



EDV-Sicherheit an der Universität Heidelberg

Rechenzentrum der Universität Heidelberg

Konzept, Stand 16. Oktober 2002

Inhalt

Inhalt	3
Vorbemerkung.....	4
1. Zusammenfassung.....	5
2. Entwicklungen: Universität, EDV und Internet	11
2.1. Zunahme der EDV-Nutzung	11
2.2. Derzeitige Situation	11
2.3. Bedrohungen und Sicherheitsprobleme an der Uni	12
2.4. Schäden.....	13
3. Ziele eines EDV-Sicherheitskonzeptes.....	14
3.1. Universitätsweite EDV-Sicherheits-Policy.....	14
3.2. Wer sollte sich alles um Sicherheit bemühen?	15
3.3. Modularität	16
3.4. Firewall und Firewall-Hierarchie	17
3.5. Intrusion Detection und proaktive Netzwerk-Scans	21
3.6. Incident Response	21
3.7. Weitere Sicherheitsaspekte.....	22
4. Umsetzung des EDV-Sicherheitskonzeptes	24
4.1. Geleistete Maßnahmen	24
4.2. Notwendige weitere Maßnahmen	28
5. Ausblick.....	31
Anhang.....	32
A.1. Security-Hinweise im WWW.....	32
A.2. Sicherheitskonzept zum HD-Net	32
A.3. Firewall-Dokumentation im WWW.....	34
A.4. Vorträge in der Fortbildungsveranstaltung für Netzbeauftragte.....	34
A.5. BelWü Sicherheitsempfehlungen	34
A.6. Weitere Referenzen	34
A.7. Glossar verwendeter Fachbegriffe.....	35

Vorbemerkung

Auf den folgenden Seiten wird ein Konzept zur Erhöhung der allgemeinen EDV-Sicherheit an der Universität Heidelberg entwickelt und vorgestellt. Inhärent im Thema liegt die Notwendigkeit zur regelmäßigen Weiterentwicklung und Überarbeitung, zur Verbesserung und Reaktion auf neue technische Möglichkeiten und Gefahren.

Das EDV-Sicherheitskonzept eines Unternehmens ist nie „fertig“, sondern durchläuft immer neue Zyklen der Analyse, Planung, Nachverfolgung und Steuerung, in welche immer neue Gefahren und gemachte Erfahrungen einfließen. Die vorliegende Empfehlung verkörpert einen neuen „Lifecycle“, welcher mehr Entscheidungsbedarf enthält als der vorige, der im Wesentlichen aus wahlfreien Angeboten für die Institute bestand.

1. Zusammenfassung

Dieses Konzeptpapier beschäftigt sich vor allem mit dem Thema „Sicherheit und Internet.“ Die Sicherheitsproblematik im Internet ist allgemein bekannt und über die Schäden, die Hacker und Viren anrichten können, wurde in vielen Medien berichtet. Die Problematik ist so alt wie das Internet selbst.

Zwei Entwicklungen haben in den letzten Jahren das Problem verschärft. Zum einen können heute vergleichsweise unerfahrene Leute mit Hilfe von leicht zu bedienenden Programmen Viren erstellen oder in Rechner einbrechen. Es sind also keine spezialisierten Hacker, sondern eine Flut von mehr oder weniger kompetenten „Script-Kiddies“, die diese Programme einsetzen und so z. B. Zugang zu Rechnern sammeln, wie früher Fußballbilder oder Briefmarken.

Zum anderen hat ja die Bedienungsfreundlichkeit moderner Rechner vielen Menschen überhaupt erst die Möglichkeiten einer EDV-gestützten Arbeitsorganisation eröffnet. Für die Bedienung eines Rechners ist heute kein Informatik-Studium nötig, und der EDV-spezifische Kenntnisstand der Nutzer dementsprechend niedrig. Die Vorteile der Nutzung von Email und WWW haben die Zahl der vernetzten Rechner explodieren lassen. Insbesondere an der Universität ist kaum ein Arbeitsplatz ohne PC mitsamt EDV-Anschluss denkbar. „EDV-Anschluss“ heißt aber an der Universität Heidelberg derzeit noch „freier Anschluss an das Internet“ und damit weltweiter Zugriff auch vom Internet auf den PC.

Das wäre alles kein Problem, wenn die Betreiber der Rechner genau wüssten, was sie wo und wie konfiguriert haben, täglich die Entwicklung zu Angriffen auf die benutzten Betriebssysteme und Programme verfolgen und die veröffentlichten Programmaktualisierungen zeitnah installieren würden.

Diese Anforderungen sind jedoch von den Nutzern und Rechnerbetreibern an den Instituten nicht flächendeckend zu realisieren. Es bleibt daher nur ein Schutz der Rechner durch „das Netz“, also der Versuch, die Angriffe erst gar nicht an die Rechner weiterzuleiten.

Dabei geht es hier insbesondere um die Frage, inwieweit sich die gängigen Modelle von „Firewall“-Topologien auf die Universität übertragen lassen, in welcher die Bedürfnisse und Möglichkeiten in vielfacher Hinsicht anders sind als bei anderen Unternehmen:

1. Die Freiheit des einzelnen Wissenschaftlers kann und soll nicht auf dieselbe Weise eingeschränkt werden wie anderswo, wo einfach zentral vorgegeben wird, welche Internet-Dienste erlaubt und verboten sind.
2. Die Offenheit der Universität macht die Abgrenzung zwischen „außen“ und „innen“ schwieriger als in anderen Unternehmen, wo einfach zwischen Kunden und Personal unterschieden werden kann.
3. Die Personal-Fluktuation ist außergewöhnlich hoch, so dass es besonders schwierig ist, qualifiziertes IT-Personal heranzubilden und zu halten.

Aus dem ersten Grund ist das gängige Modell der so genannten *Whitelist* hier nicht so leicht anwendbar, das besagt: „Es ist alles verboten, was nicht ausdrücklich erlaubt ist.“ Im Gegensatz dazu steht das Modell der *Blacklist*: „Alles ist erlaubt, außer den ausdrücklich verbotenen Aktivitäten auf einer Schwarzen Liste.“ (wie wir sie im vorigen Konzept-Lifecycle in abgestufter Form angeboten haben).

Wegen der zweiten Besonderheit muss die gängige Firewall-Topologie, die vor allem zwischen Kunden-Eingang und Personal-Eingang unterscheidet, bei uns doppelt realisiert werden, nämlich auf zwei ineinandergeschichteten Ebenen. Nur so kann die universitätsinterne Öffentlichkeit berücksichtigt werden, deren Angehörige als Mitglieder der Universität zwar „Personal“ sind, aber gegenüber den meisten Instituten als „Kunden“ gelten müssen.

Fazit: Diese genannten Besonderheiten machen kosten- und personalintensive Sondermaßnahmen zusätzlich zu den gängigen Sicherheits-Konzepten notwendig, die bekanntlich ihrerseits schon unmodifiziert als außerordentlich aufwändig gelten.

In diesem Sinne wurden im BelWü-AK (Landesforschungsnetz in Baden-Württemberg) unter Mitwirkung von Mitarbeitern des URZ Sicherheitsempfehlungen erarbeitet, die wir im Rahmen eines Sicherheitskonzeptes für das HD-Net umgesetzt haben. Dieses Konzept enthält verschiedene Sicherheitsstufen, die mit zunehmender Sicherheit aber auch zunehmende Einschränkungen bei der Anbindung an das Internet und der Bereitstellung von Diensten (WWW-Server etc.) bedeuten.

Im Wesentlichen sind die im folgenden genannten Maßnahmen möglich und teilweise schon rudimentär realisiert:

1. Uni-Firewall für den allgemeinen Datenverkehr

Im allgemeinen werden „interne Firmennetze“ als sogenanntes „Intranet“ durch Firewalls vom Internet abtrennt und damit gesichert. Beim HD-Net entspräche dies der Einführung einer Uni-Firewall wie in Abb. 1.

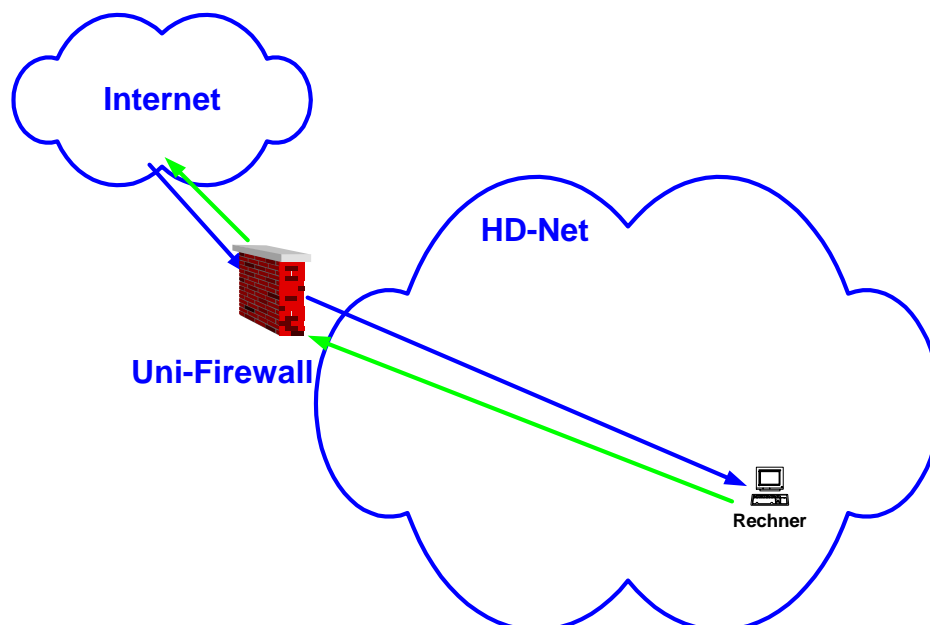


Abb. 1 Uni-Firewall: Der gesamte ein- (blau) und ausgehende (grün) Datenverkehr wird am Eingang zum Universitätsnetz (HD-Net) nach vorgegebenen Regeln erlaubt oder verboten

Eine technische Umsetzung existiert bereits, nur wird diese bislang sehr eingeschränkt verwendet. Wir empfehlen - insbesondere für von außen neu einkommenden Datenverkehr,

durch den es immer wieder zu Sicherheitsproblemen kommt - eine Beschränkung nach der Methode „was nicht explizit erlaubt ist, ist verboten.“

2. Instituts-Firewalls

Die Regeln, nach denen Verbindungen erlaubt oder abgelehnt werden, sind bei einer Uni-Firewall für das gesamte HD-Net einheitlich. Hier eine gemeinsame strenge Regelung zu finden ist nicht möglich, da es in den Instituten unterschiedliche Anwendungen und Sicherheitsbedürfnisse gibt. Daher sind für die Institutsnetze Firewalls nach Abb. 2 nötig. Beide Abbildungen sehen ganz ähnlich aus und sind es auch. Die Institutsfirewalls sehen nur das Institutsnetz als „intern“ und stellen Internet und HD-Net (mit Ausnahmen) auf eine Stufe.

Für die Institute werden Firewalls in verschiedenen Sicherheitsstufen angeboten. Dabei soll nicht jedes Institut seine maßgeschneiderte, einmalige Internetanbindung bekommen, dies wäre nicht mehr zu verwalten. Ziel des Stufenkonzeptes ist es, die Anzahl der verschiedenen Filter möglichst klein zu halten. Zur Zeit sind ca. sechs verschiedene Filter vorgesehen. An den ersten Instituten sind einige dieser Sicherheitsstufen bereits eingerichtet.

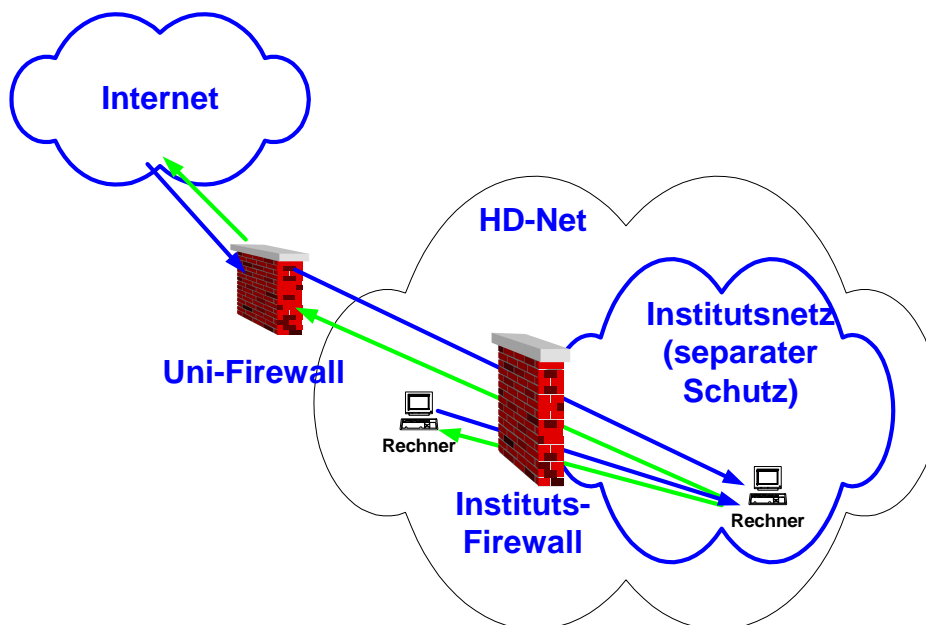


Abb. 2 Instituts-Firewall: Jedes Institut wird mit einer eigenen Firewall gegenüber dem Internet und den anderen Instituten des HD-Net geschützt.

Durch dieses Konzept wechseln die Rollen der Mitglieder der Universität je nach Netz, ob sie nun „intern“ bzw. Mitarbeiter sind oder „extern“ bzw. Kunden.

3. Absicherung bestimmter Dienste

Aufgrund massiver Probleme durch den Missbrauch der mehreren hundert Mailserver innerhalb des HD-Net wurde dieser Dienst 1999 abgesichert. Alle Emails müssen über die Mail-Firewall empfangen oder versendet werden. (Siehe Abb. 3)

Auf ähnliche Weise können in Zukunft auch andere einzelne Dienste abgesichert werden. Im Nahbereich wäre hier vor allem der WWW/http-Dienst zu nennen.

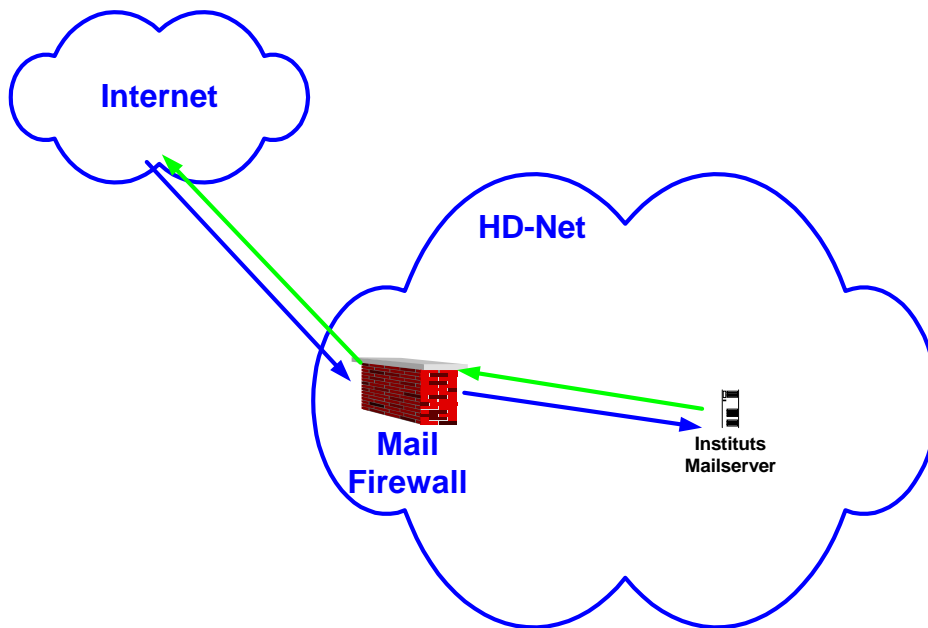


Abb. 3 Mail-Firewall: Alle eingehende (blau) und ausgehende Mail (grün) muss über die Mail-Firewall laufen. Mailserver in den Instituten sind möglich, stehen aber „in der 2. Reihe“ und werden so durch die Mail-Firewall geschützt. Direkte (smtp-) Mailverbindungen von Rechnern oder Servern mit dem Internet sind unterbunden.

4. Landesforschungsnetz BelWü

Das Netz der Uni-Heidelberg ist in das Landesforschungsnetz „BelWü“ eingebunden. Das BelWü-Netz hat die eigentlichen Übergänge zum Internet über die verschiedenen Austauschpunkte mit anderen Providern. Auch hier findet, in Absprachen mit den Universitäten, eine Filterung der Daten statt.

5. Gesamtkonzept

Um den Datenverkehr zum und vom Internet zu garantieren, müssen diese verschiedenen Filter und Firewalls aufeinander abgestimmt sein, so dass die Sperrungen tatsächlich funktionieren, aber die gewünschten Verbindungen nicht behindert werden.

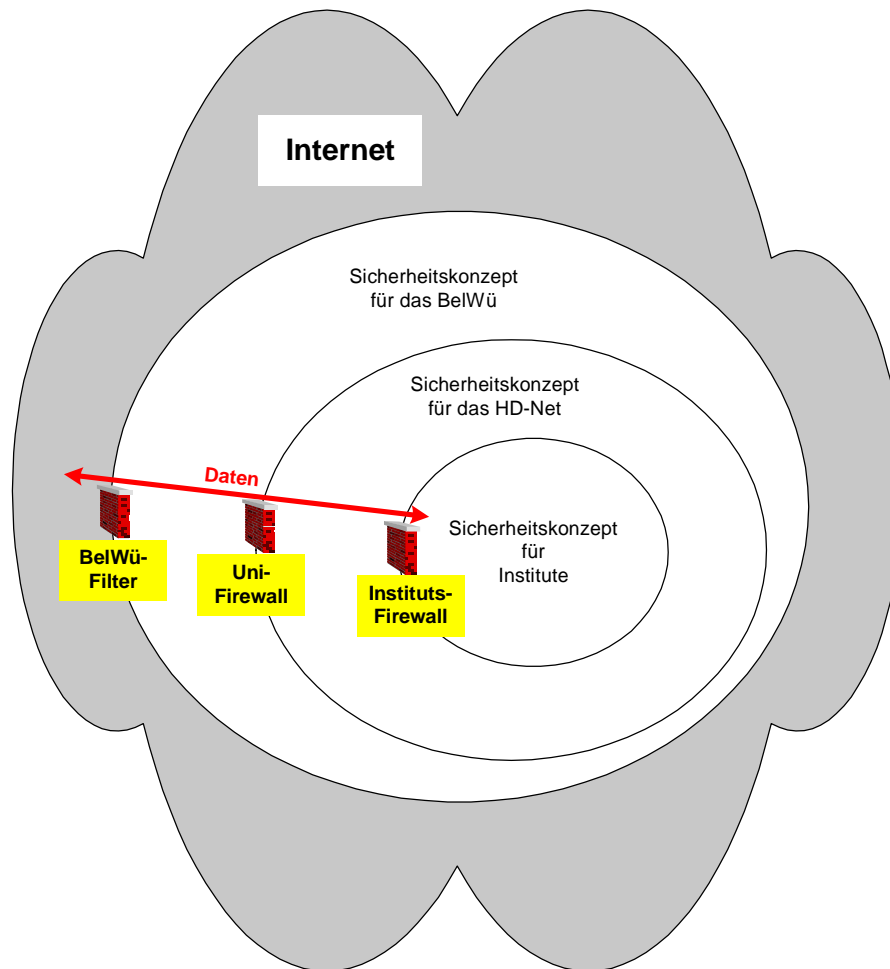


Abb. 4 Gesamtkonzept: Die Filter und Firewalls müssen so aufeinander abgestimmt werden, dass zwischen den Endteilnehmern die gewünschte Sicherheit gewährleistet ist und gleichzeitig die erwünschten Verbindungen und Dienste nicht behindert werden.

Die Erfahrung zeigt, dass ein hohes Maß an Flexibilität benötigt wird. Zum einen ändern sich die Verfahren der Angreifer und zum anderen haben die Institute wechselnde Wünsche nach besonderem Schutz oder erweiterten Möglichkeiten.

Daher gibt es kein fertiges Sicherheitskonzept. Der Wandel findet fast täglich statt. Auf viele Änderungen muss dazu auch noch schnell reagiert werden, wobei „schnell“ innerhalb von Stunden bedeutet.

Ein ernsthaftes Sicherheitskonzept stellt daher nicht nur einfach einige Filterregeln zusammen, sondern muss die folgenden Funktionen erfüllen:

- Ständige Überprüfung des Konzeptes und der Filter auf wechselnde Angriffe und Wünsche der Nutzer.
- Exaktes Verständnis aller Dienste in Bezug auf deren Verhalten im Internet.
- Weiterbildung der zuständigen Beauftragten an den Instituten.
- Aktualisieren der Dokumentation realisierter und möglicher Maßnahmen.
- Unterstützung der Institute bei erfolgten Einbrüchen.

- Ständige Verfolgung aller Sicherheitswarnungen, deren Auswertung nach relevanten Informationen und die Umsetzung dieser im Sicherheitskonzept; sowie die Information der Nutzer und/oder Netzbeauftragten.

Da der Datenverkehr durch Filter (auch an der Gegenstelle) unübersichtlicher wird, erschwert sich die Fehlersuche, und neue Dienste müssen teilweise mühsam eingerichtet werden.

Zusätzlich ist eine erhöhte Präsenz erforderlich. Da neue Angriffe meist nachts stattfinden (USA), ist es prinzipiell schwierig, rechtzeitig vor Ort zu sein. Insbesondere bei Krankheit und Urlaub kann die Position nicht gänzlich unbesetzt bleiben.

6. Ressourcen

Zur Umsetzung und Koordinierung der obigen und der im weiteren Text beschriebenen Aufgaben werden mindestens drei Mitarbeiter benötigt. Die Stellen müssen langfristig besetzt werden, damit das erarbeitete Spezialwissen nicht durch häufigen Stellenwechsel verloren geht. Regelmäßige Übergangszeiten, in denen die Stellen unbesetzt sind oder sich neue Mitarbeiter erst einarbeiten müssen, schwächen den Schutz durch das Sicherheitskonzept.

Zur Entscheidung liegt die Grundsatzfrage an, ob sich das URZ besser als bisher um das Thema EDV-Sicherheit für die Universität kümmern kann. Dazu muss die grundsätzliche Bereitschaft in der Universität vorhanden sein, allgemeine Entscheidungen über Sicherheitsfragen für die ganze Universität dem Rechenzentrum zu überlassen.

Konkret geht es darum, eine Entscheidung für eine Positivliste erlaubter Server und erlaubter Dienste zu fällen, anstelle der bisherigen Einzelsperrungen.

Die Frage, ob mehr EDV-Sicherheit für die Universität erreicht werden kann, ist zum anderen eine Frage zur Verfügung stehender bzw. benötigter Ressourcen. Diese umfassen

- Personal: Drei Stellen, davon zwei Stellen Bat IIa und eine Stelle Bat IVa/b
- Hardware: Firewall- und IDS-Module für die Core-Router im neuen Backbone, Software zur Steuerung und Auswertung dieser Module, Kosten ca. 200 T€
- Hardware/Software: WWW-Proxy, der Filterungsaufgaben wahrnehmen kann, Kosten ca. 50 T€
- Laufende Kosten (u. a. für Wartung oder die ständige Aktualisierung von Signatur-Dateien) müssen noch ermittelt werden

2. Entwicklungen: Universität, EDV und Internet

2.1. Zunahme der EDV-Nutzung

Wenn zur Zeit der Gründung der URZ noch die Ausführung von Rechnungen im Vordergrund der Arbeit der Nutzer von EDV-Systemen standen, ergab sich mit der Einführung des PCs und der grafischen Textverarbeitung eine Nutzungsmöglichkeit, die weit mehr Nutzer anzog. Spätestens seit der Vernetzung dieser Arbeitsplatz-PCs und mit den Möglichkeiten des Text- und Nachrichtenaustausches via Email sowie den Möglichkeiten der Informationsbeschaffung und -Recherche via WWW ist ein vernetzter EDV-Arbeitsplatz sowohl im wissenschaftlichen als auch im nichtwissenschaftlichen Bereich nicht mehr wegzudenken.

Die starke Verbreitung wurde dabei durch Automatismen befördert, die es mit vergleichsweise wenig Schulung möglich machten, den PC am Arbeitsplatz zu nutzen. Die notwendige Software, z. B. Email-Programme und WWW-Browser, wurde in schneller Entwicklung mit vielen bequemen Zusatzfunktionen ausgestattet.

Im Laufe dieser Entwicklung wurde der Aspekt „Sicherheit“ auf vielen Ebenen nur ungenügend beachtet. Sei es bei den Entwicklern von Software, die unter Veröffentlichungsdruck missbrauchbare Ungenauigkeiten übersahen, oder bei den Anwendern, die wegen der gestiegenen technischen Zuverlässigkeit der Hardware auf Sicherung ihrer Daten verzichteten.

2.2. Derzeitige Situation

Im Jahre 2000 begann mit dem ILOVEYOU-Email-Virus ein neuer Grad an Schadensmechanismen sich durch das Internet, in diesem Falle genauer: das Email-System, auszubreiten.

Genau die Automatismen, die das Arbeiten mit dem Computer so einfach machen, dass viele Nutzer überhaupt erst die Möglichkeiten der EDV-gestützten Arbeitsorganisation nutzen können, wurden und werden missbraucht. Es wird Schaden angerichtet durch das Benutzen des Rechners z. B. zum Versenden von Massen-Emails, oder es werden Dateien beschädigt oder gelöscht u. a. m..

Im Jahre 2001 wurden mit dem Nimda-Virus erstmals verschiedene Ausbreitungsmechanismen zugleich ausgenutzt, und zwar sowohl Server- als auch Client-Funktionalitäten bei Windows-Rechnern.

Mit der Welle von Angriffen gegen schlecht gewartete Linux-Systeme Ende 2001 / Anfang 2002 wurden auch Nutzer (und Systemverwalter) dieser Systeme schwer getroffen.

Gegenwärtig kommen - mit der sich ja immer mehr ausweitenden Nutzung von EDV-Anlagen - nicht nur ständig neue sinnvolle Serverdienste auf, sondern jeder dieser komplexen Dienste enthält mit hoher Wahrscheinlichkeit Fehler. Damit sind weiterer Missbrauch und Schäden auch für die Zukunft zu erwarten.

Spätestens seit 2001 wurde in allen Bereichen des öffentlichen Lebens der Blick auf die „Sicherheit“ von Einrichtungen und Daten gelenkt. In diesem Papier soll vor allem auf die

Netz-seitigen Bedrohungen und Schutzmaßnahmen eingegangen werden. Aber auch elementare „klassische“ Maßnahmen sollen erwähnt und müssen in einem umfassenden EDV-Sicherheitskonzept bedacht werden.

2.3. Bedrohungen und Sicherheitsprobleme an der Uni

Im folgenden wollen wir nur einige Punkte aufzählen, die an der Universität immer wieder vorkommen und eine Bedrohung der Sicherheit, insbesondere der Passwörter oder der Daten bedeuten.

- sorgloses Nutzer-Verhalten: Surfen, Email, Passwortweitergabe, Gefahr des „social engineering“
- mangelndes Schulungskonzept für Nutzung der Büroautomation
- unzureichend gewartete Endnutzerrechner:
 - keine Datensicherung
 - kein Virenschutz
 - keine „sicheren“ Standardeinstellungen für Browser und Email-Client (bzw. alte Versionen, die noch vergleichsweise unsichere Standardeinstellungen haben)
 - keine Updates der angreifbaren Standardprogramme, z. T. weil das mit der vorhandenen Hardware nicht möglich ist
- kein Passwortschutz im Netz („Ich wollte nur dem Kollegen die Daten zur Verfügung stellen, und habe dann vergessen, die Freigabe / den Dienst wieder abzustellen“, oder auch das SQL-Server-Problem in 2002, wo in vielen an das Internet angebundene Datenbank-Systemen seit der Installation einfach kein Administrator-Passwort eingetragen war.)
- Klartext-Passwörter in leicht abhörbaren (mit Hubs statt Switches aufgebauten „shared“) Netzen
- Neue Dienste, z. B. Peer-to-peer-„Netze“: Einerseits stellen diese für heutige Nutzer eine Innovation dar, andererseits sind diese entstanden, um privaten Interessen zu dienen. (Man beachte hier den Unterschied zum WWW/http-Dienst, der direkt für den wissenschaftlichen Informationsaustausch entwickelt wurde.) Es entstehen zum Teil hohe Kosten, wenn Nutzdaten-abhängige Abrechnung für die Internet-Verbindung festgelegt ist, oder ein Ausbau der Anbindung nötig wird, um ständig verstopfte Verbindungen zu verbessern. Außerdem besteht ein Risiko für die Daten, z. B. ist die versehentliche Bereitstellung aller Daten einer Festplatte leicht möglich. Durch die „Subkultur“ ist zudem nicht auszuschließen, ob in solche Software nicht „Hintertüren“ eingebaut sind.

Besonders bedrohlich werden diese Nachlässigkeiten, wenn Insider mit Wissen über die internen Strukturen bewusst Schaden anrichten wollen.

2.4. Schäden

Sehr detaillierte Auflistungen von Bedrohungen und Schäden finden sich z. B. im IT-Grundschutzhandbuch der Bundesanstalt für Sicherheit in der Informationstechnik.

2.4.1. Passwort-Kompromittierung

Eine Organisation wie die Universität verfügt über eine umfangreiche IT-Infrastruktur, die im wesentlichen durch eine Nutzerkennung und nur ein Nutzerpasswort zugänglich sind.

Würde man für jeden möglichen Dienst ein anderes Passwort verwenden, so würde eines der Hauptziele, nämlich die Nutzung der und Schulung in dieser Infrastruktur, erheblich erschwert werden.

Andererseits verwenden viele Nutzer nur Teile dieses umfangreichen Angebotes, und wissen nicht, was ein „Kundiger“ mit einer Nutzerkennung alles anstellen kann. Als Beispiel seien das Verschicken von Massen-Werbemails oder das Aufsetzen von IRC-Proxies unter fremden Nutzerkennungen genannt.

Bei rechtlich relevanten Problemen kann der Schaden für den einzelnen Nutzer recht hoch werden.

2.4.2. Denial-of-Service

Darunter versteht man ein „außer-Dienst-Setzen“ von Rechnern durch massive Datenanforderungen aus dem Internet.

Wenn Rechner der Universität sich (in der Regel ungewollt) an solchen Angriffen gegen kommerzielle Systeme beteiligen, sind in Zukunft Schadensersatzforderungen nicht auszuschließen.

2.4.3. Rechnereinbruch

Die Schäden eines Rechnereinbruchs belaufen sich unterschiedlich hoch, je nachdem, welche Bereiche betroffen sind:

- Endnutzersystem mit gesicherten (bzw. zentralgespeicherten) Daten: und ca. 2-5 Applikationen: Arbeitszeit zum Neueinrichten des Rechners, ca. 1/2 bis 1 Personentag
- Endnutzersystem mit ungesicherten „normalen“ Daten: Neuerfassung von Texten für Publikationen oder Anträgen, von Rechenschemata etc.. Selbst hier können im ungünstigen Fall schnell hohe Schäden entstehen, wenn z. B. hierdurch Antragsfristen versäumt werden.
- Endnutzersystem mit ungesicherten Forschungsdaten: Je nachdem, wie diese Daten erhoben wurden, kann eine Wiederholung des Experimentes Tage, Wochen, Monate dauern.
- Zusätzlich treten Produktivitätsverluste auf, und zwar für den Nutzer, dem der Rechner und die Daten fehlen, sowie für den, der den Schaden beheben muss.
- Bei einem Serversystem sind zusätzlich die Produktivitätsverluste für alle Nutzer, ein eventueller Imageverlust für das Institut und die Universität zu bedenken.

- Als Abschätzung für den Produktivitätsverlust an einer Universität könnte man einen Anteil des Gesamtbudgets für die Universität bezogen auf die Zahl der Wissenschaftler der Institute ansetzen: Die Dimension dieser Zahlen geht in die Tausende Euro pro Wissenschaftler-Tag Ausfall der Systeme.
- Bei mehreren gleichzeitigen Einbrüchen auf gleichartige Rechner bei einem einzigen aber massiven Sicherheitsvorfall, wie es z. B. das Kirchhoff-Institut für Physik erleiden musste, beziffert sich der Schaden leicht in die Zig-Tausende Euro!
- Wenn der Rechner bei externen System Schäden verursacht, sind in der Zukunft Schadensersatzforderungen nicht auszuschließen

Die EDV- und Netzbetreuer der verschiedenen Institute waren und sind aus verschiedenen Gründen nicht in der Lage, diese Bedrohungen zeitgerecht abzufangen, so dass z. T. erhebliche Schäden entstanden und immer wieder entstehen.

Gründe sind u.a.

- schlechtes Grundwissen, mangelnde Sensibilität, keine Zeit oder kein Interesse zur Teilnahme an / Kenntnisnahme der vom URZ angebotenen Weiterbildungs- bzw. Schutzmaßnahmen
- keine Zeit, die Maßnahmen im Institut umzusetzen
- viele, veraltete und / oder inhomogen ausgestattete Rechner oder auch Betriebssysteme
- mangelnde Akzeptanz von Sicherheitsempfehlungen durch die Nutzer („es geht doch bequemer“)

Von daher sind einerseits „zentrale“ Sofort-Maßnahmen nötig, und andererseits die Erstellung und Umsetzung eines EDV-Sicherheitskonzeptes mit entsprechendem Personal. Das URZ als Kompetenzzentrum muss die Institute in diesen Fragen besser beraten und unterstützen können, als das bislang möglich ist.

3. Ziele eines EDV-Sicherheitskonzeptes

3.1. Universitätsweite EDV-Sicherheits-Policy

Ziel eines EDV-Sicherheitskonzeptes muss es sein, die Teilnetze, die Rechner, die Daten und damit „die Nutzer“ innerhalb des HD-Net unter möglichst vielen relevanten Gesichtspunkten besser als bislang abzusichern. Dies beinhaltet zum einen die Definition eines erwünschten Grades an Sicherheit sowie die Maßnahmen zum Erreichen dieses Schutzes, zum anderen die fortdauernden Aktivitäten zum Erhalt bzw. zur Anpassung an neue Gegebenheiten („get secure – stay secure“).

Im folgenden ein kurzer Vorschlag für Richtlinien im Bereich EDV-Sicherheit, die Uni-weite Gültigkeit haben sollten, sofern nicht im Einzelfall sogar strengere Richtlinien erforderlich sind:

- Information ist für eine Universität Grundlage für Forschung und Lehre. Erworbenes Wissen wird als Information aufgezeichnet und weiterverbreitet. Verlust, Verfälschung oder ungewollte bzw. verfrühte Publikation der elektronisch gespeicherten Daten sollte in allen Bereichen der Universität vermieden werden.
- Bei aller Offenheit einer Universität und unter Beachtung der Freiheit von Forschung und Lehre sind EDV-Systeme heute in den meisten Fällen Arbeitsmittel, für die ein gewisses einheitliches Maß an Sicherheit in der Benutzung erreicht werden soll.

Diese grundlegenden Richtlinien, zusammen mit den vielen verschiedenen Zielgruppen einer Universität, machen die Einrichtung von zentral gesteuerten Sicherheitssystemen und entsprechender Regelungen zu einer komplexen, ständig zu aktualisierenden Aufgabe. Es ist nicht so einfach wie bei einem kommerziellen Produzenten, wo man klar zwischen Intranet und Kundenserver unterscheiden kann, weil die Rollen schon innerhalb der „Firma Universität“ wechseln.

3.2. Wer sollte sich alles um Sicherheit bemühen?

Eine allgemeine Sicherheitskonzeption sieht ein Nebeneinander der „drei Säulen“ vor, die zum Funktionieren des „PCs im Netz“ beitragen, die folglich auch alle drei zum effektiven Erreichen des erwünschten Maßes an Sicherheit beitragen müssen: Systemadministrator, Netzwerkadministrator und auch der Nutzer.

Die Unterscheidung der Administratoren mag dabei spezifisch für die Universität mit ihren dezentralen Strukturen bei zentraler Infrastruktur sein, muss aber gerade deswegen hier gemacht werden. Im dezentralen kooperativen EDV-Konzept finden sich die Nutzer und Systembetreuer im Institut, während die Steuerung des Datennetzes im wesentlichen vom Rechenzentrum aus geschieht.

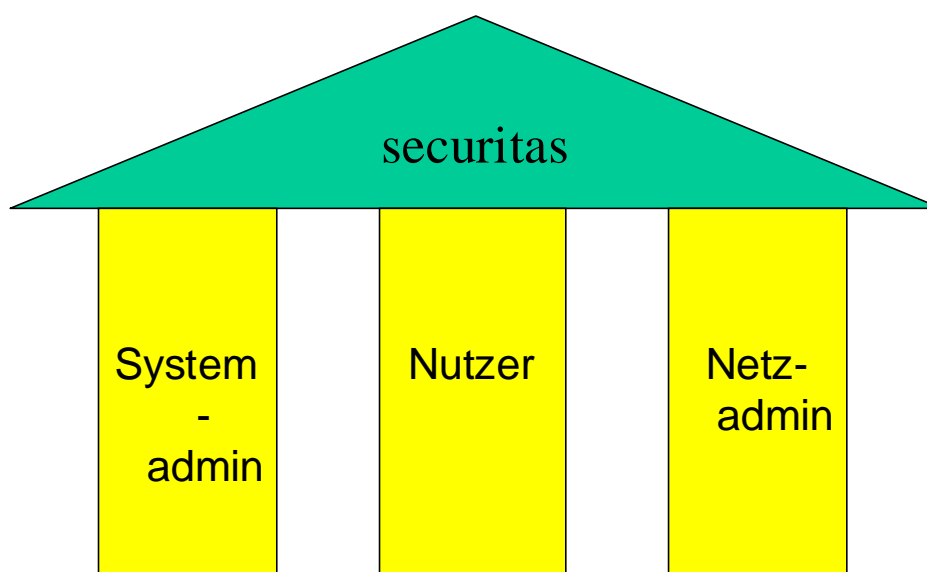


Abb. 5: Die „Drei Säulen“ der EDV-Sicherheit**1. Nutzer**

Ziele eines Sicherheitskonzeptes in Bezug auf die Nutzer müssen sein:

- verantwortungsvoller und bewusster Umgang mit den Ressourcen
- Grundverständnis für das Arbeiten am Computer und im Netz
- Wissen um aktuelle relevante Gefahren bzw. Einbindung in Informationsketten

2. System/Rechner

Endnutzer-Rechner (PCs) sollten im Systemaufbau und in der Ausstattung mit Software und deren Konfiguration so eingestellt sein, dass Fehlbedienung und Missbrauch erkannt und verhindert werden können.

Das Rechenzentrum strebt an, den Aufbau dezentraler Server im Institut für weltweite Standarddienste möglichst überflüssig zu machen. Damit verringert sich ganz erheblich die Gefahr schlecht gewarteter anfälliger Rechner mit Serverdiensten.

Als Server wird hierbei jeder Rechner und jeder Prozess auf einem Rechner verstanden, der anderen Rechnern, den Clients, die Möglichkeit bietet, über das Netzwerk Datenanfragen zu stellen und Antworten zu erhalten. Dazu zählen insbesondere auch die Datei- bzw. Druckerfreigabe unter Windows, oder auch die Peer-to-peer-Programme, bei denen man in der Regel eigene Daten zur Veröffentlichung freigibt. Die Erfahrung zeigt, dass viele Nutzer nicht wissen, dass die Verwendung dieser Programme aus Ihrem Rechner einen Server macht.

Ziel muss sein, die Betreiber von Rechnern im Datennetz in die Lage zu versetzen, die Vielzahl von Rechnern im Netz so zu administrieren, dass die Rechner möglichst geringe „Angriffsflächen“ bieten.

3. Netz

Im weiteren betrachten wir vor allem Maßnahmen, die den Schutz vor dem Netz durch das Netz erhöhen können.

3.3. Modularität

Für die Maßnahmen ist möglichst Modularität anzustreben. Dies hat mehrere Vorteile:

- Modularität kann die dezentrale Struktur besser abbilden und verschiedene erwünschte Sicherheitsstufen berücksichtigen.
- Modularität kann die verschiedenen Aufgaben der Computersysteme besser abbilden.
- Mit Modularität kann eine Hintereinanderschaltung unabhängiger Stufen erreicht werden.
- Einzelne Module können unabhängig voneinander geprüft werden.

Allerdings: In einer gewachsenen EDV-Landschaft ist das nicht sofort umsetzbar, sondern vor allem als Leitlinie hilfreich. Module erfordern zudem definierte Schnittstellen, die einheitlich umgesetzt werden müssen, z. B. IP-Adress-Bereiche, Meldung von Systemen.

3.4. Firewall und Firewall-Hierarchie

Als Mittel, alle Probleme mit Endsystemen zu „überspielen,“ die sich aus mangelnder Nutzerschulung und fehlender Systempflege ergeben, wird häufig genannt: „Installieren Sie eine Firewall!“

Was ist eine Firewall? Wer darunter eine „Kiste“ versteht, die vor den Internet-Zugang geklemmt wird und dort für „einigermaßen Sicherheit“ sorgt, hat zwar viele praktische Fälle damit beschrieben, aber nicht unbedingt recht.

Zunächst ist die Firewall - in Anlehnung an die Brandschutzmauer - das Konstrukt, das unser Netz vom brennenden Netz nebenan - dem Internet, oder dem HD-Net - trennt.

Es ist eine Mauer, also ein die Freiheit beschränkendes Hindernis, mit dem Ziel der Abschottung.

Im erweiterten Sinne bezeichnet man als Firewall „alle“ netzseitigen Maßnahmen zum Erreichen und Erhalten der Richtlinien zur EDV-Sicherheit.

Der Aufbau einer „Firewall“ setzt also voraus, dass man weiß, was man schützen will, wie weit man es schützen will, und mit welchem Aufwand man es schützen will.

Dies erfordert eine Analyse und Bewertung möglicher Bedrohungen. Im weiteren Schritt kann man dann die passenden Mittel zur Verhinderung oder Verminderung der Gefahren wählen. Detailanalysen einzelner Internet-Dienste oder -Handlungen finden sich z. B. im BelWü-Papier oder bei der BSI. Wir wollen die Frage stellen, wie wir das für die Universität und ihre Institute umsetzen können.

3.4.1. Elemente einer Firewall für die Universität

Im folgenden werden einige Elemente einer Firewall kurz vorgestellt.

Mit „Paketfilterung“ bezeichnet man die Prüfung einzelner Datenpakete aufgrund des „Adressaufklebers“ bzw. der Deklaration des Datentyps (Port-Nummer, siehe unten). Man unterscheidet die grundlegenden Prinzipien einer „Blacklist“ (was nicht explizit verboten ist, ist erlaubt) und einer „Whitelist“ (was nicht explizit erlaubt ist, ist verboten).

Bei einer „stateful firewall“ findet eine Paketfilterung unter Berücksichtigung voriger Datenpakete in einer konkreten Verkehrsbeziehung statt. Hier können gewisse Paket-Typen „einfacher“, z. T. auch „sicherer“ berücksichtigt werden.

Ein „Proxyserver“ steht wie eine „Anwendungs-Firewall“ für eine Maßnahme, alle Daten eines Anwendungstyps über eine zentrale Stelle vermitteln zu lassen. Beim Proxyserver steht dabei der Aspekt der Zwischenspeicherung und damit der Erhöhung der Zustell-Geschwindigkeit im Vordergrund, bei der Anwendungs-Firewall hingegen die weitergehende Untersuchung und Filterung von Datenpaketen.

Bei einem „Inhaltsfilter“ findet eine Prüfung nicht nur des „Adress-Aufklebers,“ sondern auch des Inhaltes statt.

Bei „NAT“ (Netzwerk-Adressen-Umsetzung/Translation) werden nicht via Internet vermittelbare Adressen verwendet. In vielen Firewall-Implementierungen gehört NAT zur Grundausstattung, im Rahmen der Universität bedeutet dies einen hohen Umstellungsaufwand, und der Verlust vieler direkter Möglichkeiten im Internet (RFC 2775, „Internet Transparency“)

Die allgemeine Sicherheitsdiskussion führte bei vielen Anwendern zur Einrichtung von Sicherheits-Lösungen auf dem Arbeitsplatz-PC, wie Virenschutz oder Personal-Firewall. Siehe dazu auch weiter unten.

3.4.2. Uni-Firewall

Gewisse Schutzmechanismen können und sollten Uni-weit einheitlich vorgesehen werden:

- Netzwerkkomponenten sollen i. a. nicht von außerhalb der Universität zugänglich sein.
- Leicht missbrauchbare LAN-Protokolle sollten nicht nach außen gegeben werden.
- Datenpakete von innerhalb der Uni sollten nicht fremde Absender-IP-Adressen tragen.
- Bestimmte IP-Adressen (z. B. private Netze) von außen sollten nicht auf das HD-Net zugreifen dürfen bzw. als Zieladresse nach außen gegeben werden.
- Nur bestimmte Rechner im HD-Net sollten als Server angesprochen werden können.

Allerdings handelt es sich dabei nur um einen groben Filter, der nicht die Detailwünsche nach „mehr Schutz“ für einzelne Institute abdecken kann.

Auch muss bei einem so zentralen Filter die Freiheit von Forschung und Lehre angemessen berücksichtigt werden. Eine Universität ist keine Bank mit rigiden Tresorwänden; neuen Entwicklungen muss Raum gegeben werden.

3.4.3. Instituts-Firewall

Die Anforderungen an den Datenschutz, insbesondere bei Verarbeitung personenbezogener Daten, hat in mehreren Teilnetzen innerhalb der Universität schon seit längerem zum Einsatz von institutseigenen Firewalls geführt. Insbesondere in der zentralen Universitätsverwaltung, dem Klinikum oder in einem Projekt der juristischen Fakultät mussten Firewalls mit z. T. aufwändiger Hard- und Software eingerichtet werden. Auch andere Institute betreiben eine Firewall in Eigenregie.

Wo diese Firewall nicht einfach komplett den Datenverkehr blockiert, berichten diese Institute von einem hohen erforderlichen Personalaufwand, nicht nur zum Einarbeiten und Einrichten, sondern auch zur Wartung und Instandhaltung der Firewall, sowie zur Reaktion auf Nutzerwünsche.

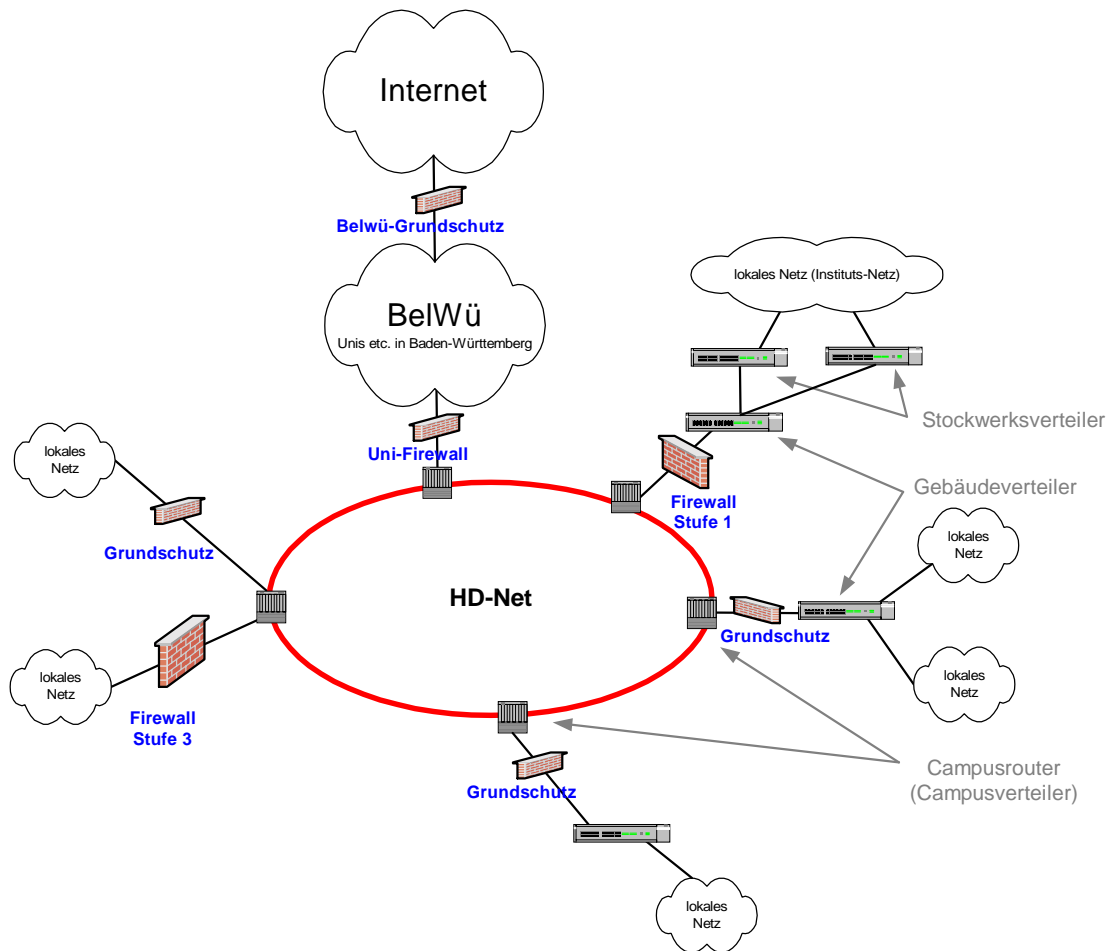


Abb. 6: Firewall-Konzept mit Instituts-Firewalls unterschiedlicher Sicherheitsstufen

Obwohl ja im Rahmen des dezentralen kooperativen EDV-Systems die Verantwortung für Instituts-spezifische Maßnahmen im Institut liegt, möchte das URZ der Mehrzahl von Instituten diesen nicht unerheblichen Aufwand ersparen, und ein abgestuftes Konzept von zentral administrierten Regelsätzen anbieten.

Die Details der Stufen sollten für die teilnehmenden Institute dokumentiert werden. Änderungen sollten bekannt gegeben werden. Das Institut kann dann aus den angebotenen Regelsätzen denjenigen wählen, der das jeweils benötigte Anwendungsspektrum am besten schützt.

Wir glauben, dass auf diese Weise ein vernünftiges Maß an Sicherheit mit einem effektiven zentralen Einsatz von Personal erreicht werden kann: Es muss nicht in jedem Institut ein Fachmann für Firewalls eingestellt werden.

Filterungen vor jeder Einheit sind sinnvoll, denn der Filter vor einer Struktur, z. B. der Uni, hilft nichts im Datenverkehr innerhalb, z. B. zwischen den Instituten.

Ein weiterer Vorteil einer solchen Konzeption mit hintereinander geschalteten Filtern ist, dass eine Verteidigung „in der Tiefe“ erreicht wird: Bei Ausfall eines Filters ist noch ein Restschutz durch die anderen vorhanden.

3.4.4. Anwendungs-Firewalls

Wenn Anwendungen zwischen Rechnen über Netze hinweg Daten austauschen wollen, so tun sie das über vereinbarte Protokolle, in denen je Protokolltyp weltweit vereinbarte Kennzahlen verwendet werden, die sog. Port-Nummern.

Ein Beispiel ist der Email-Versand: Um eine Email von einem Computer auf einen anderen zur Weiterverbreitung übertragen zu können, hat sich das Protokoll SMTP im Internet durchgesetzt, dem die Port-Nummer 25/tcp zugeordnet ist.

Als nun der Missbrauch von Mailsystemen überhand genommen hatte, wurde ein Paketfilter so geschaltet, dass Datenpakete dieses Protokolltyps nur noch zu den zentralen Mailverteiltern der Universität gelangen konnten. Dort werden die Pakete nach bestimmten Kriterien hin untersucht und von dort aus weiter vermittelt.

Auf diese Art konnte zum einen erreicht werden, dass Rechner der Universität nicht mehr zur Verbreitung ungewollter Massen-E-mails (sog. Spam) missbraucht werden, und zum anderen war hiermit die Möglichkeit gegeben, die Nutzer vor einkommender Spam-Mail und vor Email-Viren zu schützen.

Bei weiteren Diensten wäre eine solche Filterung und Kontrolle sinnvoll:

- Bestimmte ältere Protokolle (z. B. Telnet, FTP) im Internet versenden Passwörter im Klartext, solche sollten nicht mehr im Datenaustausch mit „fremden Netzen“ allgemein verwendet werden. (Dabei gibt es jedoch sinnvolle Ausnahmen, z. B. erlaubte „anonyme“ FTP-Server. Hier hilft allgemein nur, den Nutzer zu informieren.)
- In den vergangenen Jahren wurden viele Rechner, auf denen WWW-Serverdienste liefen, Ziel von Angriffen. Die betroffenen Ports sind 80, 443 und weitere.
- Mittelfristig sollten wichtige Dienste auch auf höheren Ebenen gesichert werden. Insbesondere werden heute schon viele Schadprogramme über WWW-Seiten verbreitet, hier könnte ein kompetenter Viren-/Schadprogramm-Scanner als Teil eines leistungsfähigen web-Proxies einen großen Teil ausfiltern.
- Die in den vergangenen Jahren aufgetauchten sog. Peer-to-peer-Netze, die bislang vor allem zum Tausch von Multimedia-Daten (Musik, Video) dienten, haben einen enormen Anstieg der Netzlast verursacht. Da viele Internet-Anbindungen volumenabhängig abgerechnet werden und zudem Grenzbereiche der Legalität von den Nutzern eventuell zu naiv betreten werden, ist es sinnvoll, diese Anwendungen nicht zuzulassen.
- Letztlich führen diese Forderungen dazu, nur noch erwünschte Kommunikations-Ports zu erlauben, und alle anderen als nicht erwünscht zu blockieren. Dies bedeutet, den zentralen Paketfilter künftig als „Whitelist“ zu betreiben.

Ein grundsätzliches Problem der Filterung von Anwendungs-Daten sei nicht verschwiegen: Die Filterung aufgrund von Ports beruht auf Verabredung. Wenn nun viele Nutzer einen sonst anders benutzten Port (z. B. Port 80, normalerweise http-Daten) miteinander für ihre Zwecke verwenden und wenn die Nutzdaten formal sogar den Anforderungen dieser Daten genügen, wie kann diese Form des Missbrauches unterbunden werden?

Sicherheit aus dem Netz kann hier zunächst nur vor Flüchtigkeitsfehlern helfen, nicht vor Vorsatz aus dem Inneren des Netzes. Für diese und andere künftige Probleme müssen Lösungen entwickelt und umgesetzt werden.

3.5. Intrusion Detection und proaktive Netzwerk-Scans

Um eine halbwegs nutzerfreundliche Offenheit des Systems zu bewahren, wie sie um der Freiheit von Forschung und Lehre willen sinnvoll und notwendig ist, ist Sicherheit mit Kontrollen unumgänglich.

In Kontrollen kann der Datenverkehr statistisch ausgewertet werden, um unübliche Verkehrsmuster oder charakteristische Signaturen zu erkennen. Wenn plötzlich viele Datenpakete auf bislang unüblichen Ports ankommen, so ist die Wahrscheinlichkeit hoch, dass eine neue Schwäche in einem Anwendungsprogramm entdeckt und ausgenutzt wurde.

Diese Analyse kann auf verschiedenen Stufen erfolgen, sowohl in zentralen Komponenten in der Nähe der Internet-Anbindung, als auch auf „lokalen Agenten“ im Institut, bis hin zu speziellen Programmen auf einzelnen Rechnern.

Man nennt dieses Vorgehen, mögliches oder stattgefundenes Eindringen in das eigene Netz zu erkennen, „Intrusion Detection“.

Intrusion Detection kann in zwei Richtungen ausgebaut werden:

- Frühzeitige Erkennung von Bedrohungen von außen, indem nicht nur grobe statistische Auswertungen vorgenommen werden, sondern auch charakteristische Signaturen erkannt und automatisierte Schutzmaßnahmen ergriffen werden können.
- Erkennen von Rechnern mit Problemen im Inneren des HD-Net,
 - einerseits durch Meldungen aus der Analyse der Netzwerk-Aktivitäten,
 - andererseits durch aktives Scannen seitens des URZ, um mögliche Schwächen der Systeme im HD-Net vorab erkennen zu können.

Diese Kontrollen und die eventuell nötigen Reaktionen bedeuten einen erheblichen Zeitaufwand.

Das Gegenkonzept zum Erreichen eines vergleichbaren Sicherheitsniveaus wäre, alles zu verbieten, dann muss auch nichts kontrolliert werden. Jedoch betonen wir nochmals: Eine Uni ist keine Bank, „Einmauern“ ist ja eigentlich nicht erwünscht. Wofür würden sonst Millionenbeträge für eine schnelle Netzanbindung und entsprechende Netzkomponenten ausgegeben?

3.6. Incident Response

Die Reaktion auf ein erkanntes Eindringen, auf beobachtete Gefahren oder auf von außen zentral gemeldete Probleme im eigenen Netz wird „Incident Response“ genannt. Diejenigen Mitarbeiter, die sich um die Weiterleitung, Bearbeitung (z. B. Sperren des Rechners) und Beantwortung kümmern, bilden das „Security Incident Response Team“.

Der Begriff CERT („Computer Emergency Response Team“) wird oft auch Synonym zu SIRT verwendet.

Diese Aufgaben sind sehr zeitaufwändig, weil auf erste Warnungen hin Informationen beschafft und weitergeleitet werden müssen, erste Maßnahmen ergriffen (und später dann wieder rückgängig gemacht) werden müssen, und immer wieder auch konkrete Rückfragen beantwortet werden.

Insbesondere in der Zusammenarbeit mit der BelWü-Koordination können in den Bereichen „Intrusion Detection“ und „Incident Response“ voraussichtlich gute Ergebnisse erreicht werden.

3.7. Weitere Sicherheitsaspekte

3.7.1. OSI-7-Schichtenmodell

Analog zum OSI-Modell der Datenkommunikation sollte auch der Aspekt „Sicherheit“ für jede der Übertragungs-Ebenen betrachtet werden. Im folgenden nur einige Anmerkungen und Stichpunkte, die in einer Uni-weiten bzw. Instituts-internen Sicherheits-Policy beachtet werden sollten.

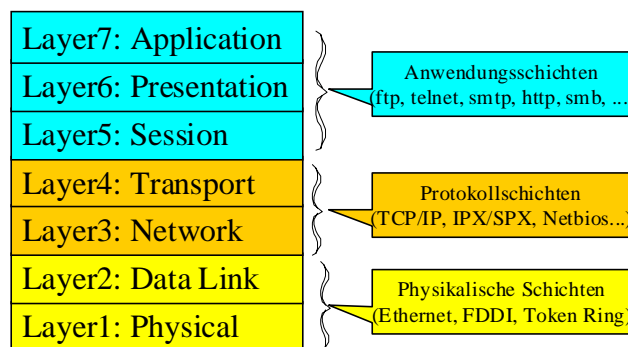


Abb. 1: Die einzelnen Schichten des OSI-Modelles entsprechen den unterschiedlichen Aufgaben in der Datenkommunikation, die von verschiedenen Programmen/Modulen erfüllt werden.

3.7.2. Ebenen 1 und 2

Hier geht es insbesondere um Kabel und den physikalischen Zugang zu Servern, Backbone- und anderen Netzwerk-Komponenten.

Wichtige Komponenten zentraler Dienste stehen in der Regel in besonders gesicherten Räumen, z. B. Maschinenraum URZ, Uni-Telefonzentrale Rektorat. Ebenso gibt es in den Instituten separate Server-Räume.

Das URZ hat in der Regel Zugang zu denjenigen Räumen, in denen zentrale Campus-Verteiler stehen. Dies wird anlässlich des anstehenden Backbone-Umbaus geprüft und vervollständigt werden.

Verteilerschränke an der Uni sind vergleichsweise „einfach“ gesichert: Es handelt sich meist um Standard-Schlösser (Dirak (1)333, Rittal 3524), diese Schlüssel werden auch an Netzbeauftragte ohne Quittung ausgegeben. Es gibt auch viele Verteilerschränke ohne Schloss, die in einem eigenem Raum untergebracht sind. Der Zugang zu solchen Räumen erfolgt oft mit Technik/Putzraum-Schlüsseln, den auch andere (auch von Fremdfirmen) haben. Im Bereich des Klinikum-Datennetzes ist eine aufwändige Klinikums-eigene Schließanlage installiert.

Betreffs der Etagen-/Zimmerverteilung hat das URZ i. d. R. keinen Zugang zum Verteiler, wohl aber viele Institutsangehörige.

3.7.3. Ebenen 2 und 3

Hier geht es vor allem um den Transport der Daten über das Netz, um Themen wie IP, IP-Spoofing, DoS, Datenverschlüsselung (VPN, ssh, ssl):

Ein echter Schutz vor „Tunneln“ ist heute nicht möglich, da Programme und Protokolle existieren, die Daten beliebig in andere Protokolle/Informationen verpacken und versenden können.

Um die Gefahr des Aushorchens und Missbrauchs von Netzen, in denen sich ein kompromittierter Rechner befindet, zu verringern, ist eine entsprechende Konfiguration und Wartung der Netzkomponenten und entsprechende fernbedienbare Geräte (wie sie in den letzten Jahren vom URZ empfohlen wurden) erforderlich. Auch dies kostet Zeit und Arbeit.

3.7.4. Ebenen 5 bis 7: Anwendungen, Rechner

Auf der Ebene des Schutzes von Anwendungen bzw. dem Rechnersystem wären die folgenden Maßnahmen zum Schutz „vor dem Netz“ zu beachten.

- Virenschutz, d. h. Untersuchung von einkommenden Dateien auf schädlichen Programmcode, wie er vom URZ auch empfohlen ist und bereitgestellt wird.
- „Personal Firewalls“, d. h. Anwendungsprogramme, die die einkommenden Datenpakete vor jeder anderen Anwendung analysieren und filtern sollen. Diese führen immer wieder zur Verunsicherung der Nutzer und zu zeitaufwändigen Rückfragen. Andererseits können solche Meldungen dann Sinn machen, wenn eine zentrale Verteilung, Konfiguration und auch Auswertung der Meldungen im Rahmen eines kollektiven Intrusion-Detection-Systems möglich wäre. Wir erwarten zukünftig eine Integration von Virenschutz- mit Personal-Firewall-Software. Entsprechende Angebote am Markt wären zu beurteilen, und Uni-weit anzubieten und zu implementieren. Ein solcher Ansatz geht über die bisherige Software-Verteilung hinaus und ist wesentlich personalintensiver.
- Es gibt auch spezielle Programme um sicherzustellen, dass die Systemdateien auf dem Rechner nicht verändert wurden, z. B. Tripwire auf unix-/linux-Systemen.
- Ebenso gibt es Programme, die verhindern sollen, dass nicht unbefugt Informationen zur Profilbildung verschickt werden, z. B. Ad-Aware auf Windows-Systemen.

Die Schädlinge kommender Zeiten werden natürlich bemüht sein, die Sicherheits-Software auf dem Endsystem (PC, Server) zu umgehen bzw. abzuschalten. Dies wird immer vor allem dann erfolgreich sein, wenn Nutzer mit hohen Privilegien arbeiten, oder die Sicherheits-Software entsprechende Sicherheitsmängel aufweist.

3.7.5. „Ebene 8“: Die Nutzer

Grundsätzliche Aussagen zum Nutzerverhalten wurden von der Universität bereits getroffen, siehe die Richtlinien unter

<http://www.urz.uni-heidelberg.de/OrgInfo/> Abschnitt „Rechtliche Grundlagen“

Nutzerschulung bzw. -Erziehung, gerade im Bereich Verhalten im Web, Email, oder auch Peer-to-peer scheinen darüber hinaus angebracht zu sein. Dazu muss jedoch aktiv auf die Nutzer zugegangen werden. Dies kann im Uni-weiten Maßstab kontinuierlich nur durch die Instituts-EDV-Beauftragten als Mittler sinnvoll geschehen. Für studentische Nutzer (Öffentliche Terminals, Laptop-Zugang, Wohnheime mit Internet-Anbindung) sind entsprechende Informationen und Hinweise zu verbreiten. Auch in der Vergangenheit war hier bereits einiger Zeitaufwand nötig, wenn das Fehlverhalten einzelner Nutzer zu Störungen ganzer Netze oder Rechnersysteme geführt hat.

4. Umsetzung des EDV-Sicherheitskonzeptes

Die oben beschriebenen Ziele und Maßnahmen wurden in vielen Punkten schon umgesetzt, andere befinden sich in Testphasen oder zum Teil auch schon „in Produktion,“ ohne von sich aus weitere Verbreitung gefunden zu haben.

4.1. Geleistete Maßnahmen

Das Universitätsrechenzentrum unternahm verschiedene Maßnahmen zur Erhöhung der Sicherheit der Endgeräte (Clients und Server).

Neben dem Angebot von zentraler Datenspeicherung (AFS) und zentraler Datensicherung (ADSM) gibt es eine Uni-weite Lizenz für ein Virenschutzprogramm (McAfee) und Beratung in Browser- und Email-Konfigurationsfragen.

Des Weiteren wurden die folgenden netzwerk-technischen Maßnahmen bereits umgesetzt.

Als „Implementierungs-Policy“ galt bislang vor allem, möglichst mit vorhandenen Geräten und Personal auszukommen.

4.1.1. Mailfirewall

Hierzu gibt es bereits ein eigenes Konzeptpapier und einen Beschluss des EDV-Ausschusses.

Details hierzu finden sich unter

<http://www.urz.uni-heidelberg.de/AllgemeinInfo/Ordnungen/firewall.shtml>

Zu erwähnen sind dabei die positiven Nebenwirkungen des Konzeptes: Was ursprünglich zur Eindämmung des Missbrauchs von Rechnern der Universität, die zur Versendung von Spam-Mail nach außen missbraucht wurden, begann, lieferte die technische Voraussetzung für eine sich ständig verbessernde Erkennung und Eindämmung von Spam-Mails und Viren-Sendungen an die Email-Empfänger in der Universität.

4.1.2. Uni-Firewall

Derzeit ist diese Firewall als Paketfilter mittels einer Accessliste auf dem Eingangs-Router der Universität implementiert. Einige Elemente dieser Filterliste werden veröffentlicht, z. B. gesperrte Netze oder Ports. Die Implementierung bzw. Automatisierung erfolgt derzeit im wesentlichen durch eigene Scripte.

Weitere Informationen zur aktuellen Implementierung finden sich auf der Seite

<http://www.urz.uni-heidelberg.de/Netzdienste/firewall/uni-firewall.shtml>

In naher Zukunft wäre eine Umstellung von der bisherigen Blacklist, bei der einzelne Dienste bzw. Rechner gesperrt sind, und ansonsten alles freigegeben ist, auf eine Whitelist zu empfehlen, also eine Positivliste einzelner erlaubter Dienste, wobei andere Dienste dann nicht mehr allgemein erlaubt sind, jedoch möglichst flexibel auf Anfrage/Antrag freigeschaltet werden sollten.

Diese Umstellung würde eine Meldung von Servern für bestimmte besonders geschützte Dienste, sowie eine Verlagerung von Servern auf festgelegte IP-Adress-Bereiche universitätsweit erforderlich machen. Dies kann im Einzelfall mit einigem Arbeitsaufwand in manchen Instituten verbunden sein.

Steigende Datenlast sowie vor allem dann steigende technische Anforderungen an die Filterung bzw. Automatisierung machen eine Verlagerung auf eigenständige Geräte bzw. Module in Netzkomponenten mit spezieller Verwaltungssoftware erforderlich.

4.1.3. Instituts-Firewall: Stufenkonzept

Anstelle für jedes Institut ein „individuelles Sicherheitskonzept“ mit den konkret verwendeten Anwendungen zunächst herauszukristallisieren und dann umzusetzen, bieten wir ein abgestuftes Angebot an „Sicherheits-Stufen“ an, aus dem ein Institut auswählen kann.

Dieses Konzept wurde den EDV- und Netzbeauftragten der Universität bereits vorgestellt, siehe auch im Anhang.

Im folgenden seien die derzeit definierten Stufen kurz beschrieben. Details dieser Stufen sind im Web für Netzbeauftragte zugänglich dokumentiert, Änderungen werden mitgeteilt.

Stufe 0:

Filter-Policy: Ausfilterung von Broadcasts mit fehlerhaftem allgemeinem Netzbereich, Verhinderung von Broadcasts in das Subnetz, Schutz der Netzkomponenten.

Grundschutz für jedes Netz.

Stufe 0,5:

Filter-Policy: Clients dürfen im wesentlichen alle Ports verwenden, nur im Bereich ankommender Verbindungen sind einige nicht erlaubt. Fernsteuerungs- und andere Serverdienste auch für Clients erlaubt. „Echte“ Server liegen ab .240, alle Ports (außer den an der Uni-Firewall blockierten) sind frei ansprechbar.

Stufe 1:

Filter-Policy: Die Clients dürfen über viele Protokolle direkt ins Internet, insbesondere auch Standard-Protokolle. Serverdienste für Clients (SMB etc.) innerhalb des HD-Net erlaubt. Server liegen ab .240, alle Ports (außer den an der Uni-Firewall blockierten) sind frei ansprechbar.

Vorteile: Direkter Internet-Zugang für Clients für viele Protokolle, Schutz vor Missbrauch durch andere. Versehentlich auf Clients konfigurierte Serverdienste können nicht vom Internet aus missbraucht werden.

Risiken: z.T. direkte Angriffe auf Serverdienste bei Clients und Servern möglich; „ungefilterte“ Mail/Webinhalte etc.

Stufe 1b:

Filter-Policy: Clients dürfen über viele Protokolle direkt ins Internet, die Standard-Protokolle sollten über Proxies (lokal oder URZ) abgedeckt werden. Keine direkten Port-Zugänge von außerhalb der Uni (kein ssh-Serverdienst etc. für Clients). Keine Uni-weiten LAN-Serverdienste für Clients. Server liegen ab .240, bestimmte IP-Adressen lassen nur bestimmte Serverports durch.

Vorteile: weiter direkter Internet-Zugang für Clients mit Spezialanwendungen

Risiken: Direkte Angriffe auf wenige offene Serverdienste; „ungefilterte“ Mail-/Webinhalte für Clients etc.

Stufe 2:

Filter-Policy: Wie Stufe 1, nur dass hier keine Server mehr im Netz sein sollen.

Internet-Server stehen außerhalb des Instituts-Hausnetzes, vor allem wird empfohlen, URZ-Serverdienste zu nutzen.

Um jedoch eventuell benötigte Instituts-eigene Internet-Server aus den Instituts-Hausnetzen entfernen zu können, denkt das URZ daran, sogenanntes „Server-Hosting“ für Instituts-Server in dafür vorgesehenen speziellen Netzen („DMZ“) anzubieten.

Vorteile gegenüber Stufe 1: Ein kompromittierter Internet-Server bedroht nicht das Hausnetz des Institutes. Lokale Server und die User-Passwörter sind damit weniger bedroht.

Risiken: „ungefilterte“ Mail-/Webinhalte etc. auf den Clients, die Serverdienste selbst bleiben dennoch bedroht und müssen gewartet werden.

Stufe 3:

Filter-Policy: „Proxy-Zwang“, d. h. Clients dürfen mit Standard-Dienst-Anfragen (Email, WWW etc.) nur ans URZ bzw. Uni-weite Servernetze, und zu möglichst wenigen definierten nicht-Standard-Servern bzw. -Ports außerhalb. Serverdienste wie bei Stufe 2 außerhalb des LAN. (Zugriff möglichst mit verschlüsselten Protokollen, was aber nicht durchgängig auf Layer 4 erzwungen werden kann.)

Risiken: „ungefilterte“ Inhalte dort, wo die Clients direkt nach außen zugreifen. Um das Risiko der Inhalte besser angehen zu können, sind Dienst-spezifische Proxy-Server und

entsprechende Filterungen auf Viren oder aktive Inhalte nötig. Besonders wichtig wäre dies neben dem Email-Dienst für den WWW-Dienst. Die Serverdienste selbst, siehe oben.

Derzeit sind die folgenden Institute ganz oder zu Teilen durch eine vom URZ administrierte Instituts-Firewall betreut:

- Akademie der Wissenschaften
- Angewandte Mathematik, Statlab
- Historisches Seminar (und Nachbar-Institute am Routerport)
- Institut für ausländisches Privat- und Wirtschaftsrecht, Musikwissenschaftliches Institut, Orientalistik/Semitistik
- Institut für Deutsch als Fremdsprache, Hochschule für jüdische Studien
- Kirchhoff-Institut für Physik
- Physikalisch-Chemisches Institut, Theoretische Chemie
- Physikalisches Institut
- Universitätsbibliothek
- Universitätsrechenzentrum (spezielle Filterungen für einzelne Server)
- weitere in Vorbereitung: Psychologisches Institut, ...

Die Details der Stufen sind für Netzbeauftragte im Web dokumentiert, allgemeine Informationen zur Instituts-Firewall finden sich ebenfalls im Web, zum Teil auch im Anhang abgedruckt.

Die derzeitige Implementierung dieser Sicherheitsstufen erfolgt als Paketfilterliste auf den Routerports, die für die Institute zuständig sind. Die Verwaltung und automatische Dokumentation erfolgt mit eigenen Scripten. Um steigenden Anforderungen an die Qualität solcher Filterstufen gerecht zu werden, ist es sinnvoll, spezielle Routersoftware bzw. Module einzusetzen. Konfiguration und Auswertung kann mit spezieller Software geschehen.

4.1.4. Intrusion Detection

Ein starker Vorteil der vom URZ eingerichteten Instituts-Firewalls ist die zentrale Zusammenführung einheitlicher Log-Meldungen, so dass ungewöhnliche Netzaktivitäten einfacher erkannt werden können.

Aus den Auswertungen von BelWü (Stichproben) sowie aus den Statistiken der Router-Überwachung ergeben sich ebenfalls wertvolle Hinweise auf problematische Rechnersysteme bzw. Netze.

Dies führte zu einem ersten Ansatz eines Intrusion-Detection-Systems. Dieses „Uni-IDS“ wird derzeit mit einer studentischen Hilfskraft betrieben, die vor allem die entsprechenden von eigenen Scripten vorausgewerteten Router-Log-Meldungen beurteilt und entsprechende Emails an die Netz- bzw. Rechnerbetreiber versendet.

Weitere Details hierzu unter

<http://www.urz.uni-heidelberg.de/Netzdienste/firewall/ids/>

Derzeit wird das System mit vergleichsweise geringem Automationsgrad betrieben. Später, bei steigenden Ansprüchen bzw. Anforderungen an die Leistungsfähigkeit des Systems, kann separate Hard- / Software sinnvoll sein.

4.1.5. Weitere

Eine Erhöhung der Sicherheit wird auch durch verbesserte Information und Schulung der „drei Säulen“ erwartet. Es wurde eine „Security-Site“

<http://www.urz.uni-heidelberg.de/Security/>

aufgebaut, auf der gebündelte Informationen und Verknüpfungen zielgruppengerecht für Nutzer, Rechner- und Netzadministratoren bereitgestellt werden.

Es wurden Schulungen der Netzbeauftragten zu Sicherheitsfragen angeboten, die in einigen Instituten auch schon zu Konsequenzen geführt haben.

4.2. Notwendige weitere Maßnahmen

Die bislang umgesetzten Maßnahmen reichen jedoch nicht aus.

Gerade bei der Umsetzung wurde generell festgestellt, wie zeitintensiv sich dieses Arbeitsgebiet darstellt: Neben der ständigen Überwachung und Verbesserung sind immer wieder Beratungsgespräche mit den und Hilfestellungen für die Institutsbeauftragten nötig.

Es ist unwiderrspochen in der Industrie und in öffentlichen Einrichtungen, die eigene Firewalls betreiben, dass für Aufgaben der EDV-Sicherheit eigenes Personal benötigt wird. Nötig – neben dem erforderlichen hohen Zeitaufwand – auch schon von daher, um eine hinreichend hohe Priorisierung von Sicherheitsfragen neben den stets dringenden und drängenden Fragen von Betrieb und Kundenkomfort zu gewährleisten.

Das Erreichen bzw. Erhalten des gewünschten Grades an Sicherheit ist zudem ein kontinuierlicher Prozess, nicht das Ergebnis einer einmaligen Maßnahme oder Investition.

Damit das URZ den Instituten an der Universität besser helfen kann, den erwünschten Sicherheitsstandard im Institut zu definieren, zu erreichen, zu halten, zu verbessern bzw. andererseits im Falle eines Schadens schneller wieder „ans Netz“ zu kommen, ist u. E. notwendig, mindestens drei zusätzliche Mitarbeiter dafür einzustellen:

- Eine Stelle BAT IIa für die Koordination der zentralen und netzseitigen Maßnahmen des Rechenzentrums für die Universität.
- Eine Stelle BAT IIa für die Unterstützung der Institutsrechner vor Ort vom Rechenzentrum aus.
- Eine Stelle BAT IVa/b für technische Durchführung und Pflege der Maßnahmen, sowie die konkrete Ausführung und Auswertung des Normalbetriebes.
- Wissenschaftliche Hilfskräfte zur Unterstützung von Entwicklungen und Routine-Aufgaben.

Stelle 1: Maßnahmen zur zentralen Erhöhung der Sicherheit.

- Fortschreiben des Uni-Sicherheitskonzeptes
- Verfolgung, Bewertung und ggf. Organisation der Umsetzung jeweils aktueller Sicherheitskonzepte
- Paketfilterung, Firewall: Umsetzung der derzeitigen Maßnahmen für viele/alle Institute an der Uni, aktive Beratung der Institute in Sicherheitsfragen, Hilfe beim Erstellen, Einrichten und bei der Umsetzung von Sicherheits-Policies in den Instituten.
- IDS: Umsetzung, Erweiterung, Information betroffener Betreiber
- Verfolgung aktueller Sicherheitsprobleme (allgemein wie auch konkret) im Netz, Information der Zuständigen, Koordination mit lokalen Netzwerk-Zuständigen, sowie mit den CERTs (Computer Emergency Response Team) und NOCs (Network Operating Center) anderer Netze/Domains
- Insbesondere intensive Zusammenarbeit mit der BelWü-Koordination

Stelle 2: Maßnahmen zur Herstellung, Erhaltung und Wiederherstellung der Sicherheit von Endsystemen:

- Sicherheits-Scans, Beratung, Konfigurationshilfen vorab und im Falle der Kompromittierung
- zumindest für die Systeme Windows, Linux, Mac, eventuell auch für Solaris
- Aber ein Sicherheitsspezialist für gleichzeitig ALLE Systeme ist am Markt wohl nicht zu haben, daher wäre ein Windows- oder Linux-Spezialist nicht schlecht, der dann die Koordination mit Anwendungs- und Betriebssystem-Zuständigen am URZ und anderswo übernimmt
- forensische Analyse (Auswertung der Informationen von kompromittierten Rechnern zur Beweissicherung) bei rechtlich relevanten Fällen

Die Kompetenzen dieser Mitarbeiter sollten im Rahmen der Nutzungsordnungen des Rechenzentrums weitreichend sein, um bei erkannten Problemen wirksam schützen und auch präventiv zum Handeln auffordern zu können.

Für Sicherheitsfragen werden Fachleute mit profundem Wissen über Rechner und Rechnernetze benötigt. Dieses Wissen ist von wissenschaftlichen Hilfskräften nicht bzw. erst nach Ablauf des Zeitraumes eines typischen Hiwi-Vertrages und auch nur bei intensiver Schulung zu erwarten. Bei betriebskritischen Abläufen wie Sperrungen kommt es auch auf Präsenz an, die bei Hiwis in der Regel nicht gegeben ist.

Gerade im Sicherheitsbereich ist außerdem persönliche Bekanntheit und Vertrauen bei den Verantwortlichen wichtig, ebenso wie ein kontinuierliches Ansammeln von Kompetenz und Erfahrungswissen.

Es werden also unbefristete Vollzeitstellen für diese Aufgaben benötigt.

Sicherheitsbedrohungen ändern sich ständig, es kommen ständig neue hinzu; neue Entwicklungen überall in der Welt müssen verfolgt werden; Englischkenntnisse und die Bereitschaft zu ständigem und eigenständigem Lernen sind nur die ersten

Grundvoraussetzungen für eine solche Stelle. Eine wissenschaftliche Ausbildung und die Dotierung der Stellen als wissenschaftliche Angestellte ist für solche Mitarbeiter also notwendig.

In der Umsetzung konkreter Maßnahmen sollten diese Stellen durch einen technischen Mitarbeiter unterstützt werden.

Stelle 3: Technische Durchführung und Pflege, Ausführung und Auswertung des Normalbetriebes

- Update/Upgrade-Besorgung, Test, Verteilung für Netzwerk-Sicherheitssoftware, Wartungsarbeiten
- Pflege der notwendigen Systemdateien und -Konfigurationen
- Auswertung von Logdateien im Alltagsbetrieb
- regelmäßige Kontrolle der Firewall-Funktionen
- Unterstützung der beiden anderen Stellen
- Dotierung mit BAT IVa/b. Alternativ kann diese Stelle eventuell auch durch den Einsatz mehrerer studentischer bzw. wissenschaftlicher Hilfskräfte ausgefüllt werden, wobei auch hier die üblichen Probleme auftreten würden, siehe oben.

Sicherheit ist eine Querschnittsaufgabe am URZ für die Institute. Nur hier fallen Log-Dateien in der Zusammenschau an, nur hier ist eine Koordinierung der Vorfälle nach außen und zwischen den Instituten möglich. Zudem ist hier erfahrungsgemäß eine Weiterführung von technischem EDV-Detailwissen beim Wechsel von Stelleninhabern besser gegeben als in den Instituten.

Solche besonderen Stellen für Sicherheitsfragen sind an vielen Universitäten bereits eingerichtet. Die Universität Heidelberg - mit ihrem hohen Anteil an modern ausgerichteten geisteswissenschaftlichen Instituten, wo einerseits zwar der Rechner-Administration wenig Aufmerksamkeit geschenkt wird, andererseits aber ein hoher Anspruch an die Nutzung moderner Informationstechnik besteht - muss hier durch das URZ zentrale Dienstleistungen bereitstellen, um ein zeitgemäßes Niveau an Sicherheit für die Beteiligten erreichen und halten zu können.

5. Ausblick

Mit diesen drei Stellen wäre zwar immer noch keine durchgängige Unterstützung der Institute möglich - wie man dies von einem SIRT (Security Incident Response Team) bzw. CERT (Computer Emergency Response Team) vielleicht am liebsten hätte - schon, weil jeder dieser Spezialisten auch mal Feierabend hat oder Urlaub macht.

Ein Vollservice seitens des URZ ist im Rahmen des Konzeptes der dezentralen Ressourcenverantwortung jedoch auch an vielen anderen Stellen nicht möglich. Dennoch ließe sich das Aufgabengebiet durch wechselseitige Vertretung bzw. thematische Teilvertretungen, auch durch die Fachkollegen im Netzwerk- und Systembereich, so organisieren, dass eine deutliche Verbesserung der gegenwärtigen Lage eintritt.

Mit diesen Stellen könnte das Rechenzentrum auch in dem wichtigen Bereich der EDV-/ Netzwerk-Sicherheit zentrale Dienstleistungen im Rahmen des dezentralen kooperativen EDV-Konzeptes kompetent erbringen.

Anhang

A.1. Security-Hinweise im WWW

siehe <http://www.urz.uni-heidelberg.de/Security/index.shtml>

Im Haupttext zurückgestellt wurden die verschiedenen „Arten möglicher Sicherheit“, die hier aus der entsprechenden Web-Seite kurz aufgeführt seien:

Arten von Sicherheit

Datensicherheit

Maßnahmen, um die eigenen oder übertragene Daten zu schützen vor fremdem Zugriff, Abhören, oder Verfälschung auf dem Transportweg

Datensicherung

Maßnahmen, um Daten bei Verlust an einer Stelle dennoch verfügbar zu haben

Datenschutz

Maßnahmen und Gesetze, um alle Bürger vor Missbrauch durch gespeicherte Daten zu schützen

Rechnersicherheit

Maßnahmen, durch die ein Rechner vor unbefugtem Ge-/Missbrauch (über Netz oder an der Konsole) geschützt werden soll

Rechnersicherung

Maßnahmen, um den Rechner vor physischen Schäden, Verlust und Hardware-Ausfällen zu sichern

Netzwerksicherheit

Maßnahmen, durch die der Datenverkehr und die Rechner vor Angriffen/Missbrauch aus dem/durch das Netzwerk geschützt werden

Authentifizierung

Maßnahmen, durch die sich jemand als der ausweist, als der er bekannt ist

Identifizierung

Zuordnung einer Authentifizierung zu einem Nutzer

Autorisierung

Zuordnung bestimmter Erlaubnisse für den Nutzer

Quittierung

Maßnahmen, durch die eine Aktion bestätigt wird

...

und weitere...

A.2. Sicherheitskonzept zum HD-Net

Im folgenden seien nur URL und Inhaltsverzeichnis der den EDV- und Netzbeauftragten vorgelegten früheren Version dieses Sicherheitskonzeptes angeführt.

Der komplette Text ist – kennwortgeschützt – abrufbar unter https://www.urz.uni-heidelberg.de/Netzdienste/nur_fuer_netzbeauftragte/HD-Net-Sicherheitskonzept-2.1.pdf

Sicherheitskonzept für das Datennetz der Universität Heidelberg (HD-Net)

Teil 1: Netzwerk

Teil 2: Rechner- / Serverbetrieb

Teil 3: Nutzerverhalten

Inhalt

- A Vorwort**
- B Veröffentlichungen**
- C Allgemeine Sicherheitshinweise**
- D Sicherheitskonzept für das HD-Net**
 - D.1 Netzübersicht
 - D.2 Firewalls und Sicherheitskonzepte außerhalb des HD-Net
 - D.3 HD-Net Übersicht
 - D.4 Universitätsfirewall
 - D.5 Institutsfirewall
- E Weitere Sicherheitsverfahren**
 - E.1 Adresstranslation (NAT)
 - E.2 Intrusion Detection
 - E.3 Mail-Firewall
 - E.4 Weitere Maßnahmen
- F Extremfälle**
 - F.1 ZIM (ehemals Kliniknetz)
 - F.2 Zentrale Univerwaltung
 - F.3 SAP
 - F.4 Wohnheime
 - F.5 Landesverwaltungsnetz
- G Formalitäten**
- H Störungen und Probleme**

A.3. Firewall-Dokumentation im WWW

siehe <http://www.urz.uni-heidelberg.de/Netzdienste/firewall/>

A.4. Vorträge in der Fortbildungsveranstaltung für Netzbeauftragte

Im Rahmen der Fortbildung für EDV- und Netzbeauftragte haben bereits mehrere Vorträge zum Thema Netzwerksicherheit und Sicherung von Rechnern, verbunden mit Hinweisen zur Nutzerschulung stattgefunden.

Diese können im Web unter

<http://www.urz.uni-heidelberg.de/Netzdienste/betrieb/#admin>

abgerufen werden.

A.5. BelWü Sicherheitsempfehlungen

siehe <http://www.belwue.de/security/>

insbesondere <http://www.belwue.de/security/sicherheitskonzept.pdf>

A.6. Weitere Referenzen

- RFC 2196, „Site Security Handbook“: <ftp://ftp.isi.edu/in-notes/rfc2196.txt>
- BSI-Grundschutz-Handbuch: <http://www.bsi.de/gshb/deutsch/menue.htm>
- BSI allgemein: <http://www.bsi.de/>
- DFN-Cert: <http://www.cert.dfn.de/>

A.7. Glossar verwendeter Fachbegriffe

Backbone	Das „Rückgrat“ des Datennetzes, ein Netz (oder mehrere Netze), das die Daten zwischen den lokalen Netzen weitergibt und somit die lokalen Netze verbindet
Broadcast	Rundsendung „an alle“; Verfahren, um alle angeschlossenen Geräte in einem LAN anzusprechen
Campus-Bereich	Mit diesem Begriff bezeichnen wir ein Areal aus mehreren Gebäuden, das durch Anbindungen an ein lokales Zentrum leitungstechnisch erschlossen wird
Class-B-Netz	Kennzeichnung des IP-Netzbereiches. Ein Class-B-Netz enthält ca. 65.000 IP-Adressen. An der Universität Heidelberg sind diese aus Verwaltbarkeitsgründen in Subnetze mit je ca. 250 Adressen eingeteilt
CERT	<i>Computer-Emergency-Response-Team</i>
Client	Rechner, der von einem Server Daten abrufen, also dessen Dienste in Anspruch nimmt.
DMZ	De-Militarisierte Zone, bezeichnet hier ein Netz, in dem via Internet erreichbare Server stehen, die deswegen besonderer Pflege und Wartung sowie besonderer Sicherheitsanstrengungen bedürfen.
Ethernet	Paketorientierte Netzwerktechnik, die davon ausgeht, dass alle Teilnehmer ein gemeinsames Medium „als Äther“ verwenden, siehe Kollision; führende Technik im LAN, Übertragungsgeschwindigkeit 10 Mbit/s; zunächst durch Switching-Techniken, dann durch Fast Ethernet auf 100 Mbit/s und Gigabit Ethernet auf 1.000 Mbit/s wurde der mögliche Datendurchsatz kontinuierlich erweitert
FDDI	<i>Fiber Distributed Data Interface</i> ; alte Technologie des HD-Net, Ende der achtziger Jahre die führende sichere und mit 100 Mbit/s schnelle LWL-Datenübertragungstechnik in Ring-Topologie
Firewall	Netzwerkfilter, der Datenpakete bis zur Ebene der Nutzdaten hinauf analysieren und filtern/verändern kann. Eine Maßnahme, bestimmte Aspekte der Rechner- und Netzwerksicherheit zentral bereitzustellen
HD-Net	Bezeichnung des Heidelberger wissenschaftlichen Daten-Backbone, ein MAN
http, https	<i>HyperText Transfer Protocol</i> , Port 80/tcp, <i>http-secure</i> , Port 443/tcp. Das Protokoll, mit dem die Daten der Web-Seiten übertragen werden.
Hub, Konzentrator	einfacher Datensignalverteiler, eingehende Signale werden verstärkt und an alle angeschlossenen Geräte weitergegeben, an alle Ausgänge wird dasselbe Signal ausgegeben, das Netz wird von allen geteilt. Wer in einem solchen „shared network“ einen Rechner dazu bringen kann, den Datenverkehr an der Netzwerkkarte abzuhorchen, der hört allen Datenverkehr im ganzen Netz mit.
Internet	„Netz zwischen Netzen“, Verbindungsnetz; das HD-Net ist ein Internet, wohingegen mit „ <u>das</u> Internet“ das aus allen verbindenden Netzen gebildete Gesamtkonstrukt bezeichnet wird

Internet-Dienste	heute vor allem WWW, Email, aber auch Usenet-Diskussionsforen, zukünftig verteilte Datenbanken, Verzeichnisdienste, Multimedia-Angebote...
Intranet	meist firmeninternes Netz, das besonders gegen das Internet abgeschottet ist und nicht die volle Internet-Funktionalität bietet
IP, IPv4/6	<i>Internet Protocol</i> ; früher vor allem zur Anbindung zwischen LANs entwickelt, ist es heute das auch im LAN führende Protokoll. IPv6 ist die erweiterte Version von IP, wird bislang nur im Probebetrieb eingesetzt
IPSec	<i>IP secure</i> , verschlüsselte Version von IP, im IPv6-Standard enthalten, kann von modernen Komponenten auch unter/neben IPv4 eingesetzt werden
L2, L3, L4	<i>Layer 2/3/4</i> , bezieht sich auf die Schichten des Datentransports gemäß dem OSI-Modell; siehe OSI; ein moderner Switch-Router kann auf allen diesen Ebenen arbeiten
LAN	<i>Local Area Network</i> ; auf einen Nahbereich (z. B. ein Gebäude) beschränktes Netzwerk, z. B. in der Regel ein Institutsnetz
LWL	<i>Lichtwellenleiter</i> , oder auch Glasfaser allgemein; wir unterscheiden Multi-Moden- (oder auch Gradienten-) Fasern (MMF) für kürzere Strecken mit relativ günstigeren Komponenten von den Single-Moden-Fasern (SMF) für längere Strecken, mit relativ teureren Komponenten
MAN	<i>Metropolitan Area Network</i> ; Netzwerk, das z. B. über eine Stadtfläche verteilt ist, und das viele LANs direkt anbindet
Multimedia	um Multimedia-Daten (Sprache, Bild...) z. B. ohne allzugroße zeitliche Verzerrungen (siehe QoS) oder mit definierten (z. T. hohen) Bandbreiten übertragen zu können, wurden verschiedene Protokolle entwickelt, z. B. für Ressourcen-Reservierung, Multicasting-Verfahren für live-Sendungen, Streaming-Protokolle für „on-demand“-Abrufe
Netzwerk-Management	alle Tätigkeiten, die die Verwaltung, Überwachung und Instandhaltung der aktiven Komponenten (Router, Switches, Hubs) und der damit betriebenen Datennetze betreffen.
OSI	<i>Open Systems Interconnection</i> , nur noch theoretisch genutztes Standardmodell der Datenübertragung, teilt den Übertragungsvorgang von der Anwendung (Layer 7) bis zum Kabel (Layer 1) in Schichten/Ebenen/Layer ein
Paketfilter	Netzwerkfilter, der bis zur Ebene der Transportdaten (Layer 4) analysieren und filtern kann; vergleiche Firewall
Peer-to-peer	Über das Internet hergestellter Anwendungsverbund, in dem jeder Rechner Client wie Server ist. Unter Verzicht auf zentrale Serverstrukturen wird ein dezentraler Datenaustausch zwischen den Nutzern betrieben.
Router	Datensignalverteiler zur Verbindung zwischen Subnetzen; muss die (z. B. TCP/IP- und IPX-) Adressfelder der Datenpakete („Layer 3“) sehr schnell lesen und auswerten können, trifft die Entscheidung, welche „Route“ ein Datenpaket nimmt; typischerweise die teuerste Komponente im Netz; ein Routerport definiert im HD-Net typischerweise ein Institutsnetz

Server	Rechner, der für andere Rechner über Netzwerk erreichbare Dienste bereitstellt.
ssh	<i>Secure Shell</i> . Anwendungsprogramm bzw. Serverdienst, das/der verschlüsseltes Arbeiten über das Datennetz ermöglicht, und dabei auch die „Identität“ des Servers überprüfen kann. Insbesondere sind hiermit auch - im Gegensatz zu telnet oder ftp - die Passwörter verschlüsselt, und werden - bei richtiger Handhabung - nur an den erwünschten Zielrechner vermittelt.
SIRT	<i>Security-Incident Response-Team</i>
smtp	<i>Simple Mail Transport Protocol</i> , Port 25.
<i>social engineering</i>	Informationsbeschaffung über ein Angriffsziel durch Ausfragen von Nutzern
<i>Spam-Mail</i>	Unerwünschte Werbemails, die in großen Mengen versendet werden
strukturierte Verkabelung	Verkabelungs-Norm, die, grob gesprochen, eine einheitliche Verkabelungsstruktur gemäß der Aufteilung in die drei Bereiche Campus/Backbone (LWL), Gebäudeverteilung/Steigbereich (LWL) und Stockwerksverteilung/Endanbindung (TP-Kupferkabel) vorschreibt. Eine solche Struktur ist auch unter Sicherheitsaspekten sinnvoll, zum Beispiel für die Betriebssicherheit.
Switch	Datensignal-Verteiler für ein Subnetz (oder mehrere, bei VLAN-fähigen Geräten), schaltet direkt auf „Layer 2“ zwischen den beteiligten Anschlüssen durch, dadurch ist im „switched network“ weniger Möglichkeit, den Datenverkehr abzuhören. Durch entsprechende Konfiguration kann hier viel erreicht werden. „Broadcastdomäne“; vergleiche Hub, Router, Kollision
TCP/IP	<i>Transport Control Protocol / Internet Protocol</i> , die Standard-Regeln, um Daten mittels Datenpaketen zwischen Netzwerken transportieren zu können; der Standard zunächst im Internet, heute auch im LAN
Topologie	bezeichnet in diesem Zusammenhang die Art der Verbindung der Netzknoten in der grösseren Struktur, man unterscheidet hier Ring-, Stern-, Bustopologie
TP-Kabel	(UTP: <i>unshielded</i> , STP: <i>shielded</i>) <i>twisted pair</i> : Paarweise verdrehte abgeschirmte Kabel, kupferbasierte Kabeltechnik, 4 Paare werden in einem Kabel verlegt. Abhörmöglichkeit bei STP geringer.
Unicast	Sendung „an einen“; direktes Ansprechen des Empfängers durch seine spezifische Adresse
URZ	<i>Universitätsrechenzentrum</i> ☺
USV/UPS	Unabhängige Strom-Versorgung / <i>Uninterruptible Power-Supply</i> : Netzteil mit Batterie, das die Stromversorgung bei einem Stromnetz-Ausfall aufrecht erhält, Element zur Erhöhung der Betriebssicherheit.
VLAN	Virtuelles LAN; Zusammenschaltung räumlich getrennter Bereiche zu einer einem lokalen Netz (LAN) vergleichbaren Einheit; meist wird die Norm IEEE 802.1Q gemeint/erfüllt
VLAN-trunk	bezeichnet die Möglichkeit, die Signale mehrerer VLANs über eine gemeinsame Leitung zu geben, die dann zur Endverteilung entsprechenden Ausgängen zugeordnet werden; dies wird mittels Markierungen („tags“) der Datenpakete erreicht (VLAN-tagging)

VoIP	<i>Voice over IP</i> , von manchen Herstellern bereits verwirklichtes Konzept, Telefonie über Datenleitungen direkt zu betreiben. Um hier Störungen und Abhören bestmöglich auszuschließen, sind detaillierte Konfigurationen der beteiligten Netzkomponenten nötig.
VPN	<i>Virtuelles Privates Netzwerk</i> , im Gegensatz zum VLAN wird hier mehr Wert auf Sicherheit/Nichtabhörbarkeit gelegt. Kann z. B. mit IPSec umgesetzt werden.
WAN	<i>Wide Area Network</i> ; Weitverkehrsnetz über große Strecken, z. B. zwischen Städten oder Universitäten
<i>wireless LAN</i>	Drahtlose Netzwerktechnologie mit Reichweite 30-100 Metern. Alle <i>wireless</i> -Techniken können im Prinzip leichter abgehört werden als kabelgebundene Verfahren, daher muss hier Wert auf Verschlüsselung gelegt werden.
WWW	<i>world-wide web</i> . Bezeichnet zunächst via http erreichbare Serverdienste, in denen vielfältige Informationsformate bereitgehalten und mittels Web-Browser abgerufen werden können. Für die einfache Vernetzung (<i>web</i>) sorgen dabei Verknüpfungselemente (<i>links</i>) und ein entsprechendes Adressformat (URL, Uniform Resource Locator). Für viele bedeutet die Nutzung von WWW-Diensten schlichtweg „das Internet.“