Sicher vernetzte Universitätsverwaltung und Dezentralisierung (UVsec)

Die Ausgangssituation

An vielen Hochschulen und ebenso an der Humboldt-Universität (HU) werden Tendenzen der Dezentralisierung von Verwaltungsaufgaben immer deutlicher, d. h. Aufgaben, Kompetenzen und Verantwortung werden in die Fakultäten und Institute verlagert. In der zentralen Verwaltung wird vorrangig die formale Umsetzung der Entscheidungen belassen. Schon heute besitzen nahezu alle Mitarbeiterinnen und Mitarbeiter der Verwaltung einen Zugang zum Verwaltungs- und Universitätsnetz und damit zu Internet-Services wie E-Mail, WWW und Verzeichnisdiensten. Das Verwaltungsnetz mit seinen Personal-, Haushalts- und Studierendendaten wird gegenüber dem Universitätsnetz und dem Internet durch ein Firewall-System, einer Kombination aus IP-Filtern und Proxies, geschützt. Eine Verbindung von außen in den geschützten Bereich hinein (Inbound Connection) wird derzeit nicht gestattet. Im Zuge der fortschreitenden Dezentralisierung müssen solche Verbindungen jedoch ermöglicht werden, so dass ausgewählten Mitarbeiterinnen und Mitarbeitern der Fakultäts- und Institutsverwaltungen sensible Daten zugänglich werden.

Will man einen geschützten Bereich gezielt nach außen öffnen, bedarf es zusätzlich zum netzwerktechnischen Schutz der Clients und Server durch ein Firewall-System spezieller Mechanismen einer Authentifizierung des zur Nutzung der Dienste berechtigten Personenkreises und einer genauen Kontrolle der gestatteten Rechte (Autorisierung). In diesen Fällen sind Authentifizierungsmechanismen durch Verwendung von Login und zugehörigem Passwort sicherheitstechnisch nicht mehr ausreichend, so dass es neuer Verfahren zur Feststellung der Identität des Nutzers bedarf. Ein Ansatz ist es, diese Authentifizierung aufgrund von beglaubigten öffentlichen Schlüsseln (X.509-Zertifikaten) vorzunehmen. Schon 1998 wurde dazu eine Zertifizierungsinstanz der HU (die HU-CA) gegründet, die ihrerseits durch die DFN-Wurzelzertifizierungsinstanz beglaubigt ist (DFN-PCA).

Doch so vielgestaltig wie das Internet selbst, so vielgestaltig ist auch der Markt für Sicherheitstechnologien. Neben dem schon genannten Schlagwort *Firewall* gibt es hier eine Reihe von Begriffen, die immer wieder im Zusammenhang mit Netzwerksicherheit zu hören sind, wie etwa VPN, IPsec, LDAP, SmartCard, PKI oder IDS.

In zwei vom DFN-Verein geförderten Projekten wird der Frage nachgegangen, wie die angesprochenen Aufgaben in der Verwaltung zu lösen sind und wie darüber hinaus einzelne Sicherheitsprodukte zu installieren und in den Regelbetrieb zu überführen wären. Das erste im Januar 2000 erfolgreich abgeschlossene Projekt *Firewall – ein Kernstück zur Sicherung des Verwaltungsnetzes (Firewall)* – beinhaltete die schon erwähnte Anbindung des Verwaltungsnetzes an das Universitätsnetz. Innerhalb dieses Projektes konnten auch erste Erfahrungen bei der Benutzung digitaler Signaturen gesammelt werden. Das Projekt *Sicher vernetzte Universitätsverwaltung und Dezentralisierung (UVsec)* nutzt diese Erfahrungen und baut sie weiter aus.

Ziel des Projektes UVsec

Entsprechend den Dezentralisierungsbestrebungen müssen neue, sichere Verfahren der Kommunikation, des Austausches und der gemeinsamen Bearbeitung von Datenbeständen zwischen zentraler und dezentraler Verwaltung gefunden werden. Auf diese neuen Anforderungen an die Universitätsverwaltung müssen sich die Vernetzungsspezialisten der Hochschulen mit geeigneten Konzepten vorbereiten. Die Hauptzielstellung des Projektes UVsec besteht deshalb in der *Ausweitung des Vernetzungs- und Sicherheitskonzeptes auf die Fakultätsverwaltungen unter vorrangiger Betrachtung der Schnittstellen zwischen zentraler und dezentraler Hochschulverwaltung*.

Um das allgemeine Projektziel zu erreichen, wurden sechs Schwerpunktthemen formuliert, die im Folgenden genannt und im nächsten Abschnitt erläutert werden.

1. Weiterentwicklung des Firewallkonzeptes unter dem Aspekt der definierten Öffnung gegenüber den dezentralen Verwaltungsbereichen
2. Analyse der Bedrohungen, die sich aus der Umgehung des Firewallsystems ergeben – Konzipierung und Durchführung von Gegenmaßnahmen
3. Erprobung des Einsatzes von SmartCards in der Universitätsverwaltung
4. Kryptografische Verfahren auf Netzwerk-Ebene
5. Entwicklung von Referenzlösungen für ausgewählte DV-Systeme der Universitätsverwaltung
6. Dokumentation – Veröffentlichung eines Leitfadens für ein sicheres Verwaltungsnetz in Form eines DFN-Berichts

Die Projektbeschreibung wurde in das WWW-Informationssystem des Rechenzentrums der HU eingebunden und ist öffentlich über die Adresse *http://www.hu-berlin.de/rz/projekte/uvsec/* zu erreichen.

Aufgaben des Projektes UVsec

Zu allen im Folgenden aufgeführten Themenschwerpunkten sind weiterführende Informationen und Vortragsfolien über die Projektadresse öffentlich abrufbar.

Weiterentwicklung des Firewall-Konzeptes (1)

Innerhalb des Vorgängerprojektes *Firewall* wurde ein Firewall-System zum Schutz des Verwaltungsnetzes aufgebaut. Während des jetzigen Projektverlaufes wurde es immer wieder notwendig, dieses Firewall-Konzept zu überarbeiten und neuen Anforderungen anzupassen.

Ende des Jahres 2000 stand die Aufgabe, die Anbindung einer Abteilung der Universitätsverwaltung an einen externen Application Service Provider (ASP) vorzunehmen. Aufgrund der Nutzung von Terminalserver-basierenden Applikationen musste eine Lösung erarbeitet, erprobt und zeitnah in die Routine überführt werden. Die hier zum Einsatz kommenden MetaFrame-Clients der Firma Citrix unterstützen das Socks-Protokoll für die Anbindung über ein Firewall-System. Deshalb wurde eine Lösung unter Nutzung der Open Source Software *Dante* [1] implementiert. Der Socks-Proxy *v5* wird unter dem Betriebssystem Solaris eingesetzt sowie unter den Betriebssystemen Linux und FreeBSD getestet.

Zusätzliche Gefahren durch die Umgehung des Firewall-Systems (2)

Dieses Arbeitspaket ist in zwei Teilaufgaben gegliedert. Die erste Teilaufgabe besteht in der Entwicklung eines Konzeptes für die Sicherung und Archivierung von sensiblen Verwaltungsdaten, wobei das schon existierende Backup- und Archivsystem der HU genutzt werden soll, ohne dabei die Firewall zu umgehen. Hier wurde eine Lösung geschaffen, die über den Proxy des Firewall-Systems des Verwaltungsnetzes hinweg verläuft und PGP-verschlüsselte Daten überträgt. Eine Umgehung des Firewall-Systems konnte auf diese Weise vermieden werden. Das auf Basis des Tivoli-Storage-Manager (TSM, ehemals ADSM) bereits eingeführte System wird derzeit bezüglich der Verwaltungsdaten einem ausführlichen Test unterzogen und in Kürze in den Routinebetrieb überführt werden.

Die zweite Teilaufgabe untersucht Netzwerkanalyse- und Managementsysteme, die eine frühzeitige Erkennung von internen wie externen Angriffen auf das geschützte Verwaltungsnetz ermöglichen und eine sichere Remote-Administration von geschützten Netzwerkbereichen unterstützen. Dazu wurde zu Testzwecken ein Intrusion-Detection-System (IDS) aufgebaut, welches sich am Vorbild des NMC-Projektes [2] orientiert. Ein IDS ist ein Überwachungssystem, das es erlaubt, genaue Informationen über den Datenverkehr innerhalb des Verwaltungsnetzes und damit sofortige Warnmeldungen bei ungewöhnlichen oder böswilligen Aktivitäten zu erhalten, wie z. B. bei *Denial of Service*-Attacken und bei Versuchen, mit Administratorrechten oder über Backdoors auf Systeme zuzugreifen. Zum Einsatz kommen hier die Open-Source-Projekte *Snort* [3], *ACID* [4], *AIDE* [5] und *PostgreSQL* [6]. In naher Zukunft ist beabsichtigt, das IDS auf dezentrale Bereiche auszudehnen und somit ein Distributed-Intrusion-Detection-System (DIDS) zu schaffen.

Erprobung des Einsatzes von SmartCards in der Universitätsverwaltung (3)

Noch im Verlaufe des Projektes wird das *Banyan VINES*-basierte E-Mail-System der Universitätsverwaltung auf ein Standard-SMTP E-Mail-System umgestellt werden. Da hierbei erstmalig SMTP-fähige E-Mail-Clients zum breiten Einsatz in der Verwaltung kommen, werden sich neue Anforderungen bezüglich der E-Mail-Sicherheit ergeben. Bisher stellten sich die Sicherheitsanforderungen aufgrund des exotischen Netzwerkbetriebssystems *Banyan VINES* und der Netzarchitektur in einer anderen Form dar. Es wird zu einer wesentlich stärkeren Nachfrage nach Verschlüsselungstechnologien kommen, da E-Mails mit sensiblen Daten zwischen zentraler und dezentraler Verwaltung ausgetauscht werden müssen. Das Rechenzentrum bereitet sich darauf sowohl technisch als auch organisatorisch vor, nicht zuletzt durch dieses Drittmittel-Projekt.

Der Hauptanteil des Arbeitspaketes liegt im Ausbau einer Public-Key-Infrastructure (PKI) der HU. Eine Zertifizierungsinstanz, die HU-CA, besteht seit Anfang 1998 und muss in naher Zukunft für die Mitarbeiter der Universitätsverwaltung Anwendungen wie die Verschlüsselung und Signierung von E-Mails anbieten. Dabei wird die Speicherung des geheimen Schlüssels und des Zertifikates auf einer SmartCard angestrebt.

In diesem Kontext erfolgte eine umfassende Analyse der möglichen SmartCard-Unterstützung von Mailprogrammen. Getestet wurden die SmartCard GPK8000 der Firma Gemplus, die SmartCard Model 330 der Firma Datakey, die SmartCard STARCOS SPK 2.3 der Firma Giesecke & Devrient sowie der USB Token iKey 2032 der Firma Rainbow, welcher baugleich mit der Datakey SmartCard ist. Die Gemplus-Karte wird von einigen Mitarbeitern des Rechenzentrums der HU zum Signieren von E-Mails benutzt, wobei von der HU-CA ausgestellte Zertifikate verwendet werden. Dabei findet hauptsächlich das Mailprogramm Netscape Messenger 4.7 Verwendung, wobei Outlook (Express) 5.5 ebenfalls die Funktionalitäten besitzt.

Im Zusammenhang mit der Weiterentwicklung der PKI der HU ist das DFN-Projekt an der internationalen Entwicklung einer webbasierten vollautomatisierten datenbankgestützten PKI-Lösung auf Open-Source-Basis (OpenCA [7]) mit einem Mitarbeiter im Core-Developer-Team beteiligt. Eine Umstellung der auf OpenSSL basierenden HU-CA auf das OpenCA-System wird noch für dieses Jahr angestrebt.

Kryptografische Verfahren auf Netzwerk-Ebene (4)

Das Ziel dieses Arbeitspaketes besteht in der Analyse von Verschlüsselungstechnologien innerhalb der Netz-

werkebene (OSI Layer 3). Dazu wurde unter anderem die Software *F-Secure VPN+* untersucht, womit ein Virtual-Private-Network (VPN) aufgebaut werden kann. Das hierbei verwendete Security-Protocol IPsec nach RFC 2401 bündelt verschiedene Technologien (Verschlüsselung und Authentifikation), die eine sichere Kommunikation über beliebige Rechnernetze ermöglichen, und arbeitet auf der Netzwerkebene des OSI-Modells. Da jede Netzkommunikation über diese Schicht läuft, kann mittels IPsec das Netzwerk auf dieser Schicht fast alle Anwendungen sichern. Die IPsec-Sicherheitsdienste sind hierbei transparent für Anwendung und Nutzer. Die Anwendung dieser Technologie bietet umfangreiche Möglichkeiten bezüglich der Absicherung von sicherheitsrelevanten Anwendungen innerhalb des Verwaltungsnetzes.

Diese Technologie ist weiterhin Bestandteil der Netzwerk-Architektur von Windows 2000 (XP) und wird ebenfalls getestet. Replikationen des Active-Directory-Service von Windows-2000-Servern über Firewall-Systeme hinweg sind mittels dieser Technologie überhaupt erst sinnvoll zu bewältigen.

Entwicklung von Referenzlösungen für ausgewählte DV-Systeme der Universitätsverwaltung (5)

Aus dem Haushaltsbereich werden verstärkt die Anforderungen gestellt, den dezentralen Bereichen der Verwaltung den Zugang zu „ihren“ Haushaltsdaten zu gestatten. Dies erfordert die Öffnung des Firewall-Systems nach innen. Derartige Verbindungen können nur ermöglicht werden, wenn die einzelnen Kommunikationspartner stark authentifiziert werden und die Übertragung der Daten stark verschlüsselt erfolgt. Hier kommt eine Kombination aus VPN-Technologie und Anwendungsverschlüsselung zum Einsatz. Im Endausbau werden die Teilnehmer des Teilprojektes über eine IPsec-Verbindung und ein Security-Gateway mit einer Anwendung kommunizieren, die auf einem Terminalserver im inneren Verwaltungsnetz installiert ist und die den Zugriff auf die zentralen Datenbanken ermöglicht.

Für die Referenzlösung kann die Erfahrung aus den anderen Arbeitspaketen genutzt werden. So wird bereits jetzt schon in einer Pilotlösung das VPN mit der Software *F-Secure VPN+* aufgebaut und mit der Software *Citrix MetaFrame* eine Terminalserver-Sitzung gestartet. Es ist für den Nutzer weiterhin möglich, sich gegenüber dem Netz mit einem Zertifikat der HU-CA, gespeichert auf einer SmartCard, zu authentifizieren. Diese Pilotlösung soll zu einer Referenzlösung ausgebaut werden.

Dokumentation der Projektergebnisse (6)

Im Ergebnis der Projekte *Firewall* und *UVsec* wird ein DFN-Bericht entstehen, in dem die Ergebnisse der einzelnen Projekte in überarbeiteter Form zusammengefasst sein werden. Ziel dieses Berichtes ist es, die Erfahrungen und konkreten Ergebnisse in einer Form darzustellen, die eine umfassende Nachnutzung seitens der Mitgliedseinrichtungen des DFN-Vereins möglich macht. Fragen, die in diesem Zusammenhang beantwortet werden sollen, sind z. B.:

- Welche organisatorischen Schritte sind vor dem Zusammenschluss der Verwaltung einer Einrichtung mit dem übrigen Rechnernetz zu gehen?
- Welche Untersuchungen müssen in diesem Zusammenhang durchgeführt werden und wie gehen die Ergebnisse in die Planung und Durchführung des Vorhabens ein?
- Welche technischen Probleme müssen bei einer solchen umfangreichen Aufgabenstellung analysiert und gelöst werden?
- Wie groß sind die Ressourcen (technisch und personell), die benötigt werden, um ein derartiges Vorhaben zu realisieren?

Aktuelles von der Zertifizierungsstelle HU-CA

An dieser Stelle werden zum Zwecke der sicheren Validierung die Downloadseiten und die Fingerprints der aktuellen Wurzelzertifikate (X.509v3) der Zertifizierungsstellen veröffentlicht. Es wird darauf hingewiesen, dass zum Ende des Jahres das Zertifikat unserer Wurzelinstanz (DFN-PCA) seine Gültigkeit verliert und neu erstellt wird. Dieses muss erneut in die Anwendungen eingelesen werden. Hinweise dazu werden auf den Seiten der DFN-PCA [8] und der HU-CA [9] abrufbar sein.

Fingerprints:

DFN Top Level Certification Authority:
`MD5 Fingerprint:`
`45:BB:9B:C8:8A:A4:84:8B:2D:A0:08:8F:9E:B6:B8:10`

HU-CA [sign only]:
`MD5 Fingerprint:`
`24:AF:DD:47:7D:47:02:1D:3C:AB:67:88:FC:C0:94:D3`
siehe Abb.1

RZ-DCA [sign only]:
`MD5 Fingerprint:`
`33:E2:4E:A0:FB:43:B8:A1:8C:09:3D:0A:FA:5D:F2:7B`

Download-URL für X.509 CA-Zertifikate:

DFN-PCA:
http://www.pca.dfn.de/dfnpca/certify/ssl/dfnpca.der

HU-CA:
http://ca.hu-berlin.de/hu-ca/certs/hucacert.der

RZ-DCA:
http://ca.hu-berlin.de/hu-ca/certs/rzdcacert.der

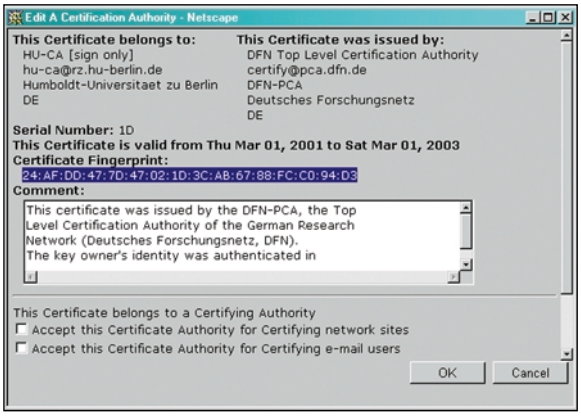

Abb. 1: Zertifikat und Fingerprint der HU-CA

Weitere Informationen zu den Projekten

URLs:

http://www.hu-berlin.de/rz/projekte/firewall/
http://www.hu-berlin.de/rz/projekte/uvsec/
http://www.cert.dfn.de/dfnpca/
http://ca.hu-berlin.de/

Quellen

[1] http://www.inet.no/dante/
[2] http://hdshc.asu.edu/support/nmc/
[3] http://www.snort.org/
[4] http://www.cert.org/kb/acid/
[5] http://www.cs.tut.fi/~rammer/aide.html
[6] http://www.postgresql.org/
[7] http://openca.sourceforge.net/
[8] http://www.cert.dfn. de/dfnpca
[9] http(s)://ca.hu-berlin.de

Das Projektteam:

Dr. Peter Schirmbacher, Projektleiter
Doris Natusch, Projektkoordinatorin
Roland Herbst, wissenschaftlicher Mitarbeiter
Matthias Schwan, wissenschaftlicher Mitarbeiter
Michael Bell, studentischer Mitarbeiter
Till Hoke, studentischer Mitarbeiter

Roland Herbst
roland.herbst@rz.hu-berlin.de

So war es zu lesen in den RZ-Mitteilungen Heft Nr. 12/1996
Eine andere Möglichkeit läßt sich wie folgt formulieren: „Unterschreiben Sie einfach mit ihrem guten Namen“.