HUMBOLDT-UNIVERSITÄT ZU BERLIN
RECHENZENTRUM

Firewall - ein Kernstück zur Sicherung des Verwaltungsnetzes der Humboldt-Universität

Abschlussbericht an den DFN-Verein

13. Juni 2000

Auftragnehmer	Humboldt-Universität zu Berlin ZE Rechenzentrum
Kennzeichen	**TK 598-SD027**
Kurzbezeichnung	Firewall
Laufzeit des Vorhabens	25.08.97 - 31.01.2000
Berichtszeitraum	25.08.97 - 31.01.2000
Projektleitung	Dr. P. Schirmbacher
Fachliche Betreuung	D. Natusch
Projektdurchführung	A. Geschonneck R. Herbst

Inhalt

Verzeichnis der Abbildungen

1 Anliegen des Projektes

Innerhalb kurzer Zeit sind die Anwendungen des Internets weltweit zu Standard-Arbeitswerkzeugen avanciert. Die Nutzer von Internetdiensten tauschen Email aus, recherchieren in Datenbanken und veröffentlichen ihre Forschungsergebnisse im Web, um sie weltweit einem breiten Interessentenkreis zur Verfügung zu stellen.
Auch in der Verwaltung einer Universität besteht die Forderung, die Vorteile der Internet-Technologie zu nutzen. Da im Wesentlichen mit personenbezogenen Daten, die einem höheren Schutzbedarf unterliegen, gearbeitet wird, kann man diesen Anschluss nicht ohne weiteres vornehmen. Es muss ein IT-Sicherheitskonzept erarbeitet werden, in dem dann Schutzmaßnahmen wie die Einrichtung eines Firewall-Systems festgelegt werden. Die mit der Konzeption und der Umsetzung eines Sicherheitskonzeptes in Verbindung stehenden Aufgabenstellungen erfordern tiefgreifende Kenntnisse der Internet-Technologie, der System-Installation und -konfiguration, die den Einsatz von hochqualifiziertem Personal erfordern.
Um diesen Anforderungen gerecht werden zu können, startete das Rechenzentrum der Humboldt-Universität zu Berlin im August 1997 ein Projekt mit folgenden Kernthemen:

- **Netzstrukturierung unter Sicherheitsaspekten**
- **Entwicklung einer Beispiellösung für ein Firewall-System**
- **Einsatzmöglichkeiten von Verschlüsselungstechnologien in der Verwaltung**

Es bestand die Aufgabe, die im Zusammenhang mit dem Anschluss des Netzes der Universitätsverwaltung an das Internet entstehenden Sicherheitsrisiken zu erkennen, Wege zu deren Lösung zu finden und anhand konkreter Installationen oder Veränderungen der Netzwerk-Infrastruktur direkt umzusetzen. Das Projekt wurde vom Verein zur Unterstützung des deutschen Forschungsnetzes (DFN) gefördert.

Mit diesem Abschlussbericht sollen der Projektverlauf geschildert und die erreichten Ergebnisse dokumentiert werden.

2 Ergebnisse

Nachfolgend eine kurze Zusammenfassung der Ergebnisse, die sich unmittelbar auf den DV-Alltag der Verwaltung auswirken und die zu großen Teilen durch das Projekt beeinflusst bzw. erst möglich geworden sind:

1. 90% der Mitarbeiter der Universitätsverwaltung (ca. 380) verfügen über einen Zugang zu Netzwerk-Diensten.

2. Die Mitarbeiter der Zentralen Universitätsverwaltung können von ihrem Arbeitsplatz aus Kommunikationsdienste (E-Mail, Web, Filetransfer) und ebenso Anwendungen im Intranet (Bearbeitung von Personen- und Stellendaten) benutzen.

3. Jeder vernetzte PC verfügt über eine Standard-Installation mit den Anwendungen, die für die Bearbeitung von Verwaltungsvorgängen benötigt werden, inkl. Web-Browser für Internet-Anwendungen und E-Mail-Client.

4. Der Schutz vor Gefahren aus dem Internet konnte durch die Nutzung von Proxies (Filterung von aktiven Web-Inhalten, Schutz vor Ausspähung des Nutzerverhaltens, Verschleierung der Netzwerk-Struktur des zu schützenden Netzwerkes) verbessert werden.

5. Es erfolgte der Aufbau und Betrieb einer Zertifizierungsinstanz für PGP und S/MIME / SSL am Rechenzentrum der Humboldt-Universität zur Gewährleistung der sicheren Kommunikation über unsichere Netzwerke (Anwendung der Digitalen Signatur).

6. Die Möglichkeit der stark authentifizierten und verschlüsselten Fern-Administration der Haushalts-Systeme für die Mitarbeiter der HIS-GmbH wurde zur Verfügung gestellt.

7. Das Pilotprojekt "Studentische Hilfskräfte", das die Bearbeitung von Personaldaten über das Universitätsnetz zum Inhalt hatte, wurde durch den Einsatz von stark authentifizierten und verschlüsselten Netzwerk-Verbindungen technisch ermöglicht.

8. Die zentrale Adressdatenbank wird über einen SSL-fähigen Web-Browser stark authentifiziert und verschlüsselt bearbeitet.

9. Die UNIX-Systeme der Universitätsverwaltung wurden neu konzipiert und dem gestiegenen sicherheitstechnischen Bedarf entsprechend neu installiert.

10. Die Akzeptanz der Notwendigkeit der Auseinandersetzung mit Problemen der Sicherheit von Rechnernetzen auch in der Verwaltung der Universität konnte erhöht werden.

Fazit:

Zusammenfassend sind wir der Überzeugung, dass wir die im Projektantrag formulierten hohen Zielstellungen erfüllt haben.

- Die Universitätsverwaltung verfügt über einen gesicherten Zugang zu Internet-Diensten.

- Es wurden die ersten Voraussetzungen für eine breite Nutzung von Verschlüsselungs-Technologien an der Universität geschaffen.

- Während der Laufzeit entstanden viele für andere Einrichtungen nachnutzungsfähige Ergebnisse.

- Es wurde uns ermöglicht, die notwendige Thematik tiefgreifend zu bearbeiten und dabei anwendungsbereite Kenntnisse über weitere notwendige Themen zu erlangen.

Nicht zuletzt aufgrund der erreichten Ergebnisse in diesem Projekt ist es gelungen, den Zuschlag für ein nächstes DFN-Projekt zu erhalten, das sich inhaltlich mit der Weiterentwicklung der Thematik "Sicherheit in vernetzen Systemen" beschäftigt:

"Sicher vernetzte Universitätsverwaltung und Dezentralisierung".

3 Projektverlauf und Beschreibung der Arbeitspakete

Ursprünglich war es geplant, die im Projektangebot genannten Teilthemen

1. Grundschutzkonzept und Risikoanalyse
2. Netzstrukturierung
3. Firewall
4. Kommunikationswege unter Umgehung des Firewall-Systems
5. Verschlüsselung und Signatur

zeitlich nacheinander und unter Beachtung der Ergebnisse der vorhergehenden Etappe zu bearbeiten.

Durch seinen praktischen Bezug war das Projekt eng an die Anforderungen der Universitätsverwaltung gekoppelt. Die Ergebnisse flossen direkt in die Vorgänge des Verwaltungsprozesses ein. Einerseits war dies eine große Herausforderung, andererseits beeinflusste es auch die Projektplanung in den einzelnen Phasen. So wurden einzelne Aufgaben aufgrund der Aktualität modifiziert sowie andere hinzugenommen, wenn dies für die Sicherheit des Verwaltungsnetzes erforderlich war. Diese Modifikationen erfolgten dabei grundsätzlich in enger Abstimmung mit dem DFN-Verein.

3.1 Arbeitspaket 1: Grundschutzkonzept und Risikoanalyse

3.1.1 Zielstellung

- Aufbau eines Grundschutzkonzeptes Verwaltungsnetz, wodurch ein Mindeststandard definiert wird, der bereits die Verarbeitung personenbezogener Daten im Netz gestattet. Dieser Standard kann im Einzelfall bei der Verarbeitung sensibler Personendaten erweitert werden.

3.1.2 Ergebnisse

- Durchführung einer Risikoanalyse unter Verwendung des methodischen Instrumentariums des BSI-Sicherheitshandbuches
- Erarbeitung einer Rahmengliederung für ein "Sicherheitskonzept Verwaltungsnetz", nach der bereits in Teilen verfahren wird

Dieses Arbeitspaket bereitete uns große Schwierigkeiten. Richtig ist es, ein Sicherheitskonzept aufzustellen, bevor man an die Umsetzung der in diesem Konzept festgelegten Maßnahmen geht. Außerordentlich schwierig gestaltet sich eine Gefahrenabschätzung in einer Umgebung, wie sie die IT-Infrastruktur der Universitätsverwaltung der Humboldt-Universität darstellt.
Das Instrumentarium des IT-Sicherheitshandbuches des BSI (Version 1.0, Ausgabe 1992) erweist sich als bedingt brauchbar, ein IT-Sicherheitskonzept für eine bestehende IT-Landschaft zu formulieren. Mit den im IT-Sicherheitshandbuch beschriebenen IT-Systemen und Anwendungen ist eine Beschreibung eines modernen heterogenen Netzwerkes mit Client-

Server-Anwendungen schwer durchführbar (...die Personal-Computer sind nicht vernetzt oder auf andere Weise direkt mit anderen Rechnern verbunden[1]).
Es kann bestenfalls zur Unterstützung bei der Erstellung des Konzeptes dienen. Insbesondere erweist es sich als schwierig, die möglichen Schadenshöhen bei den verschiedenen Schadensursachen sinnvoll zu bewerten. Das ebenfalls in die Arbeiten einbezogene IT-Grundschutzhandbuch lag uns in einer Version von 1997 vor und beinhaltete bereits einen großen Teil der Neuerungen in der IT-Landschaft.
Eine Forderung des IT-Sicherheitshandbuches bestimmt die Fortschreibung des IT-Konzeptes. Es kommt darauf an, zu jedem Zeitpunkt eine Analyse der vorhandenen Sicherheitssysteme in der IT-Landschaft vornehmen zu können. Dies ist mit vertretbarem Aufwand nur dann zu erreichen, wenn das IT-Konzept als Report einer Datenbank über die IT-Systeme und Schutzmaßnahmen verstanden wird (Database-Publishing). Ein solcher Ansatz ist in einer mit Java-Frontend ausgestatteten Datenbank-Applikation mit HTML-Output von der Fa. Ploenzke-Informatik im Auftrag des BSI verwirklicht worden[2].

Die Ergebnisse dieses Arbeitspaketes dienen als Grundlage für eine interne "Arbeitsgruppe Sicherheit" des Rechenzentrums, die es sich zur Aufgabe gestellt hat, ein Grundschutzkonzept für alle vom Rechenzentrum betriebenen IT-Systeme zu erstellen.[3]

3.2 Arbeitspaket 2: Netzstrukturierung

3.2.1 Zielstellung

- Ausgehend von der Beschreibung des Vernetzungskonzeptes werden die Sicherheitsrisiken herausgearbeitet und Vorschläge zur Verbesserung des Vernetzungskonzeptes unter Sicherheitsaspekten gemacht.

3.2.2 Ergebnisse

- Beschreibung des Netzwerkkonzeptes des Verwaltungsnetzes
- Erhöhung der Ausfallsicherheit des Verwaltungsnetzes
- Erarbeitung eines Lösungskonzeptes zum sicheren Betrieb von Windows95-PC im Verwaltungsnetz
- Installation von zusätzlichen Sicherheitsmaßnahmen im inneren Verwaltungsnetz

3.2.2.1 Netzwerk-Konzept des Verwaltungsnetzes

Das Verwaltungsnetz der Humboldt-Universität zu Berlin beinhaltet die Gesamtheit aller aktiven und passiven Netzwerkkomponenten sowie die Client-PCs und die zentrale Servertechnik der Universitätsverwaltung. Den Übergang zum Universitätsnetz bildet das Firewall-System, welches über einen Router mit dem Universitäts-Backbone verbunden ist (s. Abbildung 1: Verwaltungsnetz).

[1] BSI Sicherheitshandbuch, Version 1.0, 3.92, Anhang 13, S. 269
[2] http://www.ploenzke.de/de/Story/19990623_bsi/index.cfm?filename=BSI Tool IT-Grundschutz
[3] Anlage 2: Entwurf der Grundschutzbeschreibung für IT-Systeme

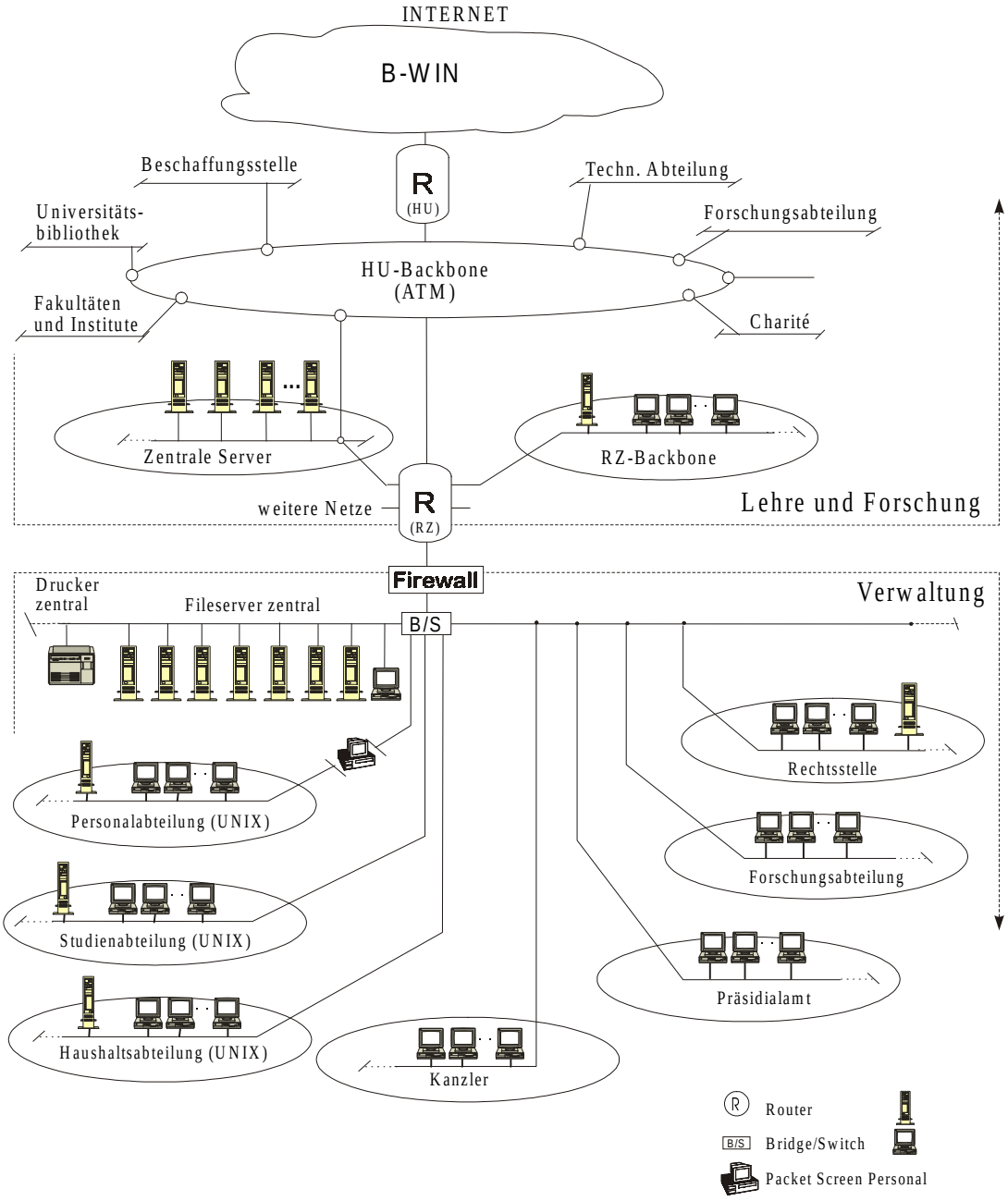

Abbildung 1: Verwaltungsnetz

Die einzelnen Netzwerkknoten werden über Ethernet-Hubs oder -Switches zusammengeführt und laufen im zentralen Rechnerraum der Verwaltung auf. Hier befinden sich die zentralen Netzwerk-Komponenten, die Banyan VINES PC-Netzwerk-Server und die UNIX-Server der Universitätsverwaltung mit den Anwendungsprogrammen für die Haushalts-, Personal- und Studierendendatenverarbeitung.

Zu Projektbeginn wurde eine zentrale Bridge zur Segmentierung und Filterung des gesamten Netzwerkverkehrs innerhalb des Verwaltungsnetzes eingesetzt (s. Abbildung 2: Segmentierung durch Bridge).

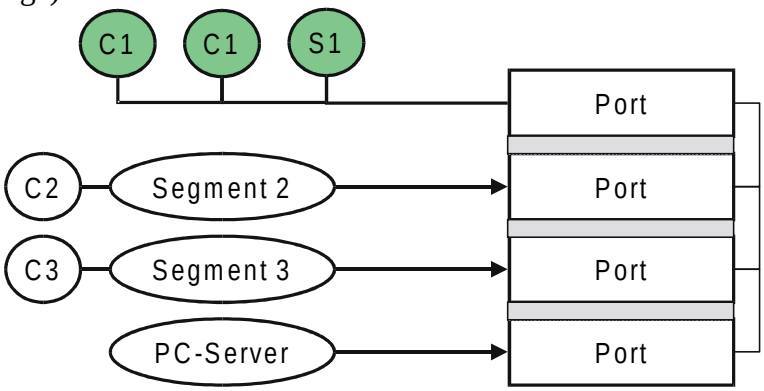

Abbildung 2: Segmentierung durch Bridge

Temporär auftretende Instabilitäten des Netzes konnten auf diese zentrale Bridge zurückgeführt werden. In einem ersten Schritt erfolgte der Austausch dieser Komponente durch eine Bridge höherer Leistungsfähigkeit. Durch diese Maßnahme konnte eine kurzfristige Steigerung der Netzwerkstabilität erreicht werden.
Die Zahl der Teilnehmer des Verwaltungsnetzes wurde weiter erhöht, so dass eine grundsätzliche Änderung des Konzeptes der Segmentierung des Netzes und der Filterung erforderlich war. Aufgrund der sicherheitsrelevanten Protokolleigenschaften von Banyan VINES[4] konnte festgelegt werden:

1. Die Segmentierung des Netzes erfolgt über einen Switch
2. Die MAC-Filterung erfolgt nur noch auf die UNIX-Server

(s. Abbildung 3: Segmentierung durch Switch).

Dieses Konzept ermöglicht eine clientabhängige Positiv-Filterung, da Filter nur noch auf die zu schützenden Server angewendet werden. Infolge dieser Veränderung wurde eine deutliche Erhöhung der Performance und der Ausfallsicherheit des Verwaltungsnetzes erreicht. Die Beschaffung eines Teiles der Switchtechnik wurde über das DFN-Projekt finanziert.

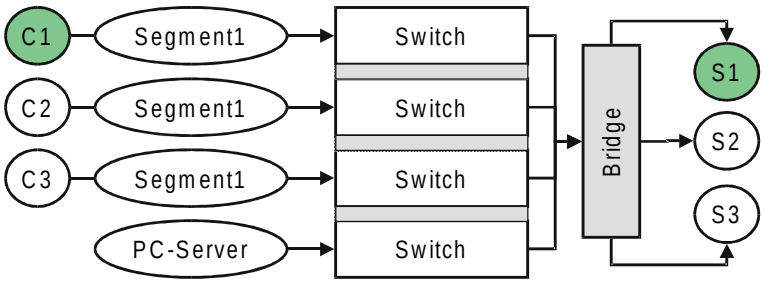

Abbildung 3: Segmentierung durch Switch

[4] Anlage 8: Banyan VINES IP Protokollspezifikation

Wenn die notwendige Firmware zur Anwendung von VLAN-Technologie in den Switches zur Verfügung steht, kann man auf die Filterung durch die Bridge verzichten und verschiedene MAC-basierte virtuelle LANs bilden, in denen sich die einzelnen Clients dann befinden (s. Abbildung 4: VLAN-Konzept).

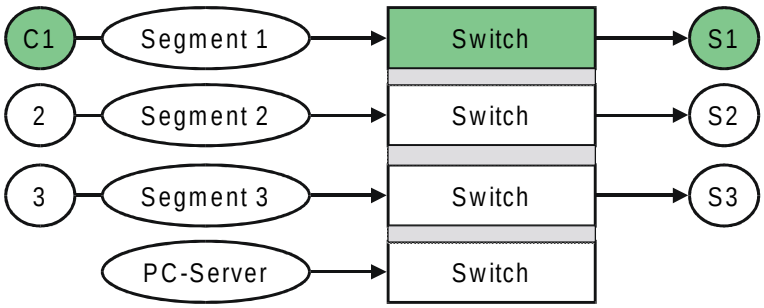

Abbildung 4: VLAN-Konzept

3.2.2.2 Lösungskonzept Betrieb von Windows95-PC

Im Ergebnis einer detaillierten Risikoanalyse entstanden Empfehlungen und Maßnahmen für die sichere Netzwerkanbindung eines Windows95-Clients an das Verwaltungsnetz[5]. Dabei waren insbesondere die Bedingungen des Banyan VINES-Netzwerkes zu berücksichtigen.

3.2.2.3 Zusätzliche Sicherheitsmaßnahmen

Basierend auf den netzwerktechnischen Schutzmaßnahmen wurden die UNIX-Systeme der Personal- und Haushaltsdatenverarbeitung des Verwaltungsnetzes Ende 1999 neu konzipiert und installiert. Dabei wurden folgende Sicherheitsmaßnahmen durchgeführt, die zu einem zusätzlichen Schutz der Systeme führen:

- Härtung des Betriebssystems (Patches, Rechte, Mirroring etc)
- SSH
- TCP-Wrapper
- Logsurfer
- Neuinstallation des Datenbanksystems unter Sicherheitsaspekten.

3.3 Arbeitspaket 3: Firewall

3.3.1 Zielstellung

- Zum Schutz des internen Netzes gegen Angriffe von außen ist ein Übergang zwischen dem sicheren Netzbereich der Zentralen Universitätsverwaltung und dem externen unsicheren Netzbereich zu schaffen.

[5] Anlage 6: Installationsanleitung Windows95 in der ZUV

3.3.2 Ergebnisse

- Neukonzeption und -installation eines Firewall-Systems unter ausschließlicher Verwendung von Open Source Software
- Erhöhung der Kapazität des Firewall-Systems (Einbeziehung von neuen Diensten und eines zusätzlichen Subnetzes)
- Erhöhung der Performance des Firewall-Systems (Austausch der Hardware, Fast Ethernet Konfiguration)
- Detaillierte Dokumentation der Installation

3.3.2.1 Funktionsprinzip des Firewall-Systems

Das Firewall-System, als Schutz des Verwaltungsnetzes gegenüber dem Universitätsnetz konzipiert, ist nach dem Prinzip der "Screened Subnet Architecture" (s. Abbildung 5: Firewall-Konzept) aufgebaut. Dieses Konzept zeichnet sich durch eine erreichbare hohe Sicherheit aus, da es mindestens zwei Barrieren gibt, die von außen überwunden werden müssen, um interne Systeme zu kompromittieren. Innerhalb der IP-Filter befindet sich die "Demilitarisierte Zone" (DMZ), die einen neutralen Übergangsbereich zwischen den Bereichen unterschiedlichen Schutzbedarfes darstellt.

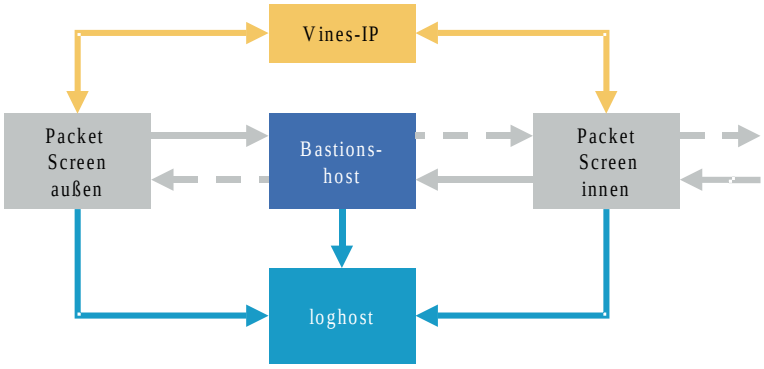

Abbildung 5: Firewall-Konzept

Das Firewall-System besteht aus den Komponenten:

1. IP-Filter außen (Packet Screen)
2. IP-Filter innen (Packet Screen)
3. Application Level Gateway (Bastionshost)
4. Loghost

Der äußere IP-Filter dient dem Schutz der dahinter liegenden Komponenten in der DMZ. Er ist so konfiguriert, dass von außen nur eine Kommunikation zum Bastionshost möglich ist.
Der Bastionshost dient als Proxy für die verschiedenen Dienste, die im Verwaltungsnetz zur Verfügung gestellt werden. Diese wurden in Abstimmung mit der Leitung der Universität und dem Behördlichen Datenschutzbeauftragten nach Tabelle 1: Standard-Applikationen innerhalb des Verwaltungsnetzes festgelegt:

Anwendung	**Dienst**	**Port**
SMTP-Mail ausgehend	smtp	25
nslookup	DNS	53
LDAP-Client	ldap	389
WWW-Browser[6]	http	8000
FTP mit Browser download	ftp	8000

Tabelle 1: Standard-Applikationen innerhalb des Verwaltungsnetzes

In begründeten Ausnahmefällen erfolgt die Freischaltung von zusätzlichen Diensten (z. B. pop3, telnet, Netscape-Calendar). Der zweite IP-Filter dient dem Schutz des dahinter liegenden Netzwerkes und ist so konfiguriert, dass er nur Verkehr zwischen dem Bastionshost und den Clients des Verwaltungsnetzes zulässt. Sämtliche Verstöße gegen die Policy werden auf dem Loghost protokolliert und automatisch ausgewertet.
Durch das verwendete IP-Filter-Konzept wird eine hohe Sicherheit erreicht, weil die eigentlichen Firewall-Komponenten von außen und innen für einen Angreifer nicht sichtbar sind. Die genauere Beschreibung der System-Installation ist der Anlage[7] zu entnehmen.
Mit dieser Form der IP-Filterung wird schon seit langem das Netz der Texas A&M University (ca. 43000 Studierende) und das Netz des DFN-CERT erfolgreich gegen Angriffe aus dem Internet geschützt.

3.3.2.2 Open Source kontra kommerzielle Lösung ?

An dieser Stelle kann keine Grundsatz-Diskussion zu dieser Thematik erwartet werden. Es ist in Fachkreisen inzwischen anerkannt, dass mit einem Open Source System prinzipiell die gleiche Sicherheit erreichbar ist wie mit einem kommerziellen Produkt. Dies zeigt auch, dass zunehmend kommerzielle Angebote entstehen, die Open Source Software aus dem Sicherheitsbereich einsetzen.

3.3.2.3 Entwicklung einer Beispiellösung Firewall-System

Innerhalb des Projektzeitraumes wurden mehrere kommerziell verfügbare Firewall-Systeme evaluiert. Alle betrachteten Systeme ließen sich nicht in die spezielle Netzwerkumgebung der Humboldt-Universität (fehlende Unterstützung von Banyan VINES IP) integrieren. Im Ergebnis der Diskussion mit den Netzwerk-Spezialisten innerhalb des Rechenzentrums wurde festgelegt:

1. Das bisherige Konzept (Screened Subnet mit Application-Level-Gateway) wird beibehalten.
2. Es sollen möglichst zwei Hersteller an der Lösung beteiligt sein.
3. Das Konzept soll modular sein, d. h. Änderungen des Firewall-Konzeptes sollten keine komplette Neubeschaffung erfordern.
4. Es sollen möglichst viele Stufen des Schutzes vorhanden sein.

[6] bei HTTP erfolgt eine Filterung von ActiveX, Java und JavaScript
[7] Anlage 9: Sicherheitsrelevante Komponenten des Verwaltungsnetzes

Nach der Neubeschaffung der Hardware[8] wurde das Firewall-System im September 1999 unter ausschließlicher Verwendung von Open Source Software neu installiert.

Innerhalb des Projektzeitraumes wurden immer wieder Angriffsversuche von außen auf das Netz der Universitätsverwaltung bemerkt, sind jedoch nach unserem derzeitigen Kenntnisstand davon überzeugt, dass es bei keinem der Versuche gelungen ist, sich über diesen Weg Zugang zum Verwaltungsnetz zu verschaffen.

3.4 Arbeitspaket 4: Kommunikationswege unter Umgehung des Firewall-Systems

3.4.1 Zielstellung

- Für die Unix-Server der Studien-, Personal- und Haushaltsabteilung soll ein Sicherungs- und Archivierungskonzept entwickelt werden, das die im RZ verfügbaren technischen Ressourcen zur Archivierung nutzt, ohne das Firewall-System zu umgehen.
- Es erfolgt die Recherche nach Hard- und Software, mit der unerlaubte Fax-Anschlüsse im Verwaltungsnetz detektiert werden können.

3.4.2 Ergebnisse

3.4.2.1 Sicherungs- und Archivierungskonzept

Es entstand ein Konzept zur Einbindung in das Archivierungs-Gesamtsystem der Humboldt-Universität auf der Basis von UniTree und dem Tape-Robotersystem. Unmittelbar danach wurde die strategische Entscheidung getroffen, das Archivsystem der Universität zu modernisieren, um den gestiegenen Anforderungen durch den Standort Adlershof gewachsen zu sein. In Absprache mit dem DFN-Verein wurde festgelegt, die in diesem Arbeitspaket zu behandelnde Thematik noch einmal in einem folgenden Projekt aufzugreifen.

3.4.2.2 Hard- und Software-Recherche

Die Suche nach geeigneter Software zur Detektion von unerlaubten Modem-Verbindungen im Verwaltungsnetz gestaltete sich problematischer als erwartet. Deshalb können zu diesem Punkt keine Ergebnisse vorgelegt werden. Durch den verstärkten Einsatz von zentralen Management-Lösungen im Netzwerkbereich kommen Aspekte hinzu, die den ursprünglich betrachteten Schwerpunkt dieser Aufgabenstellung verschieben und ein erneutes Aufgreifen verlangen:

- Analyse der verwendeten Systeme zur Netzwerk-Administration (snmp, telnet)
- Sicherheitstechnische Beurteilung und Gefahrenabschätzung
- Erarbeitung von Lösungsvorschlägen zur Erhöhung der Sicherheit

[8] Anlage 12: Beschaffungsliste für die Firewall-Komponenten

Arbeitspaket 5: Verschlüsselung und Signatur

3.4.3 Zielstellung

- Mit zunehmender Vernetzung wird die sichere Übermittlung von Daten immer bedeutsamer. Durch den Einsatz suffizienter Verschlüsselung soll die Sicherheit, Integrität und Unfälschbarkeit der transportierten Daten gewährleistet werden.
- In enger Abstimmung mit dem DFN-Projekt "Policy Certification Authority" (PCA) wird eine HU-interne Zertifizierungshierarchie aufgebaut.

3.4.4 Ergebnisse

- Aufbau und Betrieb einer Zertifizierungsinstanz für PGP und S/MIME SSL für die Humboldt-Universität
- Bearbeitung von Personaldaten durch Nutzung von stark authentifizierten und verschlüsselten Verbindungen
- stark authentifizierte und gesicherte Bearbeitung der Adressdatenbank der Universitätsverwaltung über einen SSL-fähigen Web-Browser
- SSH-basierte Administration der UNIX-Server
- Schaffung der Voraussetzungen für die Fern-Administration der Systeme der Haushalts-Datenverarbeitung für die Mitarbeiter der HIS-GmbH

3.4.4.1 Zertifizierungsinstanz der Humboldt-Universität zu Berlin (HU-CA)

Die Voraussetzungen für den Betrieb einer Zertifizierungsinstanz wurden geschaffen und es entstand eine Policy, welche innerhalb des Rechenzentrums, mit dem Behördlichen Datenschutzbeauftragten der Humboldt-Universität und inhaltlich korrelierenden DFN-Projekten (DFN-PCA, AMBIX) abgestimmt wurde. Im Dezember 1997 wurde der interne Testbetrieb der Zertifizierungsinstanz (HU-CA) und der Unter-Zertifizierungsinstanz des Rechenzentrums (RZ-DCA) begonnen. Auf Beschluss der SKR[9] begann im Februar 1998 der reguläre Betrieb der CA. Eine aus den Mitteln des DFN-Projektes beschaffte Sun-Workstation dient als WWW-Server der CA. Hier erfolgt die Beantragung, Versendung und Veröffentlichung von Zertifikaten für PGP und S/MIME für die Studierenden und Mitarbeiter der Universität. Zur Veröffentlichung der Zertifikate wurden ein PGP-Keyserver sowie ein LDAP-Directoryserver installiert. Die Mitarbeiter und Studierenden der Humboldt-Universität, die einen UNIX-Account im Rechenzentrum haben, bekamen die Möglichkeit, über eine von der HU-CA zertifizierte verschlüsselte Verbindung, ihre Mail sicherer über das Internet zu lesen. Die Zertifizierung der SSL-Schlüssel der HU-CA durch die DFN-PCA wurde Ende Dezember 1998 beantragt und erfolgte im ersten Quartal 1999.

An dieser Stelle soll auf die umfangreichen Web-Ressourcen verwiesen werden, die im Verlauf der Projektarbeit zur Thematik der Verschlüsselung und Signatur entstanden: https://ca.hu-berlin.de/

[9] Senatskommission für Rechentechnik

3.4.4.2 Dezentraler Zugriff auf Personaldaten

Dezentralisierungstendenzen innerhalb der Verwaltung der Universität machten es erforderlich, einen Zugang zu den zentralen UNIX-Servern vom Universitätsnetz ausgehend zu ermöglichen. Anfang 1998 wurde eine diesbezügliche technische Lösung auf der Basis von SSH und ACE-Server zur Verfügung gestellt. Das Pilotprojekt konnte Anfang 2000 erfolgreich abgeschlossen werden.
Eine Anwendung der Zertifizierungsinstanz ist die stark authentifizierte und verschlüsselte Bearbeitung der zentralen Adressdatenbank der Universitätsverwaltung über einen SSL-fähigen Web-Browser.

3.4.4.3 SSH-basierte Administration

Die Systeme der UNIX-Server wurden mit SSH ausgestattet, um die Administration sicherer zu gestalten. SSH verwendet das asymmetrische RSA-Verfahren zur starken Authentifizierung der Kommunikationspartner und ein symmetrisches Verfahren zur Verschlüsselung der übertragenen Daten. Nicht zuletzt durch die Vorbildwirkung des Projektes erfolgt inzwischen sämtlicher administrativer Zugriff auf die Server des Rechenzentrums mit SSH.

4 Öffentlichkeitsarbeit

Anfang Februar 1998 wurden die Ergebnisse und Erfahrungen des Projektes auf einem Arbeitstreffen der Zertifizierungsinstanzen in Jena vorgestellt und mit den Teilnehmern diskutiert. Es erschien ein Artikel, der sich mit grundsätzlichen Fragen zur Problematik von Sicherheitskonzepten beschäftigt:[10]

Am Rechenzentrum der TU Wien fand im Mai 1998 ein Vortrag zur Thematik der Rechnersicherheit statt: "Angriffsszenarien und Verteidigungsstrategien in öffentlichen Netzwerken"[11].

In der Zeitschrift RZ-Mitteilungen, die vom Rechenzentrum der Humboldt-Universität herausgegeben wird, erschienen zwei Beiträge:

- "Vertrauen gegen Vertrauen" - Die Zertifizierungsinstanz der Humboldt-Universität zu Berlin[12]
- Sicher vernetzte Universitätsverwaltung - Bericht über die erste Phase eines Drittmittelprojektes im Rechenzentrum[13]

Auch innerhalb unserer Universität erlangte die Thematik der Netzwerksicherheit einen wachsenden Stellenwert. So konnte es als Erfolg verbucht werden, dass im Februar 1999 ein zweitägiger Weiterbildungs-Lehrgang am Rechenzentrum angeboten wurde. Die Veranstaltung beinhaltete die Themen der Internet-Sicherheit von UNIX-Systemen und eine Einführung in die Verschlüsselungs-Thematik. Zielgruppe dieser Veranstaltung waren die Syste-

[10] Anlage 3: Sicherheitskonzept, aber wie?
[11] http://www.edvz.tuwien.ac.at/security/
[12] http://www.hu-berlin.de/rz/rzmit/rzm16/2.html
[13] http://www.hu-berlin.de/rz/rzmit/rzm16/3.html

madministratoren der Universität. Hier wurde ein Überblick über Probleme und Gefahren beim Betrieb von UNIX-Systemen in Netzwerken, speziell beim Betrieb im Internet, aufgezeigt.

Am 23. Juni 1999 fand ein offenes RZ-Kolloquium im Senatssaal der Humboldt-Universität zu Berlin statt, auf dem die Ergebnisse des Projektes in einer Reihe von Vorträgen dargeboten wurden. Hier wurden 150 DV-Entscheidungsträger und -Organisatoren aus ganz Deutschland über die organisatorischen und technischen Maßnahmen informiert, die ein Anschluss des Verwaltungsbereiches einer öffentlichen Einrichtung an das Internet erfordert. Im Einzelnen fanden Vorträge zu folgenden Themen statt:

- Was hat die Universitätsverwaltung von sicheren Netzen - Einschätzung aus Verwaltungssicht
- Das Vernetzungs- und Firewall-Konzept der Universitätsverwaltung - jetziger Stand und Weiterentwicklung
- Authentisierte und verschlüsselte Verbindungen - Ergebnisse des Pilotprojektes "Verwaltung studentischer Beschäftigter in den Organisationseinheiten"
- Zertifikatsbasierter Fernzugriff auf Personendatenbanken - Erste Erfahrungen und Empfehlungen
- Gesicherter Web-Aufsatz für die Adressdatenbank - Datenpflege per Web.

Im September 1999 wurde anlässlich des Semesterbeginns ein Poster veröffentlicht, über das die Mitarbeiter und Studierenden der Universität angeregt werden sollen, Sensibilität für Probleme der Netzwerk-Sicherheit und der allgemeinen Verschlüsselungs-Technologien zu entwickeln.
Im Januar 2000 fand für die Mitglieder der "Steuerungsgruppe Verwaltungsnetz"[14] der Universitätsverwaltung eine Sitzung statt, in der die Risiken bei der Nutzung von aktiven Web-Inhalten demonstriert wurden[15]. Im Ergebnis wurde festgelegt, das für das Verwaltungsnetz festgelegte Sicherheitskonzept beizubehalten, welches die Filterung der aktiven Komponenten aus den Web-Angeboten nicht hinreichend untersuchter Anbieter vorsieht.

[14] Gremium zur Ziel- und Prioritätensetzung im Verwaltungsnetz
[15] Anlage 22: Inhalt Vortrag "Sicherheitsrisiken bei aktiven Web-Inhalten"

5 Anlagen

1. Gliederung des Sicherheitskonzeptes der Verwaltung
2. Entwurf Grundschutzbeschreibung für IT-Systeme
3. Sicherheitskonzept - Aber wie ?
4. RZ-Mitteilungen Nr. 16 (2)
5. Empfehlungen und Maßnahmen zur sicheren Windows95-Installation im Verwaltungsnetz
6. Installationsanleitung Windows95
7. Inhalt Vortrag RZ-Kolloquium "Weiterentwicklung des Vernetzungskonzeptes der ZUV"
8. Banyan VINES IP Protokollspezifikation
9. Sicherheitsrelevante Komponenten des Verwaltungsnetzes
10. Einführung in die Firewall-Thematik
11. Konzept zur Evaluierung eines Firewall-Systems
12. Beschaffungsliste für die Firewall-Komponenten
13. Inhalt Sicherheitsseminar Humboldt-Universität zu Berlin
14. RZ-Mitteilungen Nr. 16 (1)
15. Policy der Certification Authority der Humboldt-Universität zu Berlin
16. Administrationsanleitung HU-CA
17. Inhalt Vortrag "Das Vernetzungs- und Firewall-Konzept der Universitätsverwaltung"
18. Inhalt Vortrag "Stark authentisierte und verschlüsselte Verbindungen"
19. Inhalt Vortrag "X.509-zertifikatsbasierter Fernzugriff auf Datenbanken"
20. Inhalt Poster "Sicherheitstechnologien im Internet"
21. Abbildung "Pilotprojekt Studentische Hilfskräfte"
22. Inhalt Vortrag "Sicherheitsrisiken bei aktiven Web-Inhalten"
23. Weiterführende Literatur

6 Glossar

- **ACE** Access Control Encryption
- **BSI** Bundesamt für Sicherheit in der Informationstechnik
- **CA** Certification Authority, Zertifizierungsinstanz oder Beglaubigungsstelle
- **DCA** Deligated Certification Authority, Untergeordnete Zertifizierungsinstanz
- **DFN** Verein zur Förderung eines deutschen Forschungsnetzes
- **IT** Informationstechnik
- **LAN** Local Area Network
- **PGP** Pretty Good Privacy, Software zur Verschlüsselung unter Nutzung von Public-Key-Verfahren
- **Public-Key-Verfahren** Daten, die mit einer allgemein zugänglichen Bytefolge, dem öffentlichen Schlüssel, verknüpft wurden, können nur mit einem (geheimen) privaten Schlüssel des Empfängers eingesehen werden
- **RZ** Rechenzentrum
- **SSH** Secure Shell
- **SSL** Secure Socket Layer, standardisiertes Protokoll zur Verschlüsselung des Datentransportes, welches zwischen Transport- und Netzwerk-Schicht liegt
- **VLAN** Virtuelles LAN
- **ZUV** Zentrale Universitätsverwaltung