Sicher vernetzte Universitätsverwaltung

Bericht über die erste Phase eines Drittmittelprojektes im Rechenzentrum

Vor ein paar Jahren galt es noch als Privileg, einen Internetzugang am Arbeitsplatz zu besitzen. Allenfalls die in den Naturwissenschaften tätigen Wissenschaftler nutzten solche Dienste wie E-Mail, News, Telnet und FTP. Die in der Universitätsverwaltung genutzte Rechentechnik bestand aus zentralen Servern, Druckern und Terminals. Das auf diese Weise aufgebaute Netzwerk besaß keinen Anschluß zur Außenwelt. Die Nutzer der Verwaltung griffen über die seriellen Verbindungen auf ihre Anwendungen zu, und es gab nur sehr aufwendige Methoden, sich unberechtigten Zugang zu den Systemen der Verwaltung zu verschaffen. Die Welt aus der Sicht der Systemsicherheit war einigermaßen in Ordnung.

Die nächste Stufe der „Evolution“ des Netzwerkes der Universitätsverwaltung begann mit dem systematischen Aufbau eines LANs und der Anbindung an das Backbone der Universität. Von Anfang an wurde dabei auf eine Strukturierung des Netzes geachtet. Die Terminals wurden schrittweise durch PCs ersetzt. Dabei bestand zu keinem Zeitpunkt eine physikalische Verbindung zwischen den PCs der Personal- und Finanzdatenverarbeitung und dem restlichen Universitätsnetz.

Im Dezember 1993 wurde in der Zeitschrift *ix* das erste Mal über *ein hypertext-basiertes Informationssystem WWW* berichtet. Spätestens von diesem Zeitpunkt an war es nicht mehr notwendig, besondere Fachkenntnisse über die Internet-Technologien zu besitzen, um die verschiedenen Dienste des Internets nutzen zu können, und es war nur eine Frage der Zeit, wann dies sich auf die Belange der Verwaltung der Universität auswirken würde.

Viereinhalb Jahre später sind solche Dinge wie die Kommunikation per E-Mail, das Abrufen von Informationen aus dem WWW von Servern, die irgendwo in der Welt stehen, auch aus der Verwaltung der Universität nicht mehr wegzudenken. Das Internet gehört heutzutage fast genauso zum Arbeitsplatz in der Universitätsverwaltung wie der Schrank mit den Aktenordnern. Damit verbunden ist jedoch die Aufhebung der physikalischen Trennung zwischen dem Verwaltungsnetz und dem Universitätsnetz. Es mußten andere Methoden gefunden werden, die einen ausreichenden Schutz der verarbeiteten Daten ermöglichen.

Leicht wird übersehen, daß mit der Erweiterung der Möglichkeiten natürlich eine Verkomplizierung der Mechanismen, die bei der Datenübertragung zur Anwendung kommen, einhergeht. Damit verbunden ist eine steigende Anfälligkeit der Systeme gegenüber Ausfällen und der „Teilnahme“ dritter, nicht berechtigter Personen am Kommunikationsprozeß.

Mittlerweile existiert eine Vielzahl kleiner handlicher Programme, die es ermöglichen, fremde Verbindungen zu belauschen oder sogar zu manipulieren. Dabei ist bei weitem nicht mehr die kriminelle Energie vonnöten, der es zur „guten alten Zeit“ des Terminals bedurft hatte. Die Grenzen zwischen der spielerischen Erkundung eines Systems und dem Einbruch in fremde Computer mit eindeutig krimineller Absicht sind nicht mehr einfach auseinanderzuhalten. Beim gegenwärtigen Stand der Technik ist ein Szenario denkbar, bei dem sich der Datendieb fernab von der Universität, vielleicht unter der kalifornischen Sonne, via Notebook und Funktelefon für die Haushaltsdaten der Universität interessiert.

War es in der Vergangenheit noch ausreichend, den Zugang zu den Büros und Terminalleitungen zu kontrollieren, müssen heute komplizierte Systeme geschaffen werden, die den Nutzer bestmöglich vor Datenspionage schützen und ihn dennoch nicht ernsthaft in seinen Möglichkeiten der Internet-Nutzung beschneiden.

Genau darin liegt ein Problem, mit dem wir als Systemsicherheits-Verantwortliche immer wieder konfrontiert werden. Uns wird nachgesagt, daß wir die Nutzer in ihrem Tatendrang einschränken, obwohl wir nichts anderes beabsichtigen, als die von ihnen bearbeiteten Daten vor Angriffen aus dem Netz zuverlässig zu schützen. Der springende Punkt ist, daß die Nutzer es gar nicht mehr merken, daß sie sich in einem Netzwerk befinden und mit einem hochkomplizierten System arbeiten, wenn sie z. B. eine Datenbank-Recherche über ein Web-Frontend irgendwo in der Welt durchführen.

Die Unantastbarkeit des eigenen Rechners wird dabei stillschweigend vorausgesetzt. Das dem nicht so ist, beweisen die unzähligen Security-Hinweise über aufgetretene Sicherheitslücken in den verschiedenen zum Einsatz kommenden Systemen.

Einordnung des Projektes

Ende August 1997 begann am Rechenzentrum ein vom DFN-Verein gefördertes Drittmittelprojekt *Firewall – ein Kernstück zur Sicherung des Verwaltungsnetzes*, welches den Schutz des Verwaltungsnetzes vor inneren und äußeren Angriffen zum Inhalt hat. Das Projekt der Humboldt-Universität ergänzt die ebenfalls vom DFN-Verein geförderten Projekte der Fernuniversität Hagen *Public Key-Service* und der FH Wilhelmshaven *DFN-Sicherheitsprojekt*.

Im Ergebnis des Projektes wird die Humboldt-Universität über ein Verwaltungsnetz verfügen, welches vor Angriffen aus dem internen sowie dem externen Internet noch zuverlässiger als bisher geschützt ist. Großer Wert wird dabei auf die Erweiterbarkeit der

bestehenden Lösungen gelegt. Die zum Einsatz kommenden Verfahren müssen flexibel gegenüber Neuerungen in der DV-Landschaft sein.

An dieser Stelle soll besonders der Referenzcharakter des Projektes hervorgehoben werden, wenn sich dies auch nur auf die grundsätzlichen Prinzipien und Lösungsvorschläge beziehen kann, da die aufgezeigten Lösungen eng an die spezifischen Bedingungen der Universität geknüpft sind. In diesem Beitrag sollen erste Ergebnisse und Erfahrungen der Projektgruppe vorgestellt werden.

Phasen des Projektes

Der Projektantrag an den DFN sah folgende Teilthemen vor:

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

Die einzelnen Themen sollten dabei in zeitlich unveränderter Reihenfolge und unter Nutzung der jeweiligen Zwischenergebnisse bearbeitet werden.

Wie aus der verwendeten Formulierung ersichtlich ist, wurde in Abstimmung mit dem DFN-Verein eine zeitliche Verschiebung einzelner Themen aufgrund der Aktualität bestimmter Aufgaben vorgenommen. Die Teilaufgabe *Verschlüsselung und Signatur* wäre normalerweise erst in der Endphase des Projektes bearbeitet worden. Einzelne für die Universität besonders dringlich zu lösende Aufgaben wurden aus dem Zeitplan herausgenommen und deren Bearbeitung begonnen.
Dies betrifft insbesondere die Themen:

- Aufbau einer gesicherten und verschlüsselten Verbindung zwischen einem PC im Universitätsnetz und dem Personalsystem (bei Projektantrag noch nicht absehbar)
- Aufbau und Betrieb einer Zertifizierungsinstanz zur Beglaubigung von PGP- und SSL-Schlüsseln an der Humboldt-Universität (HU-CA)
- Sichere Windows95-Installation im Verwaltungsnetz (dieses Thema wurde aufgrund der Aktualität und der inhaltlichen Überschneidung mit dem Projektthema aufgenommen)

Grundschutzkonzept und Risikoanalyse

Bevor man an die Installation einer bestimmten Sicherheitslösung gehen kann, ist es unumgänglich, eine genaue Analyse der bestehenden Gefahren und der daraus resultierenden Risiken durchzuführen. Ziel ist es, ein Sicherheitskonzept für eine bestehende IT-Landschaft zu formulieren. Dabei wird von einem zu erreichenden allgemeinen Grundschutz ausgegangen, der einen Mindeststandard definiert, der sicherheitstechnisch einzuhalten ist. Dieser Grundschutz repräsentiert die sicherheitstechnischen Mindestanforderungen an die untersuchten Systeme. Natürlich muß er erweitert werden, wenn es um die Bearbeitung sensibler personenbezogenen Daten geht.

Die Analyse der Gefahren und Risiken wurde für ausgesuchte Systeme der Verwaltung der Universität durchgeführt. Im Ergebnis entstand eine Rahmengliederung für das Sicherheitskonzept des Verwaltungsnetzes, nach dem in Teilen bereits verfahren wird.

Das Instrumentarium des BSI-Sicherheitshandbuches (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 bahnbrechende Entwicklung durch die breite Einführung von Internet-Technologien auch in Verwaltungen konnte zum Zeitpunkt der Herausgabe dieses Standardwerkes durch das BSI bestenfalls vermutet werden.

Besonders schwierig ist die Einschätzung der möglichen Schadenshöhen, die auftreten, wenn es zur Verletzung der Datensicherheit kommt:

- *Verlust der Verfügbarkeit*
- *Verlust der Integrität*
- *Verlust der Vertraulichkeit*

Um eine Vereinfachung der Problematik zu erreichen, wurde vom BSI (*http://www.bsi.bund.de)* ein Instrumentarium herausgegeben, welches die Systeme beschreibt, die einem niedrigen bis mittleren Datenschutz unterliegen. Das IT-Grundschutzhandbuch liegt in einer Version von 1997 vor, wird fortgeschrieben und beinhaltet bereits einen großen Teil der Neuerungen in der IT-Landschaft (*http://www.hu-berlin.de/bsi/gshb97/_start.htm*).

Hier muß allerdings erwähnt werden, daß der Grundschutz bei weitem nicht auf alle Systeme des Verwaltungsnetzes angewendet werden kann.

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 wird in Zusammenarbeit mit dem BSI von verschiedenen Herstellern angeboten. Der Einsatz dieser Software innerhalb des Projektes wurde getestet. Der Weg zu dem oben be-

schriebenen Ziel ist erkennbar, die bisher vorliegenden Produkte können jedoch noch nicht überzeugen.

Netzstrukturierung

Ein wichtiger Aspekt der Netzwerksicherheit ist die Architektur des verwendeten Netzes. Alle drei Standbeine der Datensicherheit werden hier berührt. Ein Beispiel sei die Speicherung einer Datei auf einem zentralen Server.

Es ist zu gewährleisten, daß die Daten:

auf dem Server erreichbar sind	⇒	*Verfügbarkeit*
während des Transportes nicht verändert werden	⇒	*Integrität*
von Unbefugten nicht während des Transportes oder danach gelesen werden können	⇒	*Vertraulichkeit*

Gerade in einem Verwaltungsnetz ist es wichtig, einen genauen Überblick über die eingesetzten Netzwerkkomponenten und die installierte Rechentechnik zu besitzen. Deshalb erfolgte eine Überarbeitung der Netzwerk-Dokumentation des Verwaltungsnetzes der Universität, welche zu großen Teilen abgeschlossen ist.

Es wurde eine Datenbanklösung geschaffen, die es ermöglicht, die für den Netzbetrieb notwendigen Nutzerdaten über einen SSL-fähigen WWW-Browser abzufragen. Der Betreuungsaufwand der Administratoren des Verwaltungsnetzes wurde damit erheblich reduziert.

In Zusammenarbeit mit den Netzwerkspezialisten des Rechenzentrums wurde mittels der Netzwerk-Management-Software *Spectrum* die Performance der aktiven Komponenten des Verwaltungsnetzes analysiert. Temporär auftretende Instabilitäten des Netzes konnten auf die zentrale Bridge innerhalb des Verwaltungsnetzes zurückgeführt werden. Im Ergebnis der Untersuchungen erfolgte der Austausch dieser Komponente durch eine Bridge höherer Leistungsfähigkeit. Eine weitere Erhöhung der Netzwerksicherheit konnte durch den Einsatz von Switch-Technik im Verwaltungsnetz erreicht werden. Dies dient der Vorbereitung der Migration zu VLANs in der näheren Zukunft.

In Zusammenarbeit mit anderen Abteilungen des Rechenzentrums erfolgt die Erarbeitung eines Lösungskonzeptes zum sicheren Betrieb von Windows95-PCs im Verwaltungsnetz.

Firewall

Will man auch gegen Angriffe, die sich von außen auf das interne Netz richten, geschützt sein, so ist es unumgänglich, die internen Systeme mit einer Firewall zu sichern. Der Vergleich mit einer Brandschutzmauer ist insofern richtig, als daß man den internen Netzwerkbereich nach außen hin abschottet. Unabhängig davon ist es jedoch notwendig, den internen Netzbetrieb sowenig wie möglich zu beeinträchtigen.

Die Firewall ist so konzipiert, daß sie den einzigen Übergang zwischen dem sicheren Netzbereich der Zentralen Universitätsverwaltung (ZUV) und dem externen, unsicheren Netzbereich darstellt. In der ersten Phase des Projektes konnte eine Erhöhung der Ausfallsicherheit des bestehenden Firewall-Systems unter Lastbedingungen erzielt werden. Durch die Integration verschiedener Gateways in das System ist es gelungen, zusätzliche Internet-Dienste für die Nutzer der Verwaltung verfügbar zu machen (z. B. POP3, SQL, telnet). Auf der Clientseite erfolgte die Umstellung auf eine aktuelle und somit sicherere WWW-Browser-Version.

Kommunikationswege unter Umgehung des Firewall-Systems

An der Humboldt-Universität besteht ein Client-Server-System zur Datensicherung und Archivierung in der Form eines Robotersystems auf der Basis von UniTree. Es ist geplant, dieses auch für die Systeme der Verwaltung zu verwenden. Dabei ist noch zu entscheiden, ob dedizierte Netzverbindungen zum RZ (außerhalb der Firewall) oder vorhandene Verbindungen (über die Firewall) genutzt werden.

Da die Firewall der einzige Übergang zum Außennetz darstellen soll, ist es notwendig, alle anderen Verbindungen von außen in das Netz der Universitätsverwaltung hinein zu unterbinden. Dies betrifft insbesondere Möglichkeiten der Einwahl über ISDN- oder Analog-Verbindungen. Denn es hat keinen Sinn, die Tür zum Verwaltungsnetz fest zu verschließen, wenn wir die Fenster, seien sie auch noch so klein, einladend offenstehen lassen.

Verschlüsselung und Signatur

Betrachtet man die in der letzten Zeit erschienenen Internetbeiträge in unterschiedlichen Medien, so gibt es einen eindeutigen Favoriten, die Datensicherheit. In einer Zeit der zunehmenden Vernetzung und dem Ausbau der elektronischen Kommunikation auf allen Gebieten wird die sichere Übermittlung von Daten immer bedeutsamer. Sie wollen sicher sein, daß Sie wirklich mit dem richtigen Partner kommunizieren, wenn Sie einander vertrauliche Daten senden. Für die Verwaltung einer Universität hat dieser Aspekt eine besondere Bedeutung. Die Unverfälschbarkeit der übermittelten Daten kann nur durch den Einsatz von suffizienter Verschlüsselung gewährleistet werden.

Am Rechenzentrum wurden innerhalb des Projektes die Voraussetzungen für den Betrieb einer Zertifizierungsinstanz geschaffen. Es enstand eine Policy (*http://ca.hu-berlin.de/hu-ca/huca-policy.phtml*), deren Inhalt mit dem Datenschutzbeauftragten der

Humboldt-Universität abgestimmt wurde. Der interne Testbetrieb der HU-CA und der RZ-DCA wurde im Dezember 1997 begonnen. Es wurde ein WWW-Server (*http://ca.hu-berlin.de*) eingerichtet. Hier findet man genauere Angaben zur CA der HU (HU-CA) und der DCA des Rechenzentrums (RZ-DCA) der Humboldt-Universität. Weitergehende Informationen hierzu entnehmen Sie bitte dem ebenfalls in diesem Heft erschienenen Artikel „*Vertrauen gegen Vertrauen*" – *Die Zertifizierungsinstanz der Humboldt-Universität* von Alexander Geschonneck.

Dezentralisierungstendenzen innerhalb der Verwaltung der Universität machen es erforderlich, einen Zugang zu den zentralen Servern durch einen unsicheren Bereich hindurch zu ermöglichen. Die Übertragung sensibler Daten über solche unsicheren Kanäle wird mit der Software *SSH* verschlüsselt.

An die Projektgruppe wurde der Wunsch herangetragen, eine authentisierte und verschlüsselte Verbindung zwischen einem im Universitätsnetz stehenden dezentralen PC und den Servern im sicheren Bereich hinter der Firewall zu ermöglichen. Nach Abstimmung mit dem DFN-Verein wurde für April 1998 eine diesbezügliche technische Lösung zugesagt. Ein ACE-Server authentisiert externe Nutzer auf Basis von zeitabhängigen Einmal-Paßwörtern.

Sollten Sie an weiteren Informationen interessiert sein, so besuchen Sie unsere Projekt-Web-Sites.

ACE	Access Control Encryption
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority, Zertifizierungsinstanz oder Beglaubigungsstelle
DCA	Deligated Certification Authority, Untergeordnete Zertifizierungsinstanz
DFN	Deutsches Forschungsnetz
ISDN	Integrated Services Digital Network
IT	Informationstechnik
LAN	Local Area Network
PGP	Pretty Good Privacy, Software zur effizienten Verschlüsselung von Daten
POP3	Post Office Protocol, Protokoll zum clientseitigen Abruf von email von einem zentralen Mailserver über TCP/IP
SQL	Structured Query Language, Standard-Abfragesprache für Datenbanken
SSL	Secure Socket Layer, standardisiertes Protokoll zur Verschlüsselung des Datentransportes
VLAN	Virtuelles LAN
ZUV	Zentrale Universitätsverwaltung

Projekt: *http://www.hu-berlin.de/projekte/fw*
HU-CA: *http://ca.hu-berlin.de*
Policy: *http://ca.hu-berlin.de/hu-ca/huca-policy.phtml*

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