienen vom AS5200 unterstützte Sicherheitsfeatures wie PAP/CHAP (verschlüsselte Übertragung von Nutzernamen und Paßwort) und Callback (Authentifikation mittels Verbindungsaufbau durch den Gerufenen). Letzteres kann jedoch im Hochschulnetz nicht eingesetzt werden, da eine Übernahme der Telefonkosten durch die Hochschule nicht möglich ist.

Standardmäßig unterstützt werden die Protokolle TACACS+ und RADIUS, so daß eine Ergänzung durch einen externen Server (Beispiel: CiscoSecure) vorgesehen werden kann sowie eine Integration in das zentrale Netzmanagement gewährleistet wird.

Zielsetzung der Universität ist die Übernahme der Account-Listen vom o.g. UNIX-Server (evtl. auf einen NT-Server). Aus Gründen der NT-Kompatibilität ist daher auch ein Access Server der Firma Shiva im Gespräch, der wiederum keine Unterstützung von IOS, Netzmanagement etc. bietet und daher einen erhöhten Verwaltungsaufwand bedingt (-> erhöhtes Sicherheitsrisiko).

5.2.3. Sicherheitsempfehlungen

Alle nachfolgenden Lösungsansätze zielen darauf, die Struktur eines vollständig gewitchten Backbone-Netzes, in dem die Nutzer vollständig über die Standorte verteilt sind, beizubehalten. Ansonsten wäre der angestrebte Nutzen einer übergreifenden VLAN-Struktur sowie eines einheitlichen Netzmanagements in Frage gestellt.

Screening Router

Der zentrale Router Cisco 7507 hat neben seiner primären Routing-Funktion für das gesamte RUN Filterungsfunktionen zu erfüllen. Dies kann aus zweierlei Sicht nicht befriedigen. Zum einen wird die Performance bei einer Ausweitung der Filterlisten erheblich beeinträchtigt. Zum anderen steht einem Angreifer bei Überwindung dieses Routers das gesamte innere Hochschulnetz offen. Gelingt es ihm gar, den Router herunterzufahren, ist die universitätsweite Kommunikation verhindert (da der Router gleichzeitig die heterogene Netzstruktur verknüpft).

Die Empfehlung zur Entlastung ist zunächst ein zusätzlicher Screening Router, der eine reine Filterungsfunktion ausführt (siehe Kapitel 4.4.1.). Zwingend ist jedoch eine volle Kompatibilität mit dem WIN-Router, es genügt wegen der ausschließlichen Filterungsfunktion ein Cisco-Router mit einer geringeren Performance als der des Cisco 7507, z.B. ein Cisco 4500 (siehe [Anlage 4]).

Firewall

Da ein reines Packet Filtering angesichts der geplanten Implementierung von File- und Backup-Servern in das Hochschulnetz als unzureichend anzusehen ist, andererseits jedoch ein reiner Application Level Gateway die Performance auf einen unakzeptablen Wert senken würde, ist ein Kompromiß zu suchen.

Empfohlen wird der Einsatz des Cisco PIX-Firewalls neben seiner IOS-Kompatibilität aus folgenden Gründen (siehe auch Kapitel 4.4.9. sowie [Anlage 8]):

Der PIX ermöglicht eine vollständige Verdeckung der inneren Netzstruktur nach außen hin, dies wird durch die in Kapitel 4.4.4. beschriebene NAT ermöglicht. Dabei kann zwischen der dynamischen (Pool von möglichen Adressen) Adreßumsetzung und der statischen (Eins-zu-Eins) gewählt werden, je nachdem, ob bestimmte Verbindungen von außen zugänglich sein sollen. (Dies ist nicht mit den Angaben anderer Firewall-Hersteller zu verwechseln, die bereits die statische Adreßumsetzung bei einer Gateway-Lösung (zwei Interfaces) als NAT ihrer Software spezifizieren.)

Zudem wird mit der neuen Version die Cut-Through Proxy-Technologie unterstützt. Diese realisiert eine Authentifikation des Users auf der Anwendungsebene und schaltet bei erfolgreicher Authentifikation die Verbindung auf Netwerkebene durch, was sich positiv auf den Durchsatz auswirkt. So werden bis zu 16000 simultane Verbindungen ermöglicht, bei einem Durchsatz von 46 Mbit/s. Letzteres ist bei dem 34 Mbit/s-Anschluß an das B-WIN derzeit völlig ausreichend. Wird der Anschluß im kommenden Jahr auf 155 Mbit/s erweitert, so ist es möglich, mehrere PIX-Firewalls zur Erhöhung des Durchsatzes über Fast Ethernet parallelzuschalten.

Der PIX setzt nicht auf das unsichere UNIX-Betriebssystem auf, sondern auf einen eigenen Echtzeit-Kernel.

Angesprochen wurde bereits, daß ein hoher Verwaltungsaufwand nicht nur immense Kosten verursacht, sondern auch die Fehlerwahrscheinlichkeit erhöht. Beim PIX genügt ein einmaliger Setup, der übersichtlich über ein auf dem HTML-Format (wie bei Web-Browsern) basierendes Graphical User Interface (GUI) erfolgen kann. Eine fortlaufende Verwaltung entfällt.

Schließlich ist es im Gegensatz zu anderen Firewall-Produkten nicht nötig, sich durch regelmäßige Software-Updates an den jeweils aktuellen Stand von Internet-Diensten und Angreifern anzupassen. Die PIX-Lösung ist fast ausschließlich hardwarebasiert und daher performanter sowie schlechter ausschalt- oder manipulierbar (PIX: wenige zehn Kilobytes, andere: mehrere Megabytes Software) .

Demilitarisierte Zone

Durch den Einsatz von Screening Router und Firewall bietet sich zur weiteren Sicherheitserhöhung die Bildung einer DMZ an, in der die frei zugänglichen Informationsserver angeordnet werden, dazu zählen Mail-, News-, WWW-, Gopher- und FTP-Server (siehe Kapitel 4.4.5.).

Der Screening Router wird dabei so konfiguriert, daß lediglich Verbindungen zu den wenigen dedizierten Servern in der DMZ und dem PIX möglich sind. Der PIX erhält hingegen nur zwei Ansprechpartner: innen den Cisco 7507 und außen den Screening Router.

Eine weitere Erhöhung der Sicherheit kann durch die Benutzung von zwei DNS-Servern erreicht werden (was jedoch auch mit einem erhöhten Aufwand verbunden ist). DNS-Server dienen der Zuordnung von numerischen IP-Adressen zu den besser handhabbaren Domain-Namen und dienen wegen der umfangreichen Informationen über die innere Netzstruktur als begehrte Angriffsziele. Der interne Server, der die vollständigen Zonen-Daten beinhaltet, sollte im inneren Netz installiert werden und der externe DNS-Server in der äußeren Zone (DMZ). Der externe DNS-Server enthält lediglich stark verkürzte Zonen-Dateien, die keinerlei vertrauliche, interne Informationen enthalten. Wird nun an den internen DNS-Server eine Anfrage betreffend einer externen Internet-Adresse gestellt, so leitet dieser diese Anfrage an den externen DNS-Server weiter, der sie wiederum an einen der DNS-Root-Server des Internet vermittelt.

Bild 5-2 zeigt eine mögliche Realisierung der bisher genannten Empfehlungen.

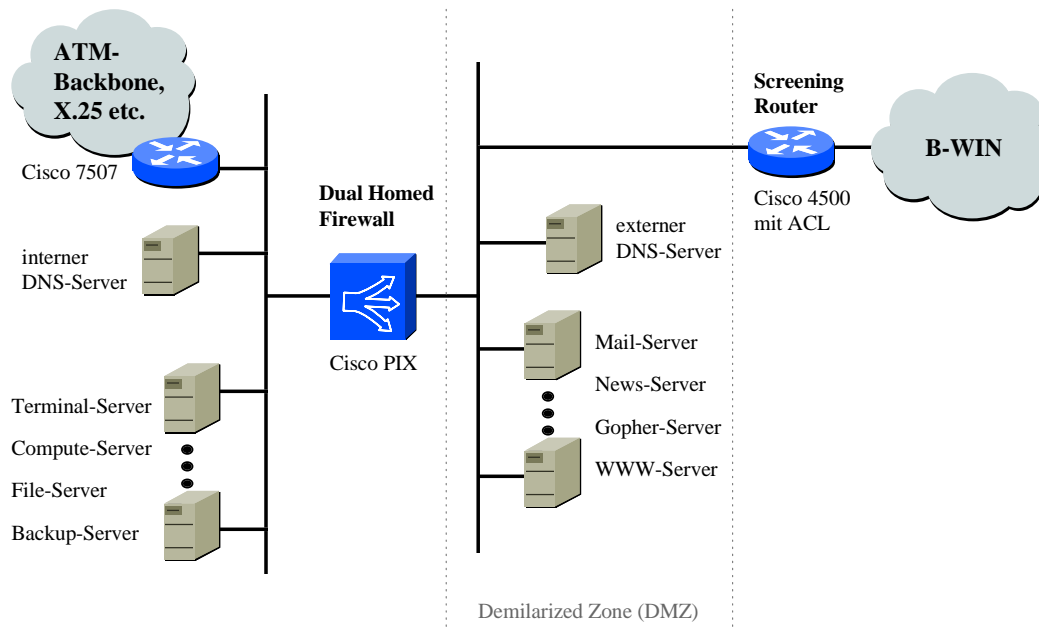


Bild 5-2 : Bildung einer DMZ mit Screening Router, Firewall und dedizierten Servern

Offensichtlich ist, daß die Anbindung des Access Servers in der DMZ wenig Sinn ergibt, auch wenn solche Einwählpunkte beliebte Angriffsziele bilden. Den sich einwählenden Anwendern (darunter Fachbereiche) müßte im Gegensatz zu den Internet-Nutzern eine Reihe von Zugriffsrechten zugestanden werden. Diese würden die Konfiguration eines offenen Pfades im Dual Homed Firewall notwendig machen, der wiederum eine Schleuse für Internet-Nutzer bieten würde.

Zentrales Sicherheits-Management

Ein weiterer wichtiger Punkt ist die Verwaltung der Zugangsrechte im Netz. Diese muß auf einen Punkt konzentriert werden, da erfahrungsgemäß eine Pflege mehrerer Datenbanken mit der gleichen Sorgfalt nicht über einen längeren Zeitraum möglich ist.

Empfohlen wird ein eigener Server, der die Verwaltung der Router, des Access Servers und des PIX auf einem sicheren Kommunikationspfad übernimmt. Voraussetzung ist die Kompatibilität mit dem Cisco-IOS-System.

Die bestmögliche Kompatibilität und Sicherheit bietet Cisco Secure, ein auf dem TACACS+-Protokoll basierendes Verwaltungssystem. CiscoSecure ist ein Anwendungsprogramm, das auf einer SUN SPARC-Workstation implementiert wird (siehe [Anlage 8]). Durch das integrierte grafische Oberfläche (GUI) kann der Administrator Datenbanken kreieren, die die Netzwerk-User und deren Privilegien definieren. Dabei können User mit gleichen Rechten (z.B. Studenten einer Fakultät) komfortablerweise auch baumhierarchieartig zu User-Gruppen zusammengefaßt werden (Bild 5-3):

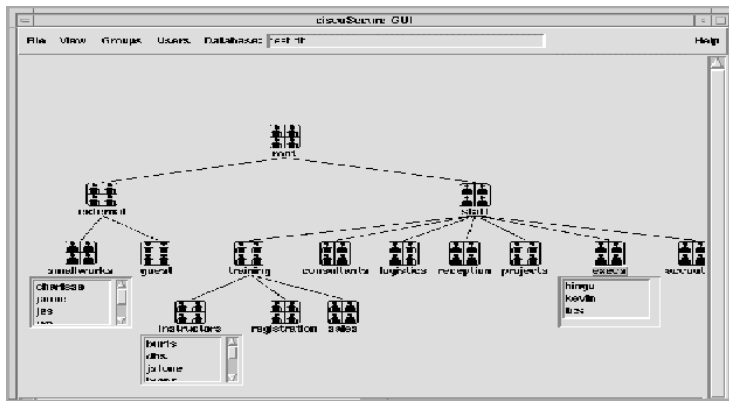


Bild 5-3 : GUI-Bildschirm von CiscoSecure

Die Kommunikation zwischen Server und den Access-Komponenten erfolgt verschlüsselt über das bereits in Kapitel 4 beschriebene TACACS+-Protokoll (siehe Bild 5-4 sowie [Anlage 7]).

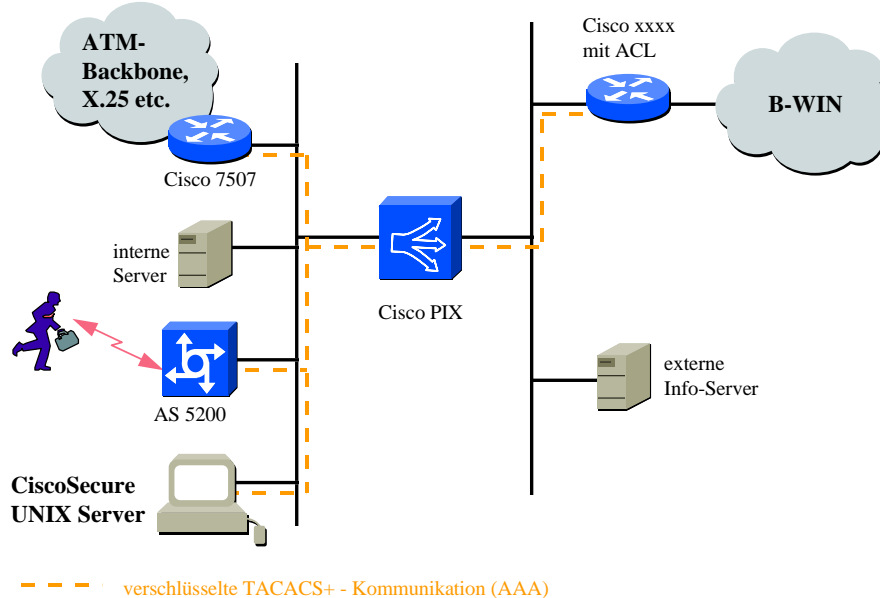


Bild 5-4 : Einsatz einer zentralen Nutzerrechte-Verwaltung

Desweiteren wird es so ermöglicht, die in den Routern begrenzt implementierten Audit-Möglichkeiten wesentlich zu erweitern, dazu zählt die Protokollierung von User-Daten, Zeit-Daten, Statistiken etc.. Dies ist in gewissem Maße zwar auch über das NMS möglich, solange das Netzmanagement jedoch auf dem unsicheren SNMP-Standard basiert, wird empfohlen, die Verwaltung der Router ausschließlich über das CiscoSecure vorzunehmen.

Zugangskontrolle bei Fernadministration

Im Zuge des Aufbaus des Hochschulnetzes kristallisiert sich der Zustand heraus, daß einige wenige Mitarbeiter das nötige Wissen um die Wartung und Fehlerbehebung an der Netztechnik erhalten.

Durch diese Spezialisierung ergibt sich die Notwendigkeit einer ständigen Verfügbarkeit derjenigen Mitarbeiter, um beispielsweise Notsituationen wie Ausfälle auch von einem entfernten Standort (z.B. von zu Hause) aus beheben zu können.

Da in diesem Zusammenhang den Administratoren umfangreiche Konfigurationsrechte zugewiesen werden müssen, wird einer sicheren Zugangskontrolle wesentliche Bedeutung beigemessen.

Die mit dem eingangs beschriebenen Paßwort-Zugängen verbundenen Risiken können durch die Anwendung von Token Cards minimiert werden (siehe Kapitel 4.3.1.).

Die Firma Security Dynamics ist führend auf diesem Gebiet und bietet sowohl Token Cards als auch die zugehörige Verwaltungssoftware an (siehe [Anlage 10]). Dabei bietet sie eine weitgehende Kompatibilität ihrer Systeme sowohl mit allen gängigen Firewall-Systemen als auch mit dem von allen Cisco-Komponenten unterstützten TACACS-Protokoll. Dank der TACACS-Unterstützung braucht sich der Administrator nicht unbedingt direkt im Hochschulnetz zu befinden, sondern er kann auch kontrollierten Zugang über Einwählserver (Cisco-Access Server) oder das Internet (Cisco-Router) erhalten (siehe Bild 5-5). Damit wird der erforderlichen Flexibilität der Administratoren Rechnung getragen.

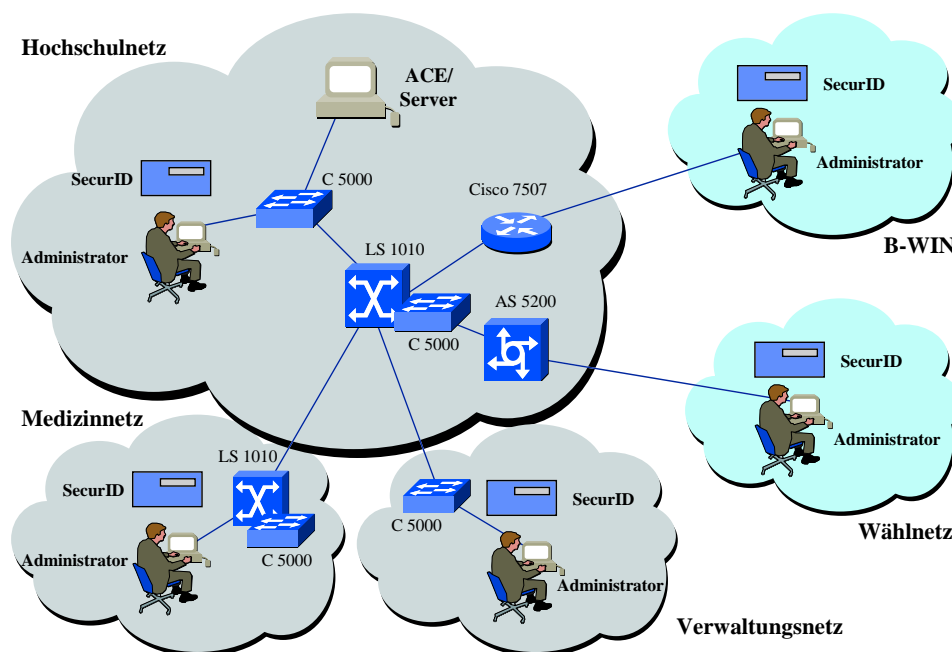


Bild 5-5 : Möglichkeiten des Zugriffs mittels Token Cards

Jeder Administrator erhält seine persönliche SecurID-Karte, die durch einen individuellen Algorithmus generierte (sich z.B. alle 60 Sekunden ändernden) Codes ausgibt. Wünscht derjenige einen Login, gibt er die Kombination aus seiner PIN und dem generierten Code an seinem jeweiligem System ein. Diese Information wird mittels TACACS automatisch an die im Host-Server implementierte ACE/Server-Software gesendet. Der Server überprüft die Authentizität des Users,

indem er mit Hilfe einer Kopie des benutzerspezifischen Algorithmus das erwartete Ergebnis berechnet und bei Übereinstimmung den Zugriff auf das Netzwerk bzw. die betreffende Komponente gestattet.

Gelangt ein Angreifer in den Besitz einer Token Card, nützt ihm das genauso wenig, wie als wenn er die PIN aufschnappt, aber nicht die zugehörige Token Card besitzt. Genauso verhält es sich beim Abhören oder Ausprobieren der PIN/Code-Kombination, da diese nur für einige Sekunden bzw. die laufende Session gilt.

Zu überlegen wäre sogar eine netzüberschreitende Verantwortlichkeit der Administratoren, d.h. daß dieses Zugangssystem von Hochschule, Verwaltung und Medizin gleichermaßen genutzt wird. Da der Backbone letztendlich eine Einheit bildet und mögliche Fehler nicht unbedingt im jeweiligen Teilnetz zu suchen sind (z.B. bei Ausfall des zentralen Routers), ist diese Vorgehensweise dringend anzuraten.

5.3. Verwaltungsnetz

5.3.1. Funktionalitäten und Sicherheitsanforderungen

Die Hochschulverwaltung steht bei jeglicher Form der DV-mäßigen Abwicklung ihrer Aufgaben vor den Problemen des Datenschutzes und der Datensicherheit.

Die Arbeitsgruppe Datenschutz und -sicherheit des Deutschen Forschungsnetzes hat eine Klassifizierung schutzbedürftiger Belange in der Hochschulverwaltung vorgenommen. Bei der Festlegung und Beschreibung der Schutzstufen wurde eine Unterscheidung hinsichtlich der beiden Gesichtspunkte Datenschutz und Verfahrens-/Datensicherheit vorgenommen. Die Ergebnisse sind in den Tabellen 5-1 und 5-2 zusammengefaßt [DFN95].

Stufe	Definition
A	frei zugängliche Daten, in die jedem Einsicht gewährt wird, ohne daß er ein berechtigtes Interesse geltend machen muß
B	Personenbezogene Daten, deren Mißbrauch keine besondere Beeinträchtigung erwarten läßt; der Einsichtnehmende muß jedoch ein berechtigtes Interesse haben
C	Personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner rechtlichen sowie beruflichen Stellung beeinträchtigen kann
D	Personenbezogene Daten, deren Mißbrauch den Betroffenen in seiner rechtlichen sowie beruflichen Stellung erheblich beeinträchtigen kann

E	Daten, deren Mißbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann (entfällt in der Regel)
---	---

Tabelle 5-1 : Klassifizierung hinsichtlich des Datenschutzes

Stufe	Definition
A	Daten, deren Modifizierung, Verlust oder Mißbrauch keine besondere Beeinträchtigung erwarten läßt; durch geringfügigen Zeit- oder Mitteleinsatz ausgleichbar
B	Daten, deren Modifizierung, Verlust oder Mißbrauch die Handlungsfähigkeit der Hochschule beeinträchtigt; durch vertretbaren Zeit- und Mitteleinsatz ausgleichbar
C	Daten, deren Modifizierung, Verlust oder Mißbrauch die Handlungsfähigkeit der Hochschule erheblich beeinträchtigt; durch erheblichen Zeit- und Mitteleinsatz ausgleichbar
D	Daten, deren Modifizierung, Verlust oder Mißbrauch die Handlungsfähigkeit der Hochschule gefährdet; durch umfangreichen, nicht kalkulierbaren Zeit- und Mitteleinsatz ausgleichbar
E	Daten, deren Modifizierung, Verlust oder Mißbrauch die Hochschule als solche gefährdet; Schadensbeseitigung nicht möglich bzw. nicht garantierbar (entfällt in der Regel)

Tabelle 5-2 : Klassifizierung hinsichtlich der Datensicherheit

Tabelle 5-3 beschreibt eine Zuordnung der in einer Hochschulverwaltung eingesetzten DV-Verfahren zu den jeweiligen Schutzstufen [DFN95].

Stufe	zugeordnete Verfahren	nach Datenschutz	nach Datensicherheit
A	Standard-, Büro- und Kommunikations-Software Kataloge in Hochschulbibliotheken	A A	A A
B	Adressenverwaltung Betriebssteuerung Gebäude-/Raumverwaltung Inventarisierung Kapazitätsberechnung Lagerverwaltung Lehrveranstaltungsplanung	A/B A A A A/B A A/B	B B B B B B B

	Telefonverzeichnis	A	B
C	Planungsverfahren	A/B	C
	Praxissemesterverwaltung	B/C	C
	Projekt-/Forschungsdatenbank	B/C	C
	Seminarplatzvergabe	B	C
	Stellenverwaltung/-bewirtschaftung	C	C
	Studentenverwaltung	C	C
	Hochschul- oder Personalratswahlen	B	C
D	Haushalts-/Kassenverfahren	B	D
	Personalverwaltung	D	D
	Prüfungsverwaltung	D	D
	Sicherheitsverwaltung	A/B	D
	Zulassungswesen	D	D
E	entfällt innerhalb der Hochschulverwaltung		

Tabelle 5-3 : Zuordnung von DV-Verfahren der Hochschulverwaltungen zu den Schutzstufen

5.3.2. Realisierung der Funktionalitäten

Das Netzsituation stellt sich momentan folgendermaßen dar [Wiener]: Die zentrale Verwaltung befindet sich, über mehrere aneinandergrenzende Gebäude verteilt, in der Innenstadt. Die dort befindlichen PCs sind über dedizierte Ethernetanschlüsse mit einem eigenen LAN-Switch Catalyst 5000 verbunden. Daneben existieren noch weitere PCs, die jedoch nicht vernetzt sind, da die darauf befindlichen Daten als besonders sensitiv eingestuft werden. Insgesamt sind etwa 100 PCs im Einsatz. Die zentralen Server sind ebenfalls über dedizierte Ethernetanschlüsse mit dem LAN-Switch verbunden. Darüberhinaus existiert noch eine LWL-Verbindung zum entfernten (neben dem URZ befindlichen) Dezernat Technik, wo ebenfalls PCs im Einsatz sind. Die Geschlossenheit des Netzes wird dadurch gewährleistet, daß der LAN-Switch noch nicht über den Uplink-Port mit dem Hochschulbackbone verbunden ist. Bild 5-6 liefert eine Schema des geschlossenen Verwaltungsnetzes.

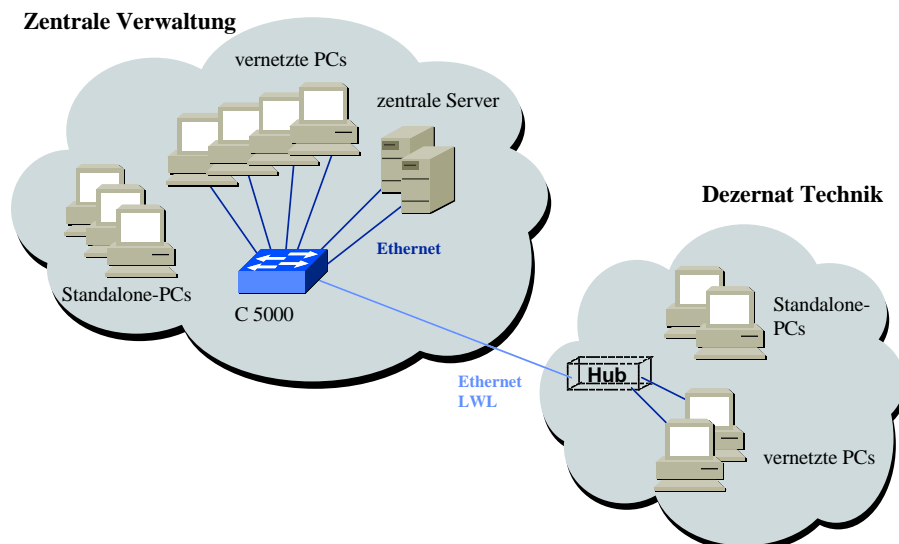


Bild 5-6 : Geschlossenes Netz der Verwaltung

Es gibt bereits Abteilungen innerhalb der Verwaltung, die auf einen Internetanschluß angewiesen sind, dazu zählen: der Transferbeauftragte, der Leiter Fernstudienwesen, das Dezernat Studium und Lehre, das Akademische Auslandsamt etc.. Diese sind mit PC-Arbeitsplätzen ausgerüstet, die über die Komponenten der Innenstadt mit dem Uni-Backbone verbunden sind. Eine elektronische Kommunikation mit dem Verwaltungsnetz ist jedoch nicht möglich.

5.3.3. Sicherheitsanalyse

Beim bisherigen Einsatz in sich geschlossener Host-Systeme mit direkt angeschlossenen Terminals ließen sich die Gefährdungspotentiale und daraus resultierenden Absicherungsverfahren noch recht genau definieren, einhalten und überwachen.

Bereits der Einsatz derselben DV-Verfahren in einem geschlossenen Verwaltungsnetz veränderte die Situation erheblich, da es zu einer Informations-, Bearbeitungs- und Datenverteilung kam. Beispiel hierfür ist die Verknüpfung einer Datenverarbeitung mit Textverarbeitungssystemen am PC.

Die Sicherheit konzentriert sich hier vorwiegend auf eine zentrale Paßwortvergabe durch den DV-Verantwortlichen. Diese Paßwörter sind dann für den jeweiligen Arbeitsplatz dauerhaft gültig. Dabei wird davon ausgegangen, daß der potentielle Angreifer nicht innerhalb, sondern im Hochschulnetz zu suchen ist. Die Begründung beruht auf der fehlenden Motivation und den hierfür fehlenden DV-Kenntnissen unter den Verwaltungs-Mitarbeitern.

Durch die sich überschneidenden Arbeitsgebiete ist es jedoch nicht auszuschließen, daß auf die gemeinsam verwalteten Daten, auch unbeabsichtigt, negativer Einfluß genommen werden kann.

Durch die Anbindung des derzeit noch geschlossenen Verwaltungsnetzes an das hochschulweite Backbone-Netz entstehen gravierende zusätzliche Probleme, da die Sicherheit vor Einsehbarkeit und Manipulierbarkeit von Daten und Programmen garantiert bleiben muß, obwohl dann die Transferwege vielfach außerhalb des Einflußbereiches der Verwaltung liegen.

5.3.4. Geplante Netzsituation

Die Anbindung des derzeit noch geschlossenen Verwaltungsnetzes an das hochschulweite Backbone-Netz ergibt sich in zunehmendem Maße vor allem aus folgenden Erfordernissen und Entwicklungen:

- Einsatz von DV-Verfahren, die sowohl seitens der Verwaltung als auch der Wissenschaft auf die gleiche Software zugreifen (z.B. File-Server des Rechenzentrums)
- hochschulweite Nutzung übergreifender und/oder teurer Ressourcen wie Mail-, Fax- und Informations-Systeme (z.B. SMTP und WWW über das B-WIN)

- Verknüpfung der über das Hochschulnetz verteilten Verwaltungsstandorte (z.B. Büros und Sekretariate, Dezernat Technik)
- Zusammenarbeit mit landesweiten Hochschulverwaltungen, hochschulnahen Institutionen und öffentlichen Einrichtungen sowie Kooperation mit Firmen

Da die Verwaltung zum jetzigen Zeitpunkt keinerlei zwingende Erfordernisse sieht, das damit verbundene erhöhte Sicherheitsrisiko für einen Mail- und Internetzugang in Kauf zu nehmen, ist die Anbindung noch nicht vollzogen. Ein weiterer Grund ist der mögliche Administrationsaufwand, der von momentan einem Verantwortlichen nicht bewältigt werden kann. Desweiteren wird der Austausch von Informationen zwischen der Verwaltung und den Fakultäten (z.B. Prüfungs- u. Abschlußlisten) noch durch den physischen Transport erledigt.

Die Anbindung des Verwaltungsnetzes an den Hochschulbackbone ist seitens der Hochschule gemäß Bild 5-7 geplant. Dabei wird eine Trennung der Transferwege durch die Bildung von geschlossenen Benutzergruppen auf der Basis von VLANs erreicht. Die Verwaltung erhält durch die Anbindung eines eigenen Routers und einer Netzmanagement-Clientstation Einfluß über die interne logische Netzstruktur.

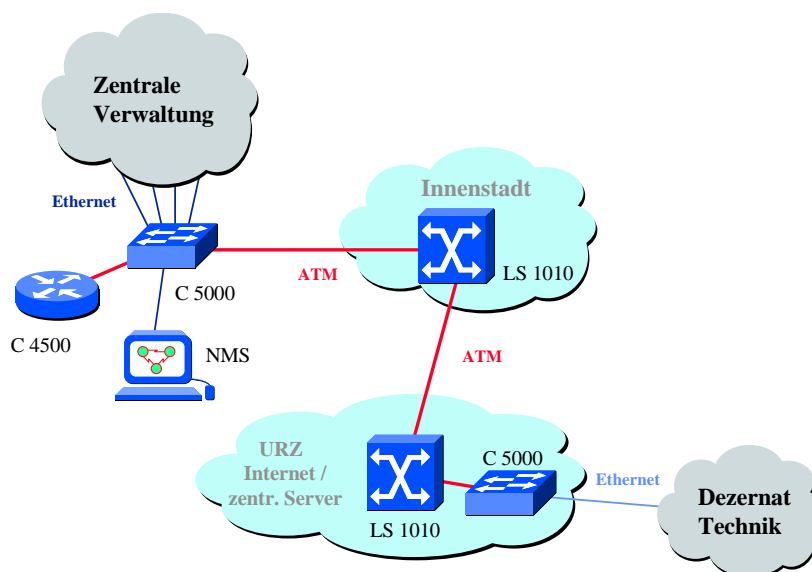


Bild 5-7 : Geplante Anbindung der Verwaltung an das Hochschulnetz

5.3.5. Sicherheitsempfehlungen

Alle nachfolgend genannten Lösungsansätze gelten unter der Voraussetzung, daß seitens der Verwaltung die Möglichkeit der Bildung von geschlossenen Benutzergruppen in Form von VLANs

und deren Sicherung durch den Router auf der Basis von Access Lists als sicherheitspolitisch nicht ausreichend erachtet werden.

Firewall

Eine Möglichkeit der sicheren Anbindung an das Hochschulnetz ist der Einsatz eines Firewall-Systems an der Schnittstelle zwischen Verwaltung und Hochschul-Backbone.

Im Gegensatz zur Hochschule ist hier ein Application Level Gateway von Vorteil, vorzugsweise der zertifizierte Harris CyberGuard (siehe Kapitel 4 sowie [Anlage 10]). Grund: Zunächst werden seitens der Verwaltung höhere Anforderungen an die Sicherheit gestellt. Andererseits geht es um eine eingeschränkte Anzahl von Nutzern (max. 100), die zumal keine großen Anforderungen an die Performance stellen und nur wenige Internetdienste nutzen werden.

Wird jedoch Wert auf einen geringen Administrationsaufwand gelegt, ist der Cisco PIX-Firewall eine mögliche Alternative. Die Vorteile wurden bereits in Kapitel 4 erläutert (siehe auch [Anlage 8]).

Bild 5-8 zeigt eine mögliche Realisierung der Firewall-Anordnung am Beispiel des Cisco PIX.

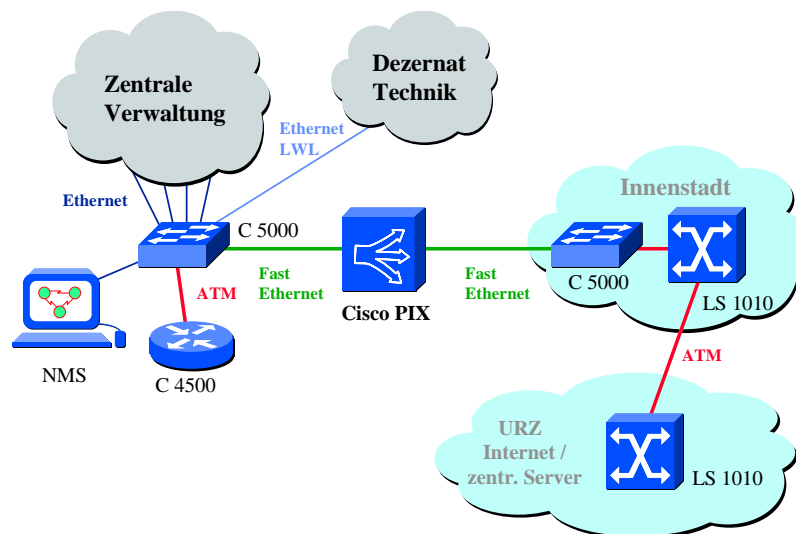


Bild 5-8 : Firewall-geschützte Anbindung der Verwaltung an das Hochschulnetz

Virtual Private Network

Eine andere Art der sicheren Kommunikation über den Backbone der Hochschule kann in der Form realisiert werden, daß man den Backbone als Virtual Private Network (VPN) nutzt, d.h. durch verschlüsselte Übertragung (Tunneling) von Daten durch den („unsicheren“) Backbone.

Hierzu sind jeweils an den Schnittstellen zwischen Teilnetz der Verwaltung und Backbone Encryption-Komponenten zu positionieren.

Cisco ermöglicht eine Umfunktionierung ihrer Firewall zu einem PIX Private Link, der eine reine Hardwarelösung für DES-Verschlüsselung auf der Netzwerkebene darstellt und gleichzeitig eine Schutzfunktion für die Teilnetze vor aus dem Hochschulnetz kommenden Angriffen bietet.

Bild 5-9 zeigt eine Realisierung der sicheren Kommunikation zwischen Verwaltung und Dezernat Technik, wodurch gleichzeitig die noch bestehende Doppelfaserverbindung zwischen den beiden Standorten für andere Zwecke frei wird (siehe auch [Anlage 8]).

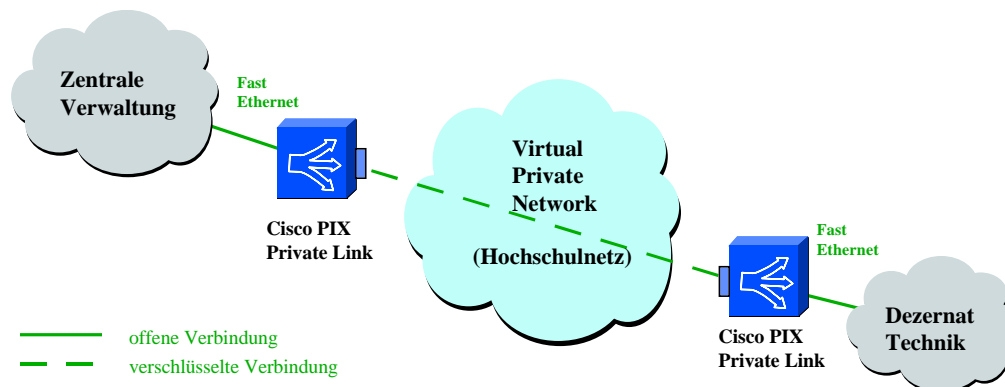


Bild 5-9 : Nutzung des Hochschulnetzes als Virtual Private Network

Eine brauchbare Lösung für den sicheren Transfer zwischen zentraler Verwaltung und einzelnen Sekretariaten der Fakultäten ist damit jedoch nicht zu erzielen, solange sich hinter den Netzknoten auch andere Zuständigkeiten befinden.

End-to-End-Encryption

Um eine erhöhte innere Sicherheit, vor allem der zentralen Server, zu erlangen, ist der Einsatz von Systemen ratsam, die eine sog. End-to-End-Encryption ermöglichen (d.h. eine Encryption bis zum Endgerät).

Als Beispiel werden Produkte der deutschen Firma KryptoKom eingebracht, da diese auch 128 Bit-lange DES-Schlüssel verwenden und daher als sicherer als aus Amerika bezogene Produkte anzusehen sind, die ihrerseits bezüglich der implementierbaren Schlüssellänge Ausfuhrbeschränkungen unterliegen (siehe [Anlage 10]).

Das Beispiel in Bild 5-10 zeigt eine mögliche Realisierung der Verschlüsselung aller Kommunikationswege auf der Sicherungsebene. Dabei wird davon ausgegangen, daß die Mehrzahl der PCs nur über mäßig sicherheitsrelevante Daten verfügt und daher mit internen Krypto-PC-Karten bzw. auch dementsprechender Software ausgestattet werden kann. Diese bieten zwar nicht den Sicherheitslevel der LAN-Boxen (sog. Black-Boxen), da sie direkt auf die PC-Hardware aufsetzen und keine Auditfunktionen wie die Boxen besitzen. Dafür sind sie jedoch erheblich preiswerter.

Hingegen sollten für die zu schützenden Server und die sensiblen PCs Boxen eingesetzt werden. Unterscheiden sich die Anwendungen auf den Servern bzw. den PCs nicht, können diese auch zusammengefaßt hinter jeweils einer LAN-Box positioniert werden.

Der Einsatz von LAN-Boxen hat darüberhinaus noch den Vorteil, daß hinter diesen auch ganze LAN-Segmente angebunden werden können, wenn diese nur PCs mit dem gleichen Schutzbedarf enthalten. Weiterhin bieten diese einen Zugangsschutz auf der Basis von Kontrolltabellen. Mit Hilfe des Security Managements können die Tabellen zentral verwaltet werden und Auditdaten aus der Box gelesen und ausgewertet werden. Außerdem versorgt das Security Management die Boxen mit sicherheitsrelevanten Informationen wie Schlüsseln.

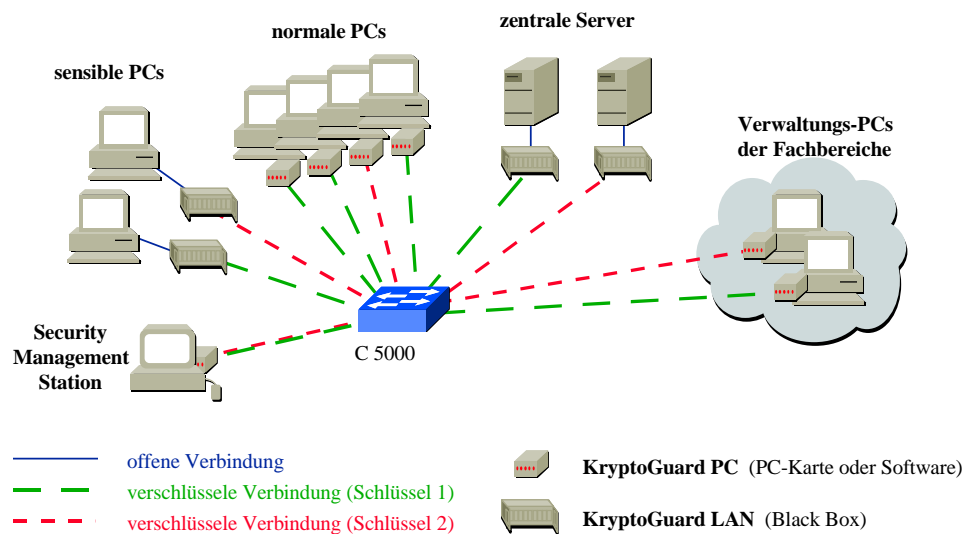


Bild 5-10 : Einsatz von Encryption innerhalb der Verwaltung

Hier kommt ein weiterer Vorteil hinzu: Alle Verwaltungsabteilungen (Studienbüros, Sekretariate etc.) der Fakultäten können, auch wenn diese hinter gemeinsamen Netzknoten mit der Hochschule liegen, ebenfalls (über den Backbone) geschützt mit den PCs kommunizieren bzw. auf die Daten der zentralen Server zugreifen.

5.4. Medizinnetz

5.4.1. Funktionalitäten

Aufgabe des Klinik-Kommunikationssystems ist es, das Personal der Kliniken bei den verschiedenen anfallenden Arbeiten mit den nötigen Informationen zu unterstützen und die Arbeiten durch Bereitstellung entsprechender Ressourcen zu versorgen. Aus diesem Grunde haben sehr viele verschiedene in den Kliniken tätige Personen Zugang zu dem System:

- Ärzte (Verwaltung von Befunden etc.)
- Pflegepersonal (Verwaltung des Pflegebefunds)
- Laborpersonal (Erstellung von Laborberichten)
- Verwaltungspersonal (Aufnahme von Patienten, Leistungsabrechnungen)
- Wissenschaftliche Mitarbeiter (Durchführung von Forschungsaufträgen)

Aufgabe dieser Personen ist es, die verschiedenen in einem Klinik-Kommunikationssystem vorhandenen Objekte zu erstellen und zu verwalten:

- ärztliche Befunde
- Laborberichte
- Organisationspläne (Pflegedienstplan, Bettenbelegplan, Terminplan etc.)
- Patientenakten
- Bestellungen (Medikamente, Essen etc.)
- Forschungsdaten

Dazu wird eine große Anzahl von Funktionen in den Bereichen Verwaltung, Versorgung und Forschung einer Klinik benötigt:

- Stationsfunktionen
- Ambulanzfunktionen
- Leistungsstellenfunktionen
- Klinikarchivfunktionen
- Arztzimmer- bzw. Untersuchungszimmerfunktionen
- sonstige Funktionen

Weiterhin sind Schnittstellen zu vorhandenen Verfahren der Klinikverwaltung im System zur Verfügung zu stellen.

Ein typisches Beispiel für die zahlreichen Zusammenhänge zwischen den einzelnen Funktionen ist der sog. Anforderungs-Befund-Kreislauf. Dabei wird zunächst in der Station der Datensatz eines Patienten sowie das entsprechende Formular ausgewählt und die gewünschte Anforderung erstellt. Die Anforderung wird dann an die Leistungsstelle (Labor) geschickt. In der Leistungsstelle werden die eingegangenen Anforderungen abgerufen. Nach Bearbeitung einer Anforderung wird der Befund in den Rechner eingegeben und an die Station geschickt. In der Station können wiederum die eingegangenen Befunde angezeigt, abgelegt und ausgedruckt werden.

Nicht zuletzt sind auch die in einer Klinik vorhandenen Rahmenbedingungen zu beachten: neben den üblichen gesetzlichen Regelungen wie Bürgerliches Gesetzbuch und Bundesdatenschutzgesetz sind

insbesondere die ärztliche Schweigepflicht und die Regelungen der Ethik-Kommissionen von Bedeutung.

5.4.2. Sicherheitsanforderungen

Ziel der Sicherheitspolitik in einem Klinik-Kommunikationssystem muß es sein, auf der einen Seite den Schutz der persönlichen Daten sicherzustellen. Dabei muß beispielsweise die ärztliche Schweigepflicht gewährleistet werden. Auf der anderen Seite jedoch muß die Sicherheitspolitik auch sicherstellen, daß in einem Notfall zum Beispiel ein Arzt schnell auf die für ihn wichtigen Befunde Zugriff hat, das heißt die Sicherheitspolitik muß auch ein hohes Maß der Verfügbarkeit der Informationen gewährleisten.

Bezüglich der Autorisierungsstruktur, die u.a. den Schutz der Patientendaten gewährleisten soll, ist anzumerken, daß diese in den Kliniken in der Regel sehr ausgeprägt ist und in einem Organisationshandbuch genau festlegt, wer sie ausführen darf. So haben zum Beispiel nur bestimmte Personen (Ärzte, Pflegepersonal) die Berechtigung, auf die ärztlichen Befunde zuzugreifen.

Die Grundanforderung an die Sicherheit ist, die Vertraulichkeit, Integrität und Verfügbarkeit der sensiblen Daten zu gewährleisten. Diese Anforderungen treten in den verschiedenen Klinikbereichen jedoch mit unterschiedlicher Priorität auf, wobei insbesondere die Anforderungen an die Integrität und Verfügbarkeit der Daten im Versorgungsbereich klinikspezifisch sind. Tabelle 5-4 gibt eine grobe Einschätzung der Bedeutung der einzelnen Aspekte der IT-Sicherheit in einer Klinik wieder.

	Verwaltung	Versorgung	Forschung
Vertraulichkeit	hoch	hoch	hoch
Integrität	wichtig	(lebens)wichtig	wichtig
Verfügbarkeit	wichtig	lebenswichtig	weniger wichtig

Tabelle 5-4 : Sicherheitsanforderungen in den einzelnen Klinikbereichen

Demgegenüber werden für die Kliniken Datenschutzforderungen vom Landesschutz-beauftragten des Landes Mecklenburg Vorpommern gestellt, die nachfolgend auszugsweise zitiert werden [KES96]:

„In den Kliniken werden personenbezogene Daten verarbeitet. Nach Einschätzung des Landesdatenschutzbeauftragten gehören diese Daten zur Sicherheitsstufe C und unterliegen damit erhöhten Datenschutzkriterien. Folgende Datenschutzmaßnahmen sind deshalb zu realisieren:

- Für die ISDN-Rufnummern der beteiligten Partner müssen geschlossene Benutzergruppen von TELEKOM eingerichtet werden.
- Die Router müssen Call-Back und Call-Identification, Firewall, PPP (CHAP) enthalten. Sie müssen kontrollierbar durch SNMP sein und Filter für TCP-Dienste bereitstellen.
- Da öffentliche Leitungen benutzt werden, müssen die Daten nach Triple DES beim Transport zwischen den Partnern verschlüsselt werden.
- Alle Zugriffe auf das System (Server) müssen durch die Einbindung des Firewall-Servers kontrolliert und protokolliert werden.
- Unberechtigte Zugriffe müssen verhindert werden, der Systemverantwortliche erhält dann sofort eine Warnung.
- Durch die eingesetzte Sicherheitssoftware (bis C2-Sicherheitsstufe) muß ein höherer Sicherheitslevel erreicht werden (auch unter Verwendung des „enhanced“-Sicherheitslevels in den Betriebssystemen, d.h. Verwendung von Paßwortalterungsmechanismen, Sperrung von Nutzerkennungen nach wiederholt mißglückten Anmeldeversuchen u.a.).
- Änderungen und Erweiterungen des Nutzerkreises der Klinik dürfen nur in Absprache mit dem Systemverantwortlichen der Klinik möglich sein (Paßwort nach 4-Augen-Prinzip).“

5.4.3. Realisierung der Funktionalitäten

In der Regel werden im Verwaltungsbereich der Kliniken, je nach Größe, eigene zentrale Rechner eingesetzt oder die Dienste von Rechenzentren (v.a. Schillingallee) in Anspruch genommen. In der Versorgung werden die für die Dokumentation und Informationen anfallenden Arbeiten in den meisten Fällen noch mit Papier und Stift sowie durch den physischen Transport erledigt. Zum Teil werden auch einzelne PCs oder kleinere Netze in den Stationen und Labors eingesetzt. In der Forschung kommen ebenfalls an erster Stelle Papier und Stift sowie einzelne PCs zum Einsatz. Zusätzlich stehen hier für manche Aufgaben zentrale Datenbanken zur Verfügung.

Derzeit ist man jedoch dabei, die Teilnetze der einzelnen Klinikstandorte zu koppeln und so die Datenverarbeitungsaufgaben der Kliniken mit Hilfe eines verteilten, heterogenen Systems zu lösen. Dies geschieht auf der physikalischen Basis einer LWL-Verkabelung, wobei innerhalb des geschlossenen Netzes 8 Fasern pro Standort reserviert sind. Bild 5-11 zeigt das bereits teilweise realisierte geschlossene Netz, wobei die FDDI-Module der Switches zu einem späteren Zeitpunkt gegen ATM-Module ausgetauscht werden sollen.

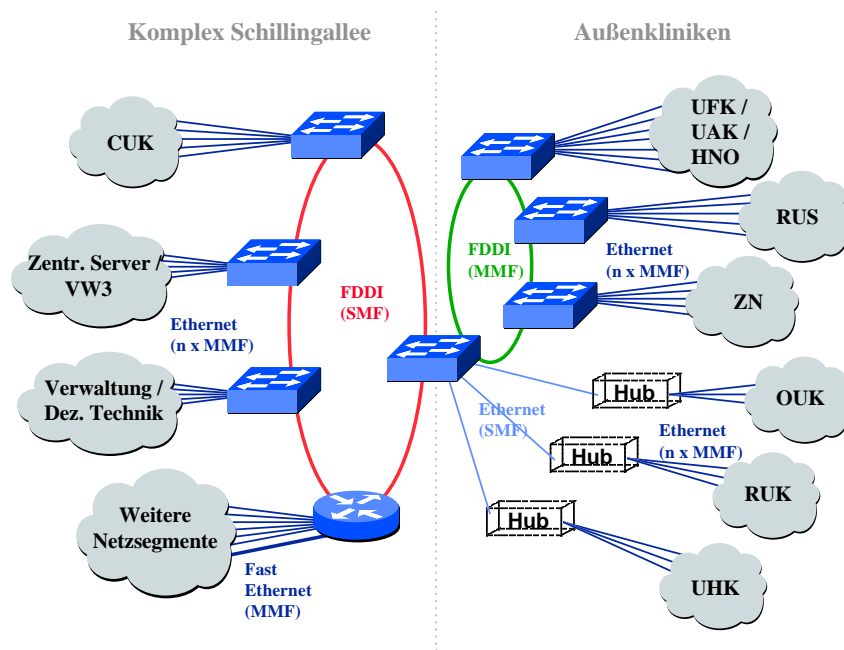


Bild 5-11 : Geplantes geschlossenes Netz der Medizinischen Fakultät

Das geschlossene Netz ist auch von der Verantwortung her vollkommen von dem offenen Netz zu trennen. Das geschlossene Netz (wobei die Ausgabenrelation für geschlossenes Netz/offenes Netz 80/20 beträgt) ist auf Initiative der Kliniken (finanziert von den Krankenkassen etc.) entstanden und besteht vorwiegend aus Komponenten der Firma 3Com. Man sieht hier momentan aufgrund der höheren Anschaffungskosten noch keinen Handlungsbedarf, die ATM-Technologie einzusetzen.

Das offene Netz ist Teil des von der Firma Siemens installierten hochschulweiten ATM-Backbones und besteht daher ausschließlich aus Komponenten der Firma Cisco. Bild 5-12 zeigt das bereits teilweise realisierte offene Netz der Medizinischen Fakultät.

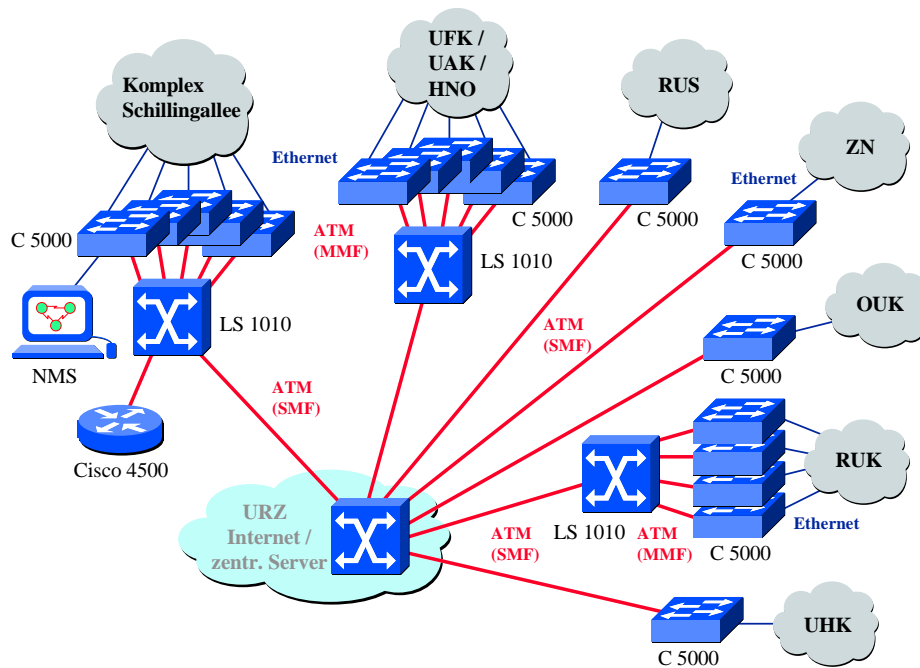


Bild 5-12 : Im Aufbau befindliches offenes Netz der Medizinischen Fakultät

Dabei ist dem jeweiligen Nutzer freigestellt, an welchem Netz er teilnehmen möchte, hier gilt lediglich die Einschränkung: „Jeder Rechner, der im offenen Netz teilnehmen will, darf keine sicherheitsrelevanten Daten auf dem Rechner haben.“ [Schulz]

Bild 5-13 macht dies noch einmal im Detail deutlich [Schulz].

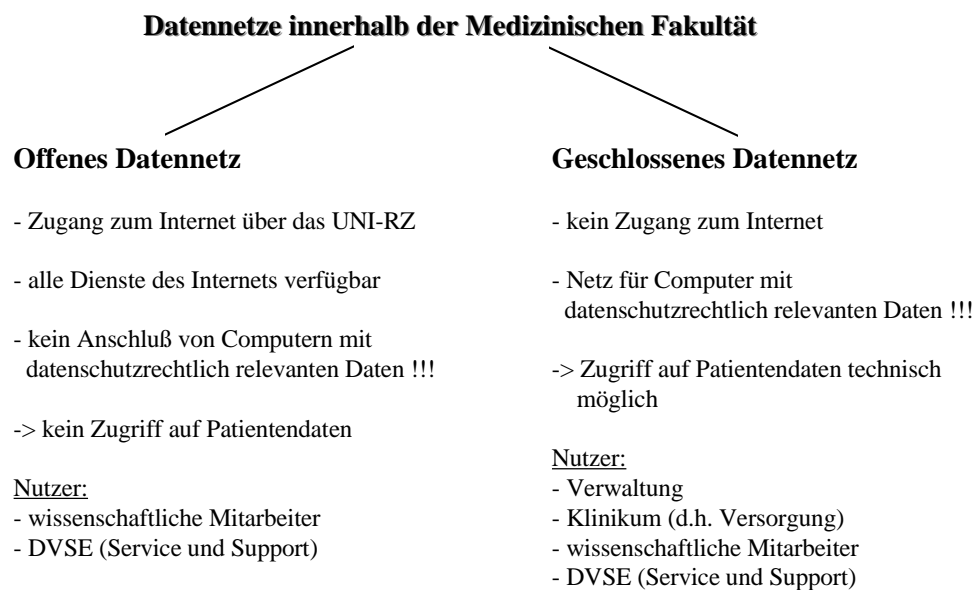


Bild 5-13 : Funktionen der beiden Datennetze innerhalb der Medizinischen Fakultät

Das hat zur Folge, daß pro Arbeitsplatz im Bedarfsfall zwei PCs vorgehalten werden müssen (z.B. für wissenschaftliche Mitarbeiter), was mit erheblichen Kosten sowie Administrationsaufwand verbunden ist.

Nach einer Umfrage in der Medizinischen Fakultät der Uni Rostock können die Ärzte jedoch am ehesten auf den E-Mail-Dienst sowie andere Internet-Dienste verzichten [Schulz].

5.4.4. Sicherheitsanalyse

Als sensitiv werden in erster Linie die personenbezogenen Daten der Patienten in allen drei Bereichen der Kliniken (Verwaltung, Versorgung, Forschung) betrachtet. Daneben existieren noch weitere sensitive Daten, wie etwa die Personaldaten der Mitarbeiter, Planungsdaten der Verwaltung und (nicht personenbezogene) Forschungsdaten und Forschungsergebnisse.

Bedrohungen ergeben sich aus dem möglichen unautorisierten Zugriff auf Daten durch Mitarbeiter, Patienten, Besucher oder Personen, die über Datennetze in die Kliniksysteme eindringen. Die Motive können zahlreich sein und reichen von Neugierde bis zu kriminellen Absichten. Ein spezifisches Problem stellt die Bedrohung personenbezogener Daten durch unkontrollierte Auslagerung zu Forschungszwecken und die unter Umständen mögliche Deanonymisierung von Forschungsdaten dar.

Beim derzeitigen Stand der Datenverarbeitung in den Kliniken ist der Bereich der Verwaltung durch die Verwendung von zentralen Rechnern und den rechenzentrumsüblichen Maßnahmen (physischer Zugangsschutz, Paßwörter) am besten geschützt. Die wichtigste Schwachstelle ist derzeit bei dezentralen Systemen in den Stationen und Labors zu sehen.

5.4.5. Sicherheitsempfehlungen

Grundmodelle

Zur prinzipiellen Darstellung der zwei grundsätzlichen Lösungsansätze sollen nachfolgende Modelle dienen. Dabei ist individuell für jede Klinik zu entscheiden, welcher Bereich welcher Sicherheitszone zuzuordnen ist, lediglich der äußere Bereich wird stets durch das Hochschulnetz repräsentiert.

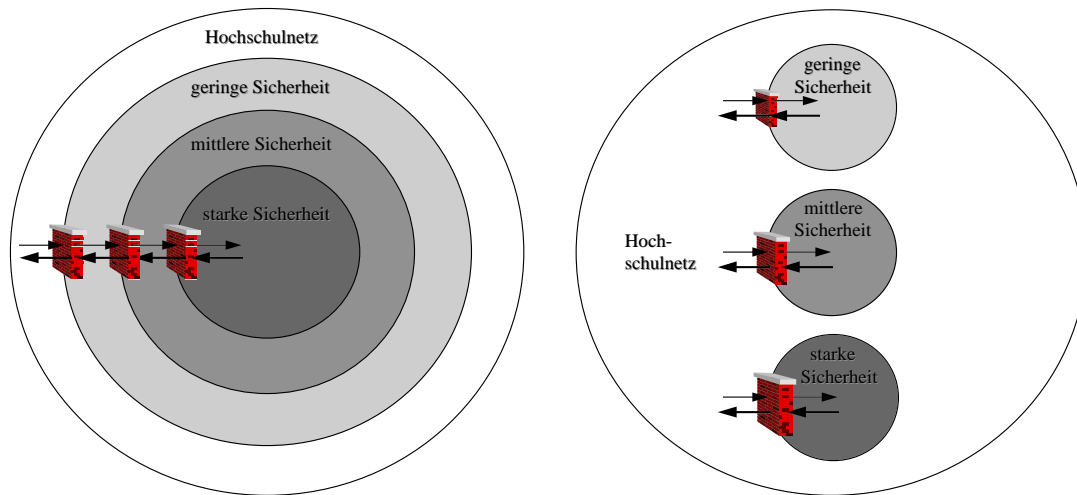


Bild 5-14 : Prinzipielle Lösungsansätze für die Absicherung der vier Teilbereiche einer Klinik

Das linke Modell in Bild 5-14 zeigt das klassische Schalenmodell, was auch von der DVSE favorisiert wird. Eine Verbindung erfolgt dabei jeweils nur bis zur nächstgelegenen Firewall. Im ungünstigsten Fall müssen dabei jedoch bis zu drei Firewalls überwunden werden. Jeder Firewall bildet dabei einen Performance-Engpaß. Diese Variante bietet bestmögliche Sicherheit bei jedoch starken Performanceeinbußen.

Das rechte Modell hingegen positioniert die verschiedenen Zonen nebeneinander. Die Höhe der Sicherheit wird dabei durch die Größe der jeweiligen Firewall markiert. Im ungünstigsten Fall müssen zwei Firewalls überwunden werden. Diese Variante ist wesentlich performanter, bietet dafür aber nicht die Sicherheit der ersten.

Obige Darstellungen sind zur Genüge in Sicherheitsabhandlungen zu finden, in denen stets von geschlossenen Unternehmen (der klassische Fall !) die Rede ist. Daß diese Modelle jedoch sehr ungenau die Situation bei einer Verteilung über mehrere Standorte beschreiben, wird nachfolgend dargestellt. Bei diesen Betrachtungen ist es unerheblich, wie die jeweiligen Firewall-Systeme konzipiert sind, empfohlen wird lediglich ein Firewall-System, das mehr bietet als reine Paketfilterung.

Erste Variante

Eine naheliegende Variante für die sichere Trennung der vier Klinikbereiche ist der Aufbau von vier physisch völlig getrennten (FDDI- oder ATM-)Netzen, denen jeweils die Bereiche einer Sicherheitskategorie zugeordnet werden. Die sichere Verknüpfung der vier Netze erfolgt über drei zentral gelegene Firewalls (vorzugsweise im verantwortlichen Bereich Schillingallee), die bei dieser begrenzten Anzahl auch von unterschiedlicher Bauart sein können (siehe Bild 5-15).

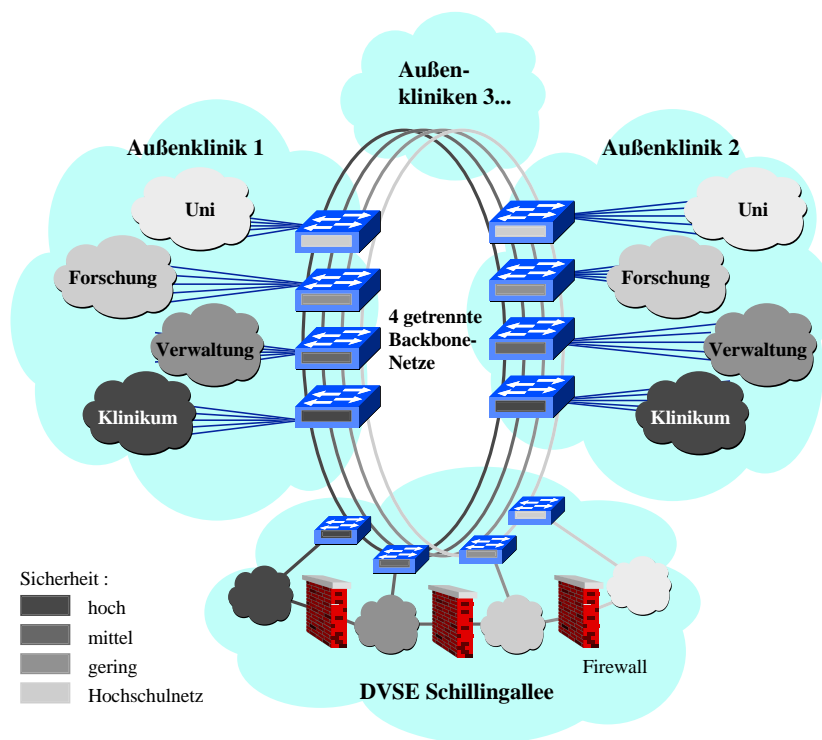


Bild 5-15 : Sicherung durch vier physisch getrennte Medizin-Netze

Ein Vorteil ist die große verfügbare Bandbreite pro User, innerhalb eines Sicherheitsbereiches kann die Kommunikation mit hoher Performance erfolgen. Ein weiterer Vorteil ist der geringe Administrationsaufwand für die Firewall-Technik.

Obwohl die Anzahl der Firewall-Systeme gering ist, ist diese Variante insgesamt sehr kostspielig: der Aufbau von vier getrennten Netzen erfordert den Einsatz einer hohen Anzahl aktiver Netztechnik (Switches, Router, etc.) und LWL-Fasern. Allein pro Standortbereich müssten bei ATM acht und bei FDDI gar sechzehn Fasern veranschlagt werden. Da für jeden Standort laut Bild 3-3 sechzehn bzw. vierundzwanzig Fasern für Datenanwendungen zur Verfügung stehen, wäre bei Einsatz der FDDI-Technologie der redundante Vorhalt von Fasern für zukünftige Erweiterungen bereits heute aufgebraucht.

Zweite Variante

Die zwei nachfolgenden Varianten haben im Gegensatz zu der vorigen eins gemeinsam:

Zur Verknüpfung der Standorte dient ein einheitliches Backbone-Netz, entweder auf FDDI oder ATM basierend.

Vorteil ist die geringe Anzahl von Fasern (ATM: zwei, FDDI: vier Fasern je Standort) und aktiver Netztechnik, Nachteil die geringere verfügbare Bandbreite je User, die hohe Anzahl an

Firewallsystemen (21 Firewalls über 7 Kliniken verteilt) und der damit verbundene hohe Administrationsaufwand.

Die zweite Variante lehnt sich an das vom DVSE favorisierte linke Schalenmodell aus Bild 5-14 an. Dabei wurden zum besseren Verständnis des Problems die verschiedenen Klinikbereiche willkürlich den Sicherheitszonen zugeordnet (siehe Bild 5-16).

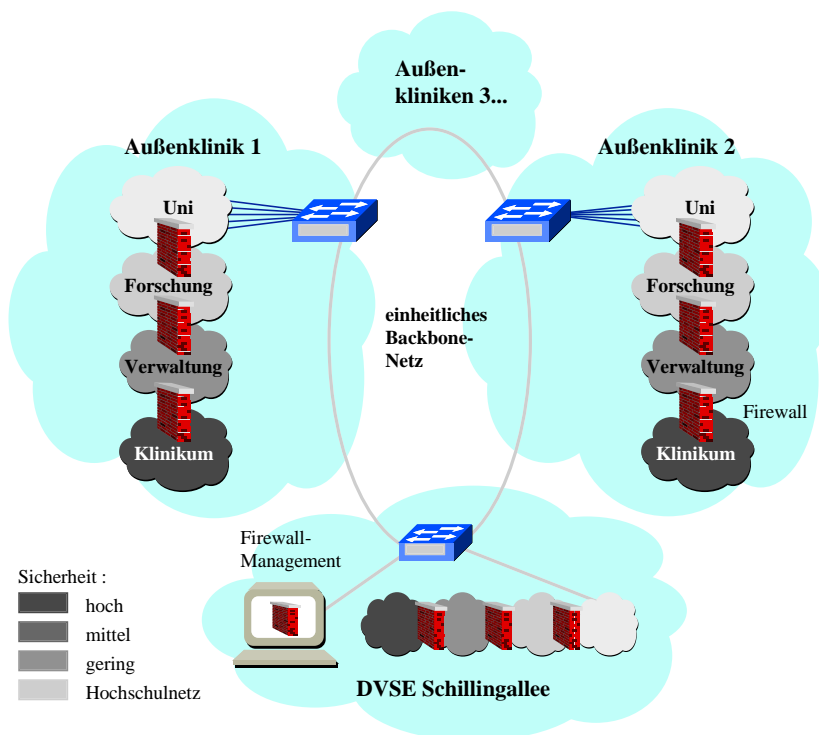


Bild 5-16 : Sicherung durch Kaskadierung der Bereiche innerhalb der Kliniken

Es wird deutlich, daß praktisch nicht (wie anfangs vermutet) bis zu drei, sondern bis zu sechs Firewalls zu überwinden sind. In diesem Beispiel wäre dies der Fall, wenn beispielsweise ein Arzt der Klinik 1 (Klinikum) mit dem Arzt der Klinik 2 (Klinikum) kommunizieren möchte. Folge ist eine geringe Performance, aber auch ein hoher Schutz der sensibleren Bereiche vor Zugriffen aus dem Uni-Netz.

Noch problematischer ist der Fakt, daß der Arzt auf diesem Wege die Netze von Verwaltung und Forschung passiert, wo auch Daten lagern, die ihn nichts angehen, wie beispielsweise die Gehaltsdaten eines Kollegen. Genauso verhält es sich, wenn ein Verwaltungsmitarbeiter auf dem Kommunikationsweg mit einer anderen Verwaltung die Forschungsnetze passiert, wo wiederum die geheimen Forschungsdaten eines Wissenschaftlers lagern. Durch die Firewall können zwar jedem Netz-User seine Dienste und seine Zielrechner genau zugewiesen werden, das ändert aber nichts an der Tatsache, daß er die Netze physisch durchläuft. Außerdem können die Dienste der verschiedenen Netze die gleichen sein. Nicht zuletzt können Administrationsfehler der Firewall die letzte Sicherheit

der Zielzuordnung schmälern, was bei einer Verwaltung einer derartig hohen Anzahl von Firewall-Systemen sehr leicht vorkommen kann, selbst wenn dies von einer zentralen Managementplattform geschieht (was wiederum ein einheitliches Firewallsystem für alle Bereiche voraussetzt). Daher ist diese Variante unter keinen Umständen zu empfehlen.

Dritte Variante

Die dritte Variante (siehe Bild 5-17) richtet sich nach dem rechten Modell in Bild 5-14. Dabei werden die Bereiche innerhalb der Kliniken sternförmig mit dem offenen Uni-Netz verbunden, jeweils geschützt durch ein Firewall-System. Diese Lösung deckt sich mit der in Bild 4-11 gezeigten Ansatz.

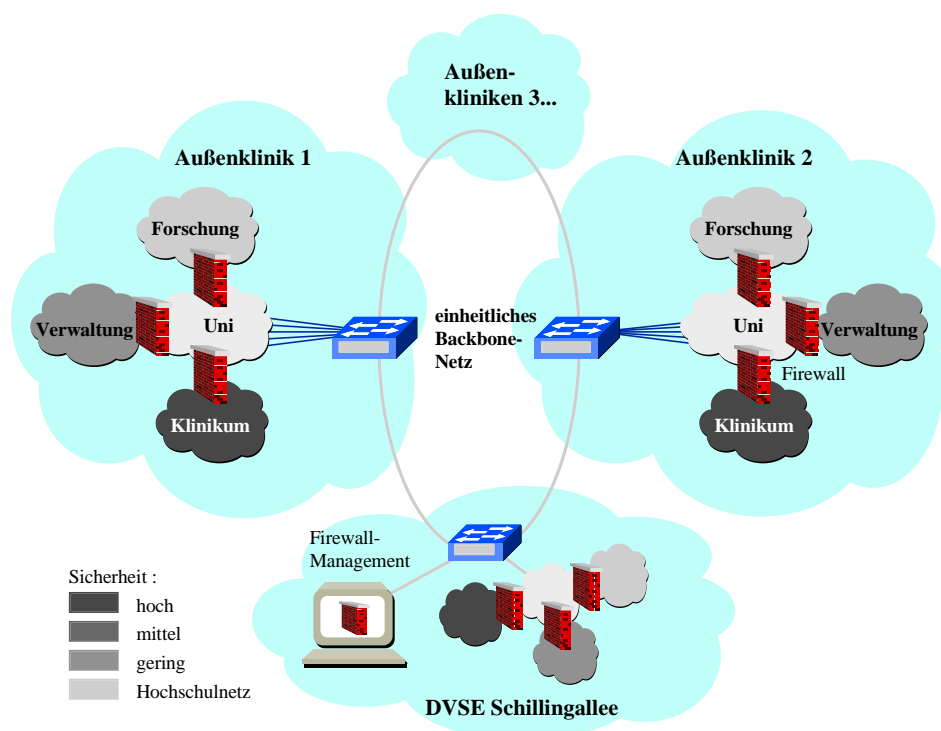


Bild 5-17 : Sicherung durch sternförmige Anordnung der Bereiche innerhalb der Kliniken

In diesem Fall sind zur bereichsübergreifenden Kommunikation tatsächlich maximal zwei Firewall-Systeme zu passieren, was eine bessere Performance zur Folge hat.

Entscheidend ist die Tatsache, daß ein Netz-User, unabhängig vom benutzten Kommunikationsweg, in keinem Falle mehr die Gelegenheit erhält, sicherheitsrelevante Bereiche zu kreuzen, wie dies in der vorigen Variante noch der Fall war.

Der gleiche Schutzgrad wie in der vorigen Variante gegenüber Angreifern aus dem Uni-Netz wird gegebenenfalls dadurch realisiert, für die einzelnen Firewall-Systeme Kombinationen bzw. Kaskadierungen von Firewalls (siehe Kapitel 4) einzusetzen.

Akzeptabler, aber dennoch nicht zu empfehlen ist diese Variante, weil sie eine Verwaltung von mindestens 21 Firewalls voraussetzt. Verlagert beispielsweise ein Arzt seinen Arbeitsplatz in eine andere Klinik, sind gleich alle Firewall-Konfigurationen zu aktualisieren, die für ihn relevant sind, im schlimmsten Fall alle 21. Nicht außer Acht gelassen darf außerdem, daß Firewalls bezüglich ihrer Software regelmäßige Updates erfordern, da sich einerseits Dienste weiterentwickeln bzw. neu hinzukommen und andererseits Angreifer ständig neue Angriffstools entwickeln, an die es sich anzupassen gilt.

Lösungsvariante

Die vierte Lösungsansatz ist zugleich der vom Verfasser favorisierte. Voraussetzung ist allerdings ein hoher Grad der zentralen Organisation. Dabei müssen die noch existierenden dezentralen Netzstrukturen und verteilten Serversysteme vollständig beseitigt werden. Die Server können in einem klimatisierten Raum in der Schillingallee platziert werden, zu dem eine Zugangskontrolle geschaffen werden kann. Eine gezieltere Fehlerbehebung ist ebenfalls möglich. Ein erhöhter Ausfallschutz des Gesamtnetzes kann durch den Einsatz einer unterbrechungsfreien Stromversorgungs-Anlage (USV) erreicht werden. Zudem besteht eine Möglichkeit des zentralen Backups.

Kern der Lösung ist die Verwendung eines einheitlichen ATM-Backbone-Netzes und die darauf fußende Bildung von vier geschlossenen Benutzergruppen auf der Basis von Virtuellen LANs (Bild 5-18). Alle bisher noch vorhandenen Server und Datenbanken auf den Festplatten der PCs und Workstations in den Kliniken müssen in diesem Zusammenhang auf zentrale Server in der Schillingallee ausgelagert werden, dabei müssen die Netz-User geringe Wartezeiten beim Zugriff auf die zentralen Ressourcen in Kauf nehmen.

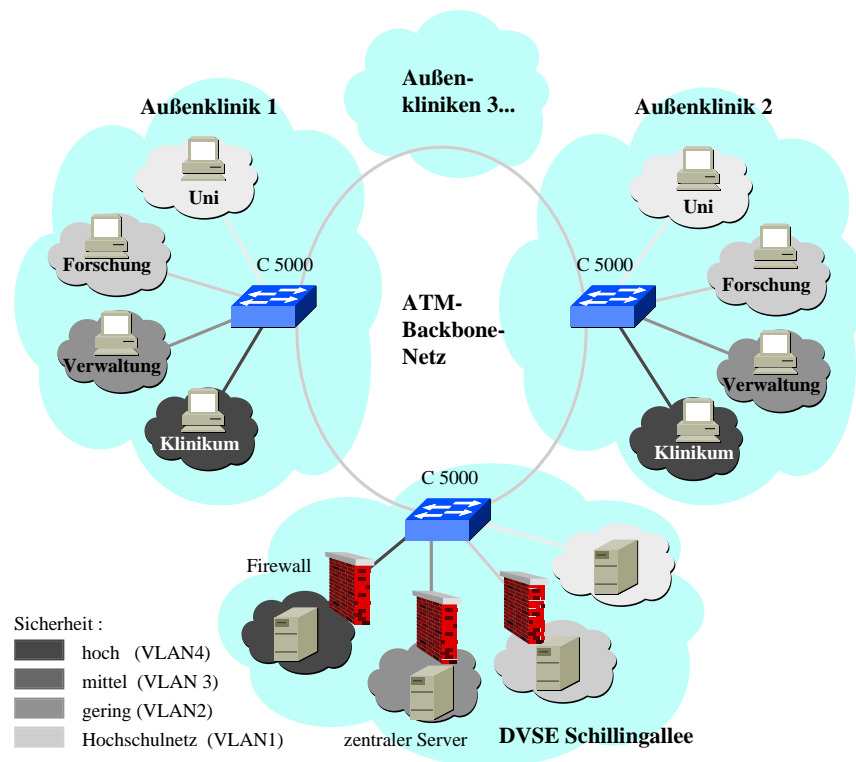


Bild 5-18 : Sicherung durch VLANs und Schutz der zentralen Server durch Firewalls

Insgesamt bietet diese Struktur eine Sicherheit in zwei Stufen: Die erste ist die Trennung der Benutzergruppen durch im Router implementierte Access Lists. Gelingt es einem Teilnehmer, unter Umgehung dieser Listen ein System in einer anderen Benutzergruppe zu erreichen, ist dies für ihn nutzlos, solange sich keine Daten mehr auf den Systemen der Kliniken befinden. Diese Daten befinden sich auf durch Firewalls (vorzugsweise Application Level Gateways) geschützten Servern in der Schillingallee.

Gleichzeitig ist durch diese Lösungsvariante ein hoher Grad an Verfügbarkeit gegeben. Soll beispielsweise einem Arzt der Zugriff auf die Datenbank in der Forschung gestattet werden, erhält er einen Account auf derjenigen Firewall, die die Forschungsserver schützt. Auch steht jedem Teilnehmer eine hohe Bandbreite zur Verfügung.

Insgesamt ergeben sich eine Reihe weiterer Vorteile:

Der Administrationsaufwand für drei Firewall-Systeme hält sich in Grenzen.

Durch die globale VLAN-Struktur kommen bei Umzügen von Teilnehmern keine Administrationsaufwendungen hinzu, die Zuordnung zu den jeweiligen VLANs bleibt bestehen, so daß sich auch keine Änderung der Firewall-Listen erforderlich macht.

Auch von der Kostenseite her ist diese Variante attraktiv: die genutzte LWL-Faser-Anzahl ist gering, es kann die vorhandene ATM-Netztechnik verwendet werden, die Anzahl der notwendigen Server vermindert sich. Zudem müssen pro Arbeitsplatz nicht mehr zwei PCs vorgehalten werden (z.B. für

wissenschaftliche Mitarbeiter, siehe Bild 5-13), was erhebliche Kosten- sowie Administrationseinsparungen bewirkt.

Letztendlich sind auch durch die zentrale Organisationsstruktur immense Kosteneinsparungen zu erzielen.

Unabhängig davon können für zum Schutz der Kommunikation bestimmter Endgeräte Systeme zur End-to-End-Encryption eingesetzt werden, wie dies bereits beim Verwaltungsnetz (Kapitel 5.4.4.) vorgeschlagen wurde.

Erwähnenswert ist noch der folgende Ansatz (siehe Bild 5-19).

Nicht jede Übertragung und Speicherung von Daten muß geschützt erfolgen. Wenn man die Daten, die große Anforderungen an Speicherplatz, Durchsatz, Verzögerung, Qualität etc. (z.B. OP-Videos und Röntgenbilder) stellen, anonymisiert, kann deren Übertragung und Speicherung ungeschützt und damit performanter erfolgen. Die zugehörigen Daten, die diese rechentechnischen Bedürfnisse nicht besitzen, können (auch zeitversetzt) über verschlüsselte Datenwege übertragen werden. Wichtig ist lediglich die Sorgfalt bei der Zuordnung von Daten zu Bildern/Videos, damit keine falschen Diagnosen aufgrund falscher Zuordnungen gestellt werden können. Eine große Rolle spielt daneben ein persönlicher Ärzte-Patienten-Kontakt, um diese Zuordnung persönlich bewerten zu können und ggf. doch aufgetretene Zuordnungsfehler rechtzeitig erkennen zu können.

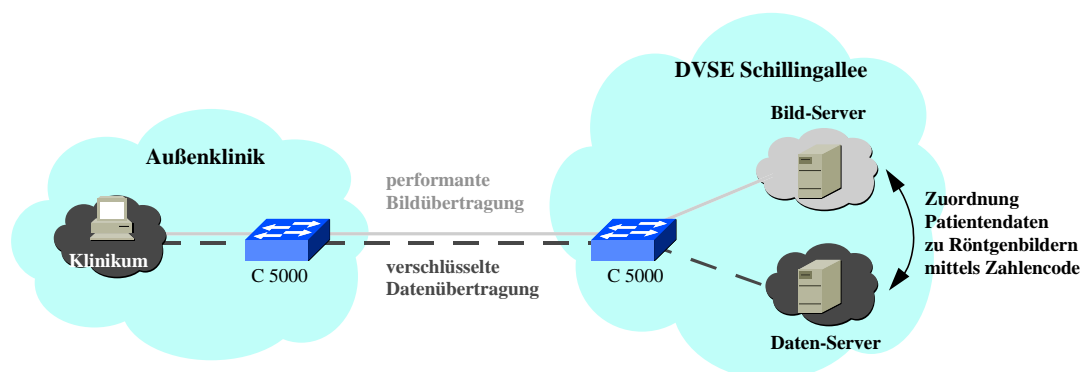


Bild 5-19 : Getrennte Übertragung von Bildern und Daten

5.5. Abschließende Überlegungen und Fazit

Die besten und aufwendigsten technischen Sicherheitsvorkehrungen sind nutzlos, wenn die Hardware-Komponenten, aus denen sie bestehen, nicht ausreichend geschützt sind. Alle kritischen Elemente wie Server, Router, Netzmanagement-Systeme, Firewalls, Verteilerschränke etc. sollten grundsätzlich physikalisch abgeschirmt in einem klimatisierten Raum installiert sein. Zugang zu diesem Raum ist

ausschließlich durch persönliche Identifikation (Magnetkarten, Zugangscode, Integration in das NMS etc.) zu ermöglichen. Dies ist zur Zeit nur im Rechenzentrum realisiert.

Bezüglich der aktiven Netztechnik sind alle nicht genutzten Ports über das Netzmanagement zu sperren, damit einem Angreifer keine Gelegenheit bleibt, sich über ein Terminal auf dem Gerät einzuloggen, um so Datenflüsse oder Konfigurationen aushorchen zu können.

Bevor jedoch konkrete Sicherheitsmaßnahmen ergriffen werden können, müssen Definitionen getroffen werden, welche Daten bzw. Objekte wovon und nach welchen Kriterien geschützt werden müssen. Weiterhin ist eine detaillierte Aussage zum auftretenden Kommunikationsaufkommen zu treffen, was jedoch erst nach vollständiger Inbetriebnahme des ATM-Backbone-Netzes sinnvoll ist.

Hierfür ist eine sorgfältige Auflistung nach dem in Tabelle 5-5 dargestellten Schema vorzunehmen.

Benutzerkreis: Gruppen/ Teilnehmer (Anzahl)	Zugangsort (Quelle)	Zielort	verfügbare Dienste	Sicherheits- kategorie	mittleres Volumen der Kommunikation [MByte]	mittlere Dauer der Kommunikation [h]	Zeitfenster (Wochentage, Tageszeiten)
--	------------------------	---------	-----------------------	---------------------------	--	---	---

Tabelle 5-5 : Relevante Ausgangsdaten für ein Sicherheitskonzept

Hinsichtlich der Benutzergruppen ist beispielsweise in der Medizinischen Fakultät genau zu klären, welcher Nutzer welcher Gruppe bzw. Sicherheitskategorie zuzuordnen ist.

Die Kommunikationsdaten können beispielsweise durch Protokollierung mit Hilfe des Traffic Directors über einen längeren Zeitraum ermittelt werden.

Anhand dieser Daten können mehrere Firewall-Systeme verglichen werden und diese ggf. Durchsatz-Messungen unterworfen werden, um eine Aussage über die Eignung auch anhand der Performance-Einschränkungen zu treffen.

Weiterhin können diese Systeme mit aktuellen Angriffssimulatoren konfrontiert werden, um diese Systeme auch hinsichtlich ihrer „Standhaftigkeit“ unter den speziellen Anforderungen der Netzumgebung überprüfen zu können.

Gängige Angriffstools sind SATAN, ISS Internet-Scanner, InfoStructure PINWARE und InfoStructure Netprobe, die verschiedene Angriffe von außen simulieren und die aufgedeckten Schwächen in Reports zusammenfassen [KYS96].

Eine Aussage ist auch über die Bedien- und Konfigurierbarkeit (einschließlich der Kompatibilität und Fernwartbarkeit) des jeweiligen Systems zu treffen. Diese können individuell verschieden ausfallen, in Abhängigkeit von Wissen und Neigung des Administrators. Hierzu gibt es auch Tools, die auf das System gespielt werden können und daraufhin die Systemkonfigurationen auf mögliche

Sicherheitslücken hin überprüfen. Gängige Tools sind Farmer/Spafford COPS und TAMU-Tiger [KYS96].

Viele Anwender, darunter auch das LIT (siehe Kapitel 4.6.2.), glauben, unterschiedliche Firewall-Systeme von unterschiedlichen Herstellern einsetzen zu müssen, da laut BSI herstellerspezifisch unterschiedliche Technologien einen hohen Schutzgrad ausmachen und folglich schwerer zu überwinden sind. Sicher ist, daß die Hersteller unterschiedliche Philosophien bei der Konzeption ihrer Systeme verfolgen. Vergessen darf jedoch nicht, daß ein Produkt bereits mehrere Technologien gleichzeitig repräsentiert (Beispiel: Harris CyberGuard vereint Packet Filter, Circuit und Application Level Gateway).

Empfohlen wird daher eine einheitliche Produktlinie, da nur so eine einheitliche Verwaltbarkeit und eine bessere Erweiterbarkeit gewährleistet werden kann. Durch die Festlegung auf den Hersteller Cisco bezüglich der aktiven Netztechnik liegt bereits eine einheitliche Sicherheits-Architektur vor, basierend auf dem Betriebssystem IOS und den beschriebenen Features (NAT, Access Management, Host Security, Encryption), auf die durch Verwendung von Cisco-Sicherheitssystemen (Cisco AS5200, Cisco PIX, Cisco-Secure) aufgesetzt werden sollte (siehe [Anlage 5, 7 u. 8]). Auch ein fortlaufender Upgrade kann in diesem Fall einheitlich erfolgen. So kann auch die häufige Fehlerquelle, daß an einem System die Streichung von Nutzern und Rechten vergessen wird, ausgeschaltet werden, da eine Kommunikation zwischen den Systemen (z.B. über TACACS) automatisch die gleichen Nutzer/Rechte-Stand für alle Systeme gewährleistet.

Grundsätzlich zu empfehlen sind vor allem Firewall-Systeme, die weitestgehend auf Hardware basieren (z.B. Cisco PIX, siehe [Anlage 8]) oder auf ein sicheres Betriebssystem aufbauen (z.B. Harris CyberGuard, siehe [Anlage 10]).

Grundsätzlich sollten jedoch keine weiteren Applikationen auf den Firewall-Plattformen ablaufen. Hier sollte besonders den Abhandlungen der Institutionen ITSEC, TCSEC und BSI Beachtung geschenkt werden (siehe Kapitel 4.1. und 4.4.7.).

Zu beachten ist, daß die Firewallsysteme an den Schnittstellen, an denen sie platziert werden, zugleich auch eine logische Trennung der Netzstruktur verursachen. Das hat zur Folge, daß das mit dem ATM-Netz angestrebte Prinzip vom vollständig geswitchten Netz mit einer vollständigen Verteilung der Nutzer über das gesamte Universitätsnetz und unter einem einheitlichen Netzmanagement nicht beibehalten werden kann.

Weiterhin ist zu prüfen, welche kritischen Applikationen außer SNMP und TFTP (UNIX r-Dienste, Sun RPC, openwindows, X windows, etc.) noch genutzt werden, so daß diese dann ggf. nach außen über die Router ausgefiltert werden sollten.

Die Installation von Software auf UNIX-Systemen sollte mit normalen Benutzerrechten und nicht als root (privilegierter Account, von dem aus alle Befehle ausgeführt werden dürfen) durchgeführt werden, um zusätzliche (unkontrollierte) Einträge und Veränderungen der Systemsoftware zu vermeiden. Hierzu kann beispielsweise ein Account zur Software-Installation erzeugt werden, der Schreibrecht in in bestimmten Bereichen besitzt, oder dieser Bereich wird für eine definierte Gruppe freigegeben.

Zu beachten ist insbesondere, daß das System keine offenen Accounts besitzen soll, auf denen sich dann beliebige Personen ohne Paßwort einloggen können, dies sollte regelmäßig vom Systemverwalter, z.B. mit einem kleinen Shellskript, überprüft werden.

Im Paßwort-File werden jedem User-Namen UID (Benutzer-Nummer zur Identifikation) und GID (Gruppennummer des Benutzers zum Gruppenzugriff auf Files) zugewiesen. Bei vielen Systemoperationen werden diese Werte abgefragt und mit den Objekten, z.B. Files oder Devices, auf die zugegriffen werden soll, verglichen, wobei bei Übereinstimmung der Zugriff erlaubt wird. Daher ist darauf zu achten, daß ein nichtprivilegierter Benutzer nicht versehentlich die UID 0 von root erhält. Dies würde ihn mit root völlig gleichstellen und beliebige Aktivitäten gestatten.

Speziell beim Einsatz von Firewall-Software auf UNIX-Rechnern ist, wie bereits erwähnt, vorher diese Plattform zu sichern. Dies wird am Beispiel einer Sun SPARC-Station erläutert:

Eine Sun SPARC mit zwei Anschlüssen arbeitet automatisch als Gateway: der Kernel erkennt, daß zwei Netzwerkanschlüsse installiert sind und beginnt daher mit dem Forwarding von ankommenden IP-Datagrammen in das jeweils andere Netz.

Um dieses Verhalten zu ändern, muß ein neuer Kernel installiert werden, der kein Forwarding durchführt. In der Konfigurationsdatei des Kernels kann dies über die Option „ipforwarding“ gesteuert werden. Der Kernel wird standardmäßig mit der Option ipforwarding=0 kompiliert. Dadurch wird das Forwarding dann aktiviert, wenn ein zweiter Netzwerkanschluß installiert ist. So muß diese Option zunächst auf „ipforwarding=-1“ geändert werden. Nach dieser Änderung der Konfigurationsdatei muß ein neuer Kernel erzeugt werden, der dann installiert wird. Nach dem Booten des neuen Kernels findet kein IP-Forwarding mehr statt, dies kann ggf. mit Analyse-Tools (z.B. tcpdump) überprüft werden. Erst nach dieser Prozedur kann die SPARC-Station als Gateway-Plattform genutzt werden.

Die Administration z.B. der UNIX-Rechner sollte wenigen Spezialisten mit dem nötigen Wissen vorbehalten sein, um die Fehleranzahl zu verringern.

Zur Wahl der Paßwörter sind folgende Richtlinien zu empfehlen:

- als Paßwort kein deutsches oder englisches Wort wählen, das sich in einem Lexikon befindet
- vor allem für Paßwörter nicht die Vornamen von Familienangehörigen und Haustieren nehmen
- sichere Paßwörter sind 6-8 Zeichen lang (oder länger) und enthalten mindestens eine Ziffer und ein Sonderzeichen (z.B. Punkt oder Komma)

- die Ziffer sollte mitten in das Paßwort gemischt werden, und nicht an den Anfang oder das Ende gestellt werden
- Groß- und Kleinschreibung verwenden, wenn relevant

Diese Regeln sollten den Universitäts-Angehörigen in einem stärkeren Maße nahegebracht werden, z.B. über ein Merkblatt, das bei der Nutzerkennungs-Vergabe ausgegeben wird.

Können Daten auf den Speichermedien bestimmter Arbeitsplätze nicht, wie bei Verwaltung und Medizin empfohlen, auf zentrale Server ausgelagert werden, gibt es noch die Möglichkeit der Unleserlichmachung mittels Encryption. Hier sollte jedoch nur ein Direktzugriff möglich sein, beispielsweise durch den Einsatz von arbeitsplatzbezogenen Kartenlesern und zugehörigen Smart Cards (Produkt-Beispiel: KryptoKom SmartGuard B).

In diesem Zusammenhang ist zu prüfen, inwieweit die in Kapitel 5.4.5. angesprochene Trennung zwischen Dateninhalten hinsichtlich Performance und Sicherheit bei der Übertragung und Speicherung sinnvoll ist.

Abschließend muß noch erwähnt werden, daß der Großteil aller Mängel von falscher Organisation herrührt, auch Social Hacking genannt. Wenn beispielsweise ein unbekannter Angreifer vom Pförtner des Rechenzentrums unter dem Vorwand einer Notsituation Zugang zum Rechnerraum verlangt und im Falle der Weigerung mit möglichen Konsequenzen droht, worauf dieser dann in seinem Sinne handelt, sind die besten technischen Sicherheitsvorkehrungen sinnlos.