



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

3. Zwischenbericht

30. August 1999

Auftragnehmer	Humboldt-Universität zu Berlin ZE Rechenzentrum
Kennzeichen	TK 598-SD027
Kurzbezeichnung	Firewall
Laufzeit des Vorhabens	25.08.97 - 31.08.99
Berichtszeitraum	01.09.98 - 15.03.99
Projektleitung	Dr. P. Schirnbacher
Fachliche Betreuung	D. Natusch
Projektdurchführung	A. Geschonneck R. Herbst

Anlagen:

1. Unterlagen „Weiterentwicklung Vernetzungskonzept der ZUV“
2. Beschaffungsliste für die Firewall-Komponenten
3. Inhalt Sicherheitsseminar HU-Berlin
4. Screenshots der Anwendungen

Inhalt

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

Allgemeines

Dieser Bericht soll die erreichten Ergebnisse und aufgetretenen Probleme kurz skizzieren. Außerdem wird auf die Anlagen und die umfangreichen WWW-Ressourcen unseres Projektes¹² verwiesen.

Für die Mitarbeiter und Administratoren der Fachbereiche und Zentraleinrichtungen der Humboldt-Universität zu Berlin wurde ein zweitägiges Seminar zum Thema „Sicherheit von Unix-Systemen / Netzwerksicherheit /Verschlüsselung“ durchgeführt. Hier wurde ein Überblick über Gefahren und Probleme beim Betrieb von UNIX-Systemen in Netzwerken aufgezeigt. Gleichzeitig konnten die Teilnehmer nützliche Hinweise für den sicheren Betrieb der eigenen Systeme bekommen.

Der Umgang mit Zertifikaten und die Beantragung bei der HU-CA war neben den Grundlagen für Public Key Infrastructures Thema des zweiten Tages. Das Projektteam erhofft sich, durch diese Veranstaltung mehrere Multiplikatoren für die Ziele und Ergebnisse dieses Projektes zu erlangen.

Das Projektteam konnte zum Jahresanfang neue Räume beziehen.

Arbeitspaket 1: Grundschutzkonzept und Risikoanalyse

Zielstellung

- Aufbau eines Grundschutzkonzepts 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.

Ergebnisse

Die Ergebnisse dieses Themas sind im ersten Zwischenbericht enthalten.

¹ <http://www.hu-berlin.de/projekte/fw/>

² <http://ca.hu-berlin.de/>

Arbeitspaket 2: Netzstrukturierung

Zielstellung

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

Ergebnisse

Das Vernetzungskonzept wurde kontinuierlich weiterentwickelt. Es wurden die Voraussetzungen für eine künftige VLAN-Struktur ausgearbeitet und mit der Umsetzung der dazu erforderlichen Maßnahmen wurde teilweise begonnen (s. Anlage) Die Ergebnisse wurden anlässlich eines internen RZ-Kolloquiums vorgestellt. Kern der Umstellung ist die Ablösung der zentralen Bridge zur Netzsegmentierung durch einen Switch. Der Einsatz der Bridge dient nunmehr nur noch der Filterung des IP-Verkehrs auf die zentralen Unix-Server. Dieses Konzept ermöglicht eine client-abhängige Positiv-Filterung, welches der Policy für das Verwaltungsnetz entspricht. Außerdem versprechen wir uns mit dieser Maßnahme eine weitere Erhöhung der Performance des Netzes, da Filter nur noch auf die zu schützenden Server angewendet werden.

Arbeitspaket 3: Firewall

Zielstellung

- Schutz des internen Netzes gegen Angriffe von außen
- einziger Übergang zwischen dem sicheren Netzbereich der Zentralen Universitätsverwaltung (ZUV) und dem externen unsicheren Netzbereich
- Schutz der übertragenen Daten gegen Angriffe auf deren Vertraulichkeit und Integrität

Aktivitäten

- Ausführliche Dokumentation des bestehenden Firewall-Systems
- Test von Software zur Unterstützung der Administration des Firewall-Systems (GUI)
- Erstellung von kleinen „Helper“-Applikationen
- Test von Firewall-Systemen

Ergebnisse

Die Beschaffung für die neuen Firewall-Komponenten wurde ausgelöst. Eine detaillierte Aufstellung der Komponenten findet sich in den Anlagen.

In Hinsicht auf die Modularität der zu beschaffenden Firewall-Lösung wurden verschiedene Varianten der Implementierung des neuen Systems gemeinsam mit den Netzwerkexperten des RZ diskutiert. Im Ergebnis wurde folgendes festgelegt:

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

Die Beschaffung der Firewall-Software wird in der nächsten Projektphase erfolgen, da diesbezüglich noch Implementierungstests stattfinden. (siehe Anlage)

Die Hilfsmittel zur Administration des Firewall-Systems wurden weiter verbessert. (siehe Abbildung 1)

Arbeitspaket 4: Kommunikationswege unter Umgehung des Firewall-Systems

Zielstellung

- Entwicklung eines Sicherungs- und Archivierungskonzepts für die Unix-Server der Studien-, Personal- und Haushaltsabteilung auf Basis von UniTree und Convex-Robotersystem (im RZ vorhanden bzw. mit RZ-Mitteln erweiterbar). Es ist noch zu entscheiden, ob dedizierte Netzverbindungen zum RZ (außerhalb der Firewall) oder vorhandene Verbindungen (über die Firewall) genutzt werden
- Recherche nach Hard- und Software, mit der unerlaubte FAX-Anschlüsse im Verwaltungsnetz detektiert werden können.

Ergebnisse

In Absprache mit dem DFN-Verein wurde festgelegt, diese Thematik noch einmal in einem folgenden Projekt aufzugreifen. Das neue Archivsystem für die Humboldt-Universität befindet sich noch in der Beschaffungsphase. Durch den verstärkten Einsatz von zentralen Management-Lösungen im Netzwerkbereich kommen Aspekte hinzu, die den Schwerpunkt dieser Aufgabenstellung verschieben.

Arbeitspaket 5: Verschlüsselung und Signatur

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
- Aufbau einer HU-internen Zertifizierungshierarchie in enger Abstimmung mit dem DFN-Projekt „Policy Certification Authority“ (PCA)

Aktivitäten

- Das Pilotprojekt Studentische Hilfskräfte (s. erster Zwischenbericht) wurde fortgeführt
- Es werden die Möglichkeiten untersucht, diese Lösung auch für künftige ähnlich geartete Aufgabenstellungen zu verwenden (Verwendung von Public-Key-Verfahren zur sicheren Übertragung beliebiger TCP/IP-basierender Applikationen , z.B. *HiSecure*)
- Es werden die Voraussetzungen für eine routinemäßige Beantragung, Erteilung und Veröffentlichung von Zertifikaten für PGP und S/MIME im Rechenzentrum der HU geschaffen.

- Mitarbeit bei der Entwicklung eines Verfahrens zur digitalen Signatur von Elektronischen Dokumenten und der Möglichkeit, Zertifikate zu über das Netz zu verifizieren

Ergebnisse

Die Akzeptanz der Zertifizierungsinstanz wurde innerhalb der Universität weiter ausgebaut. Die Zahl der Interessenten aus dem Verwaltungsbereich ist gestiegen. Dies ist unter anderem darauf zurückzuführen, daß die Adreßdatenbank der Universität jetzt im WWW auch für die Änderung zur Verfügung steht. Die Änderung der Daten kann nur mit einem gültigen persönlichen Zertifikat der HU-CA erfolgen. (Abbildung 2)

Nachdem sich der Berechtigte mit seinem Zertifikat authentisiert hat, bekommt er Zugang zur Änderungsmaske. Die Änderungen werden sofort über verschiedene Konnektoren in der Sybase-Datenbank erfaßt. (Abbildung 3)

Weiterhin ist der Zugang zu den internen IP-Konfigurationen nur mit einem persönlichen Zertifikat der HU-CA möglich. (Abbildung 4)

Den Mitarbeitern und Studenten der Humboldt-Universität zu Berlin, die ihren 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. (Abbildung 5)

Um die Administration der Zertifikate zu erleichtern wurde auf den Zertifizierungsrechnern ein einfaches Werkzeug erstellt, mit dem dann die mit der Bearbeitung betrauten Mitarbeiter einfacher Zertifikate erstellen können. (Abbildung 6, Abbildung 7, Abbildung 8, Abbildung 9)

Der Verzeichnisdienst der HU-CA wurde mit dem Netscape-Directory Server und dem web500gw von Frank Richter (TU-Chemnitz) realisiert. Hier können die veröffentlichten Zertifikate und deren Gültigkeit einfach überprüft werden. (Abbildung 10)

Problematisch erschien uns, daß die von uns verwendete freie australische Software SSLeay durch das Unternehmen RSA Inc. samt Entwicklern gekauft wurde. Der nun maßgeblich in Europa entwickelte Nachfolger OPENSSL wird aber sehr bald die Nachfolge auch bei der HU-CA antreten. Um die Entwicklung genau zu verfolgen, wurde ein FTP-Mirror eingerichtet. (<ftp://ftp.rz.hu-berlin.de/pub/security/openssl/>)

Die Zertifizierung unserer SSL-Schlüssel durch die DFN-PCA wurde Ende Dezember 1998 beantragt.

Abbildung 1: Hauptmenü zur Administration der Paket-Filter 6

Abbildung 2: Der Anwender muß sein persönliches Zertifikat angeben 7

Abbildung 3: zertifikatgeschützter WWW-Zugang zur zentralen Adreßdatenbank..... 7

Abbildung 4: zertifikatgeschützter WWW-Zugang zur internen IP-Datenbank..... 8

Abbildung 5: verschlüsselter Zugang zur IMAP-Mail 9

Abbildung 6: Hauptmenü des HU-CA Admintools..... 9

Abbildung 7: SSL-Untermenü des HU-CA Admintools 10

Abbildung 8: Clientzertifikate ausstellen mit dem HU-CA Admintool 10

Abbildung 9: PGP-Untermenü des HU-CA Admintools..... 10

Abbildung 10: WWW-Interface zum LDAP-Verzeichnisdienst der HU-CA 11

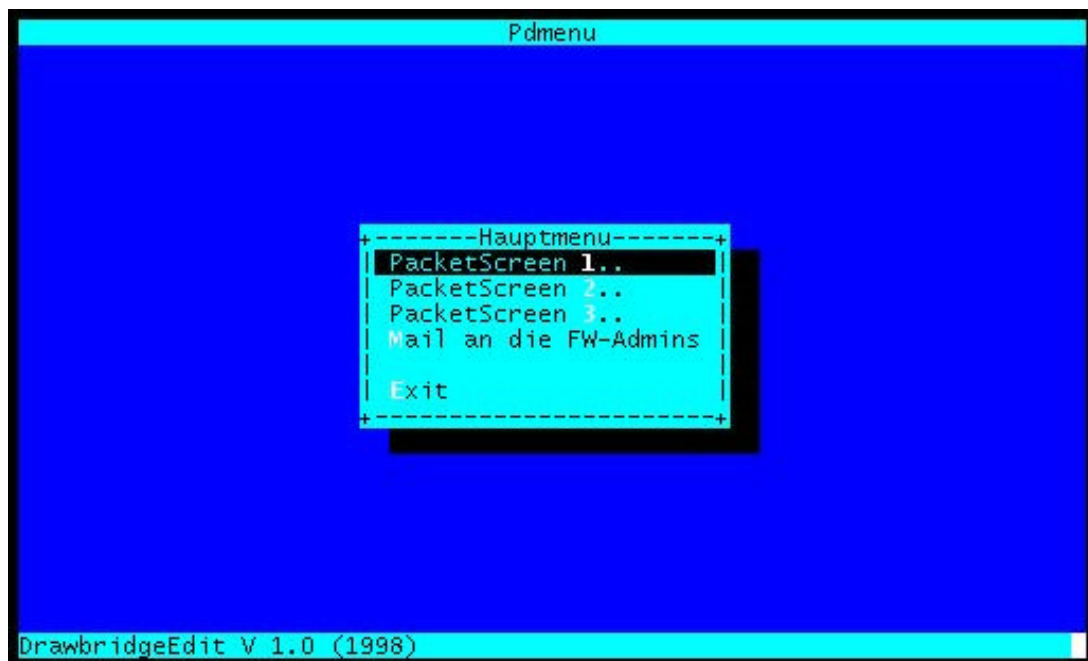


Abbildung 1: Hauptmenü zur Administration der Paket-Filter



Abbildung 2: Der Anwender muß sein persönliches Zertifikat angeben



Abbildung 3: zertifikatgeschützter WWW-Zugang zur zentralen Adreßdatenbank

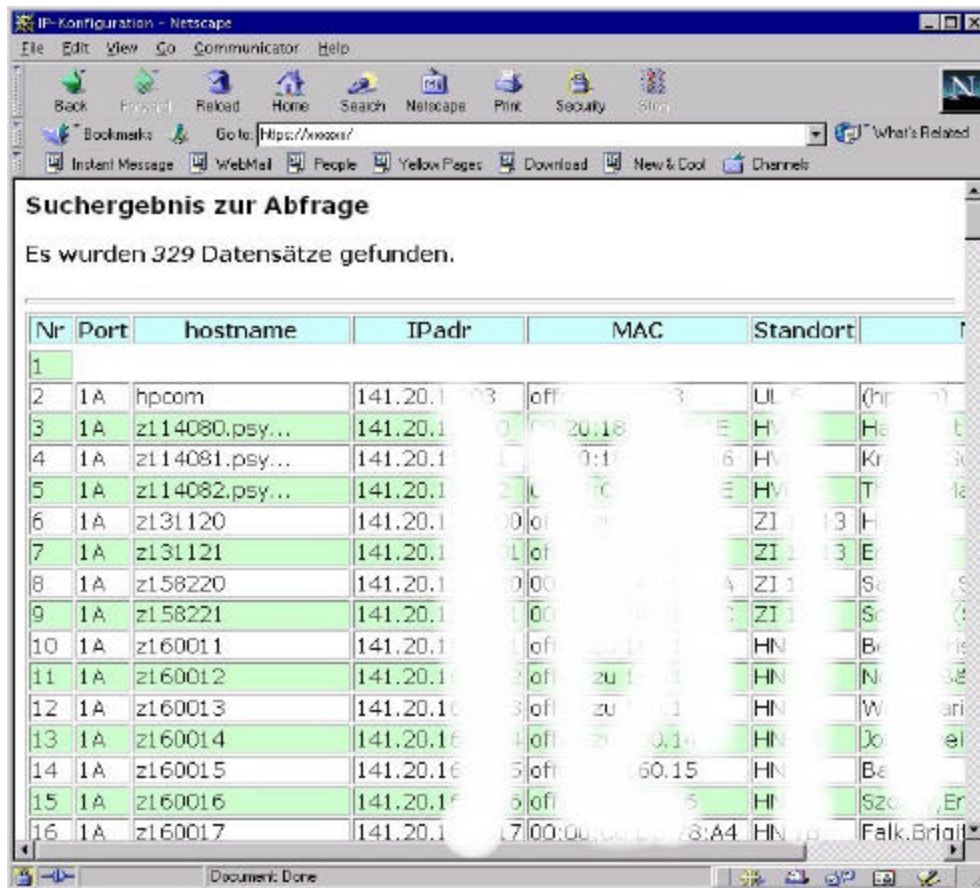


Abbildung 4: zertifikatgeschützter WWW-Zugang zur internen IP-Datenbank

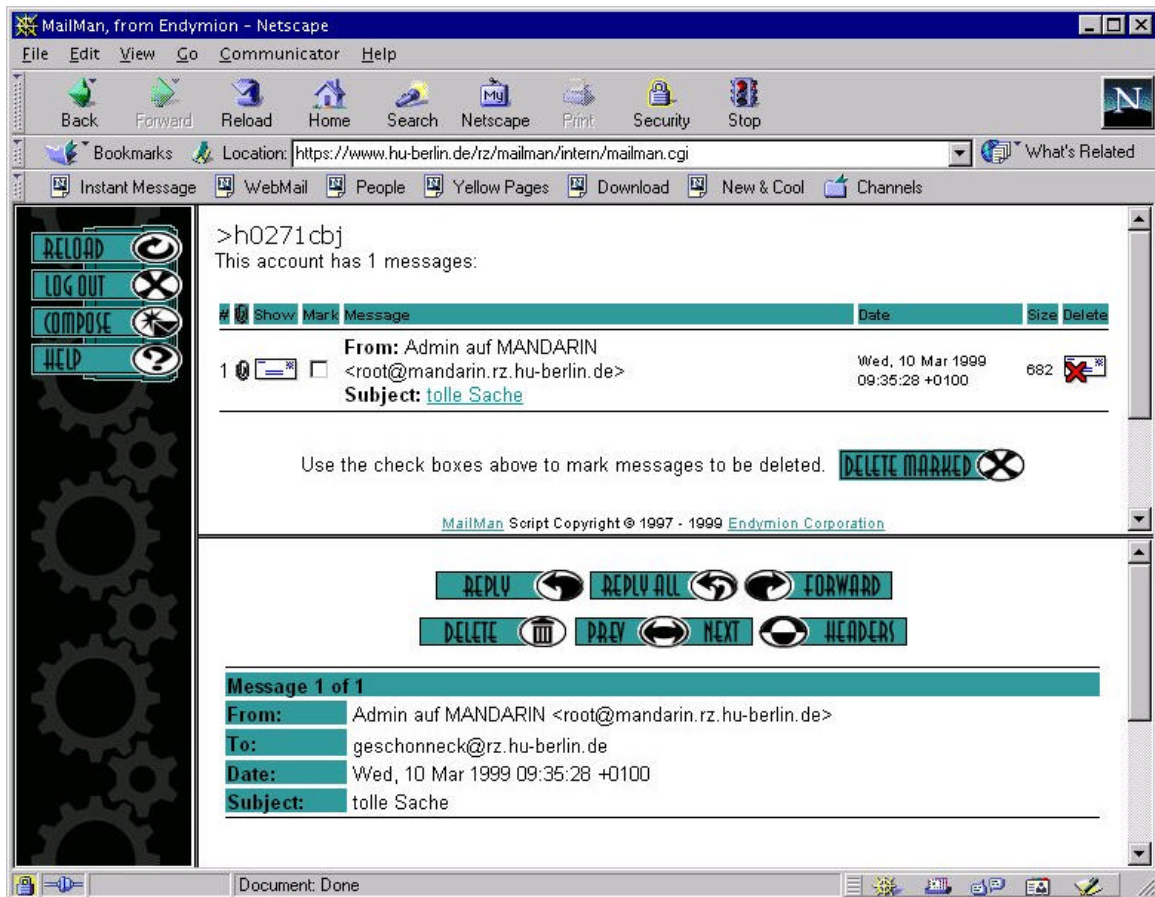


Abbildung 5: verschlüsselter Zugang zur IMAP-Mail



Abbildung 6: Hauptmenü des HU-CA Admintools



Abbildung 7: SSL-Untermenü des HU-CA Admintools



Abbildung 8: Clientzertifikate ausstellen mit dem HU-CA Admintool



Abbildung 9: PGP-Untermenü des HU-CA Admintools

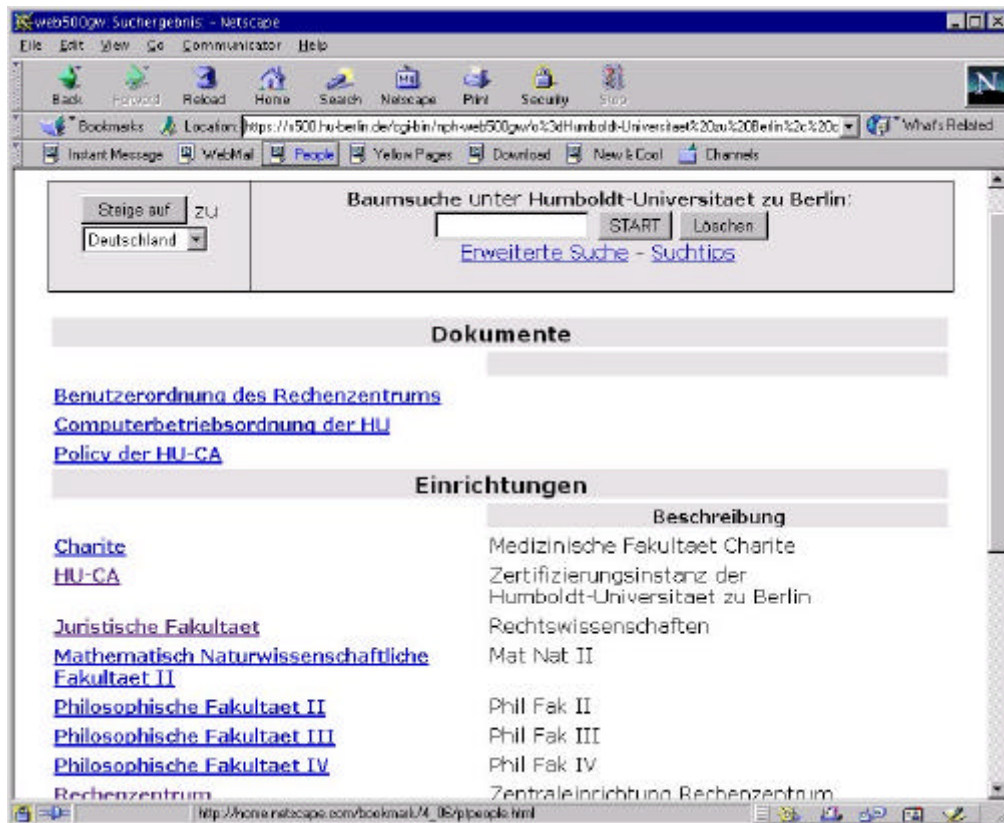


Abbildung 10: WWW-Interface zum LDAP-Verzeichnisdienst der HU-CA