

## Sicherheit im Verwaltungsnetz

Das sicherste System ist das geschlossene System ohne Kommunikation und Datenaustausch mit der Außenwelt! Als wir uns vor über drei Jahren für ein „offenes“ Verwaltungsnetz entschieden, waren wir uns darüber im klaren, daß dies der risikvollere Weg ist. Wurden uns nicht zuletzt aus der Presselandschaft die Horrorszenerarien über geknackte Personaldatenrechner, manipulierte Gehaltslisten, verfälschte Briefinhalte oder verkaufte Adreßlisten vor Augen gehalten.

Beim Aufbau des Verwaltungsnetzes sind wir nach dem Grundsatz vorgegangen, zuerst die Risiken zu erkennen, mit geeigneten technischen/organisatorischen Maßnahmen zu minimieren und danach die einzelnen Dienste explizit zu erlauben. So sind einzelne technisch mögliche Netzzugänge oder -dienste bis heute verboten, da wir glauben, sie noch nicht genügend zu beherrschen (Fernzugriffe auf sicherheitsrelevante Datenbestände in der Zentralen Universitätsverwaltung sind z. B. nicht möglich).

### Das Verwaltungsnetz

Über den Aufbau, die Struktur und die im Verwaltungsnetz angebotenen DV-Anwendungen wurde bereits in früheren RZ-Mitteilungen – u. a. in der Nummer 13 – berichtet. Hier nur noch einmal die wichtigsten Eckpunkte, die zum Thema Sicherheit einen besonderen Bezug haben:

- Das Verwaltungsnetz verfügt über eine Verbindung zum Universitätsnetz und damit zum Internet, die durch ein spezielles Firewall-System geschützt wird.
- Es wurden abteilungsbezogene Subnetze mit dedizierten Abteilungsservern aufgebaut, die z. Zt. noch mit Hilfe einer Bridge miteinander gekoppelt werden.
- Als universitätsübergreifendes Netzwerkbetriebsystem wird Banyan VINES eingesetzt. Spezielle Verwaltungsverfahren, wie z. B. Studentenverwaltung, maschinelle Zulassungsverfahren, Personal- und Stellenverwaltung und Haushaltsabrechnung und -planung basieren auf Softwareprodukten der HIS GmbH Hannover und dem UNIX-Betriebssystem.
- Die über das Netz erreichbaren ca. 350 PCs der Verwaltung sind in ihrem Ausstattungsgrad sehr heterogen, erst ca. 16% der Rechner sind Windows 95-tauglich.
- Auf gegenwärtig 11 Servern (Banyan VINES- und UNIX-basiert) werden ca. 30 DV-Anwendungen eingesetzt.

Das Verwaltungsnetz ist darüber hinaus die Basis für die Kommunikation per E-Mail, den Austausch und die gemeinsame Bearbeitung von Dokumenten, die Archivierung der Verwaltungsdaten und die Benutzung des

World Wide Web als verwaltungsinternes Arbeitsinstrument.

### Anforderungen an die Sicherheit

Es ist gerechtfertigt, dem Thema Sicherheit im Verwaltungsnetz einen gesonderten Beitrag in diesem Heft zu widmen. Gibt es doch einige Spezifika bzw. Anforderungen, die für die Verwaltung und damit für das Verwaltungsnetz in höherem Maße als für den wissenschaftlichen Bereich zutreffen. Sie lassen sich unter den Schlagworten

Verfügbarkeit	Integrität	Vertraulichkeit
---------------	------------	-----------------

zusammenfassen. Mit *Verfügbarkeit* sind die ständig bzw. innerhalb vorgegebener Zeiten bereitstehenden Dienstleistungen und DV-Anwendungen gemeint. Ein stabiler Netzbetrieb mit niedrigsten Ausfallzeiten, ein wohlüberlegtes Datensicherungskonzept und die Verfügbarkeit der zu bearbeitenden Daten sind die obersten Voraussetzungen. Ein Verwaltungsmitarbeiter wird sich erst dann auf das Netz verlassen, wenn es nahezu ausfallfrei funktioniert. Die *Integrität* bezieht sich hauptsächlich auf die in einem System abgespeicherten Daten, die nur von Befugten in beabsichtigter Weise verändert werden dürfen. Neben der Unversehrtheit der Daten soll auch die Vollständigkeit, Widerspruchsfreiheit und Korrektheit garantiert werden. Mit *Vertraulichkeit* ist gemeint, daß nur der befugte Personenkreis Zugang zu den Daten erhält und der Zugang Unbefugter ausgeschlossen werden kann.

In einem Verwaltungsnetz ist die Sicherheit durch die unterschiedlichsten Ursachen gefährdet. So sind z. B. statistisch gesehen die Benutzer und Betreiber der DV-Systeme die größte Gefahrenquelle. Fehlerhafte Software oder virenverseuchte Dateien können weitreichenden Schaden verursachen, oder ein Serverdefekt kann eine ganze Abteilung „lahmlegen“.

Das liest sich noch wie graue Theorie, aber welches sind die typischen Gefahren, mit denen eine Hochschulverwaltung rechnen muß, wenn Daten über das Netz übertragen werden oder per E-Mail kommuniziert wird? Einige Szenarien sollen das verdeutlichen:

**I:** Eine Verwaltungsabteilung ist räumlich verteilt, ein Sachbearbeiter verschickt ein Schreiben über das Netz (als Anlage zur E-Mail) seinem Kollegen zur weiteren Bearbeitung zu. Dieser fügt seine Bemerkungen hinzu und schickt es an seinen Referatsleiter.

*Gefährdung der Integrität*

**II:** Ein Mitarbeiter der Haushaltsabteilung wurde vom Kanzler beauftragt, eine Gesamtstatistik über die aktuell verbrauchten Mittel zusammenzustellen und zur

nächsten Dienstberatung den Abteilungsleitern über das Netz zur Verfügung zu stellen. Es wird ein gemeinsames Verzeichnis benutzt.

*Gefährdung der Vertraulichkeit und Integrität*

**III:** Der Jahresabschlußbericht der Forschungsabteilung steht kurz bevor und durch einen Plattencrash läßt sich eine wichtige Datenbank nicht mehr lesen.

*Gefährdung der Verfügbarkeit*

**IV:** Eine Sachbearbeiterin erhält kurz vor Feierabend den Auftrag, ein vertrauliches Schreiben fertigzustellen und zu versenden. Sie vergißt in der Eile, sich auszuloggen und ihren PC auszuschalten.

*Gefährdung der Vertraulichkeit und Integrität*

### Empfehlungen, Maßnahmen, Tips ...

Das Sicherheitskonzept für die Verwaltung gibt es leider nicht. Man kann es weder von einer anderen Hochschule übernehmen, noch von einer Firma kaufen und installieren lassen. Es kostet viel Arbeitszeit, Geld und nicht zuletzt geschultes und zuverlässiges Personal. Hat man das nicht, sollte man es lassen und statt dessen ein sicheres geschlossenes System ohne Verbindung nach außen schaffen. Einige der in den letzten Jahren gemachten Erfahrungen könnten möglicherweise auch für andere von Interesse sein, wie z. B.:

- Definieren Sie „saubere“ Grenzen des Verwaltungsnetzes, legen Sie die Zugangspunkte bzw. die Außenstellen fest, zu denen Netzverbindungen existieren sollen.
- Sichern Sie das Verwaltungsnetz über eine Firewall vor der Außenwelt und sorgen Sie dafür, daß möglichst *alle* Verbindungen über die Firewall geprüft werden.
- Der Aufwand zur Sicherung sollte in angemessenem Verhältnis zum Schutzzweck stehen. Versuchen Sie, einen einheitlich hohen Grundschutz für möglichst viele Systeme zu installieren und schützen Sie nur die sensiblen Bereiche durch zusätzliche Maßnahmen. Das Bundesamt für Sicherheit in der Informationstechnik gibt uns mit seinem Grundschutzhandbuch<sup>1</sup> ein geeignetes Instrument dazu in die Hand.
- Wecken Sie möglichst frühzeitig die Sensibilität für die Sicherheitsproblematik sowohl im Management der Universität, im Rechenzentrum, aber auch bei jedem Systemadministrator und Nutzer. Es fängt bereits beim verantwortungsbewußten Umgang mit den Paßwörtern an.
- Sorgen Sie dafür, daß den für die Sicherheit und Betreuung zuständigen Fachleuten immer (genügend) Zeit für ihre fachliche Weiterbildung und das Austeilen neuer Verfahren bleibt. Was heute als der neueste Schrei gilt, ist morgen schon veraltet!

<sup>1</sup> IT-Grundschutzhandbuch 1997, BSI, Schriftenreihe zur IT-Sicherheit, Band 3

Die besonders sicherheitskritische Kommunikations- und Servertechnik sollte möglichst in gesondert geschützten Räumen untergebracht und über gesicherte Netzverbindungen betreut werden.

Und als letztes noch: Warten Sie nicht auf den ersten Einbruchversuch, sondern legen Sie in einem Aktionsplan fest, wie bei Sicherheitsverstößen zu reagieren ist, welche Handlungskette durchzuführen und welche Vorgesetzten zu informieren sind. Bauen Sie sich am besten ein eigenes Security Team auf.

### Was ist als nächstes zu tun?

Das einmal aufgebaute Sicherheitskonzept sollte regelmäßig mit der Realität abgeglichen werden und neu entstandene Wünsche und Anforderungen der Nutzer berücksichtigen. Um diesen Forderungen gewachsen zu sein, hat das Rechenzentrum der HU an den DFN-Verein einen Projektantrag zum Thema „Firewall – ein Kernstück zur Sicherung des Verwaltungsnetzes der HU“ gestellt und das Projekt im April 1997 gestartet. Wir versprechen uns von den Projektergebnissen wichtige Erkenntnisgewinne und Lösungsvorschläge u. a. zu folgenden Teilthemen:

- alternative Konzepte zur Struktur des Verwaltungsnetzes, Einsatzmöglichkeiten von VLANs
- Weiterentwicklung des Firewall-Konzepts, vorrangig unter dem Gesichtspunkt der Performancesteigerung und Senkung des Betreuungsaufwandes
- Entwicklung eines Sicherungs- und Archivierungskonzeptes für die UNIX-Server der Verwaltung unter Beachtung der Sicherheitsrestriktionen und unter Nutzung eines Robotersystems
- Möglichkeiten der Überwachung von Modem-Zugängen
- sichere/verschlüsselte Fernzugriffe auf zentral geführte Datenbestände
- Benutzung der elektronischen Unterschrift im Verwaltungsbereich und damit eine höhere Sicherheit der „beweiserheblichen“ Vorgänge unter Netzbedingungen.

Viele Punkte konnten nur angetippt werden. Aber vielleicht reichen sie aus, die Mitstreiter anderer Hochschulen für einen gemeinsamen Erfahrungs- und Gedankenaustausch zu interessieren.

Doris Natusch  
natusch@rz.hu-berlin.de