Baden-**W**ürttembergs **e**xtended **l**an

BelWü

BelWü-AG Security

BelWü Sicherheitskonzept und Maßnahmenkatalog

V 1.0 vom 14.08.2001

Inhaltsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Der Zweck dieses Papiers ist die Erhöhung der Sicherheit im BelWü mit Hilfe von Accesslisten und/oder Firewalls im BelWü Backbone, den BelWü-Zugangsroutern sowie den RZ-Zugangsroutern bzw. RZ-Firewalls. Eine wesentliche Voraussetzung war der Bewusstseinswandel der Hochschulen hinsichtlich des Bedarfs an Sicherheit mit den damit verbundenen Diensteinschränkungen.

Dieses Papier wird ständig fortgeschrieben, da es von den technischen und organisatorischen Möglichkeiten abhängt, die zum aktuellen Zeitpunkt verfügbar sind. Die jeweils aktuelle Version ist verfügbar unter
http://www.BelWue.DE/aktivitaeten/security/sicherheitskonzept.

Das Papier wurde verfasst von Mitgliedern der BelWü-AG Security (siehe Kapitel F) mit Peter Merdian als Editor. Wenn sich die Mitglieder bei der Bewertung von einzelnen Punkten nicht einig waren, wurde dies entsprechend vermerkt (z.B.: "Diese Maßnahme ist jedoch umstritten").

Falls eine Hochschule noch keine Sicherheitsrichtlinie (Policy) für ihren Internetzugang definiert hat, kann dieses Papier hierfür eine Grundlage darstellen. Weitere Hinweise hierfür sind in Kapitel E ab Seite 55.

Kapitel 2

Zusammenfassung

Im vorliegenden Papier werden aufgrund einer am BSI orientierten Risikoanalyse Maßnahmen identifiziert, die in einer von fünf Sicherheitsstufen umgesetzt werden können.

Die beschriebenen Maßnahmen erfolgen sowohl auf zentralen BelWü-Routern (durch die BelWü-Koordination) als auch auf Hochschulroutern/firewalls (durch die einzelnen Einrichtungen). Bei Durchführung der beschriebenen Maßnahmen in einer hohen Sicherheitsstufe ist mit einer Einschränkung der bisher eher freizügigen Internetnutzung an den Hochschulen zu rechnen. Ein Restrisiko bleibt trotzdem bestehen. Dieses wird allerdings entsprechend den jeweiligen Anforderungen der Einrichtung, durch die jeweils empfohlenen Maßnahmen soweit vermindert, dass die Wahrscheinlichkeit für das Eintreten eines großen Schadens nur noch als gering eingeschätzt wird.

In einem folgenden Phasenkonzept und technischen/organisatorischen Regelungen wird die Umsetzung der Maßnahmen beschrieben. In den verschiedenen Tabellen und insbesondere in den Anhängen werden konkrete Konfigurationshinweise gegeben. Der überwiegende Teil der Maßnahmen muss von den jeweiligen Einrichtungen selbst umgesetzt werden. Damit tragen die Einrichtungen selbst einen großen Teil der Verantwortung für ihre eigene Sicherheit. Die Maßnahmen die an zentraler Stelle möglich sind (Maßnahmen der BelWü-Koordination) können aufgrund der unterschiedlichen Anforderungen nur einen begrenzten präventiven Schutz bieten, sie unterstützen allerdings die Eingrenzung und Identifizierung der Ursachen und die Einleitung entsprechender Gegenmaßnahmen.

Das Papier deckt somit drei Aspekte ab:
- Konzeption eines sicheren BelWü- bzw. Hochschulnetzes;
- Risikoanalyse/Maßnahmen/Sicherheitsstufen;
- konkrete Konfiguration von Routern und Servern.

Kapitel 3

Sicherheitskonzept

Die folgende Risikobewertung orientiert sich an den Handbüchern des BSI (IT-Grundschutzhandbuch, IT-Sicherheitshandbuch).

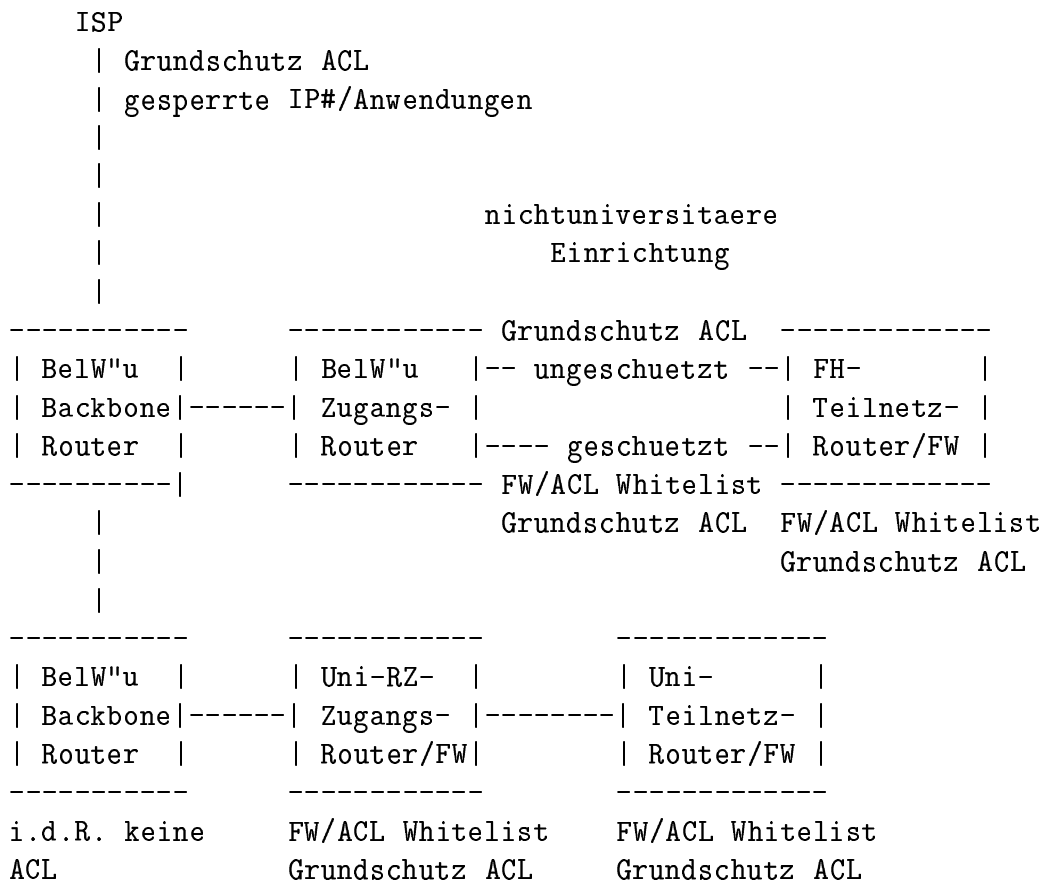
Dieses Sicherheitskonzept wird ständig weiterentwickelt. Hinsichtlich des Grundschutzes (Sperrung von bestimmten Ports auf den ISP-Interfaces, siehe Tabelle 3.1 auf Seite 30) können weitere zu sperrende Ports auf Vorschlag des BelWü-AK1 und der Zustimmung des Universitätsrechenzentrumsleiterkreises (Achern) hinzugenommen werden.

3.1 IST-Aufnahme

Derzeit erfolgt die Kommunikation zwischen BelWü-Teilnehmern und dem Internet in allen Schutzausprägungen: von einer sehr restriktiven Firewall über eine ACL-Whitelist oder eine ACL-Blacklist bis hin zu keinem Schutz. I.d.R. besteht meistens ein Grundschutz (vor allem gegen IP Spoofing); bei den Universitäten besteht i.d.R. eine ACL (heute eher als Whitelist, in der Vergangenheit eher als Blacklist). Die nicht-universitären Einrichtungen haben i.d.R. kein Personal für einen umfassenden Schutz.

Als Netzwerkprotokoll wird z.Zt. nur IP zugelassen. Das BelWü ist an verschiedenen Stellen mit ISPs (Internet Service Providern) verbunden, welche die Verbindungen zum Rest des Internets darstellen. An jeder Hochschule steht ein zentraler Router, der den Verkehr zwischen BelWü-Netz und Hochschule regelt. Dieser wird vom zentralen Netzwerkmanagement des BelWü betreut. Die Router befinden sich in einem gesicherten Raum des Rechenzentrums der jeweiligen Hochschule. Der Zugang auf den Router ist mit Access-Listen und Passwörtern geschützt. Zugriffsberechtigung hat das IP-Management der BelWü-Koordination sowie die jeweilige Einrichtung.

Der Schutz erfolgt gemäß folgender Zeichnung in unterschiedlichem Umfang an unterschiedlichen Routern (Schalenprinzip). Hierdurch kann der Schutz mehrfach erfolgen und je nach Notwendigkeit eher allgemein oder sehr spezifisch sein. Größere Einrichtungen haben i.d.R. ein abgestuftes Konzept in Form von dezentralen Sicherheitsmaßnahmen. In den BelWü-Backbone Routern werden aus Gründen der Netzperformance ("QoS") i.d.R. mit Ausnahme der ISP Interfaces keine ACLs konfiguriert.



3.2 Risikobewertung

3.2.1 Bedrohungsanalyse

Das Internet hat sich von seiner anfänglichen Bedeutung als Kommunikationsnetz für wissenschaftliche Einrichtungen zu einem kommerziell/privat geprägten Kommunikationsnetz gewandelt. Während dieser Öffnung für den privaten Sektor haben sich Zugangsmodelle (primär von Firmen) mit Hilfe von sehr restriktiven Firewalls und privatem Adressraum durchgesetzt. Diese Zugangsmodelle stehen im krassen Gegensatz zu der weitgehend offenen und ungeschützten Anbindung der wissenschaftlichen Einrichtungen an das Internet. Die Hochschulen sehen sich (wie andere Internetteilnehmer auch) inzwischen ständigen Angriffen aus dem Internet ausgesetzt:

- DoS-Attacken (Denial of Service) als Ziel,
- Distributed DoS-Attacken (DDoS) als Ziel oder als Zwischenträger,
- Einbrüche in Hochschulrechner und damit verbundener Missbrauch: Plattform für weitere Angriffe, Umschlagplatz für nicht-bestimmungsgemäße bzw. illegale Inhalte (Raubkopien/Warez, radikale Inhalte, Pornographie, etc.).

Diese Angriffe können aufgrund der an manchen Stellen praktizierten volumenbasierten Kostenabrechnung nicht unerhebliche finanzielle Auswirkungen und im Falle des Missbrauchs rufschädigende oder sogar rechtliche Folgen für den Betreiber der angegriffenen Infrastruktur haben. Ein mögliches Szenario wäre z.B. der Missbrauch kompromittierter Infrastruktur als Verteilungsplattform für kinderpornographisches Material, was ein Ermittlungsverfahren zunächst gegen den Betreiber auslösen kann. In der Folge fällt die Last seine Unschuld zu beweisen auf den Betreiber, was im Falle eines professionell vorgetragenen Angriffs äußerst schwierig bis unmöglich sein kann. Auch bei simplen Diebstahl von Daten (z.B. Forschungsergebnisse) können für den Infrastrukturbetreiber rufschädigende und/oder rechtliche Folgen entstehen.

Vor diesem Hintergrund soll künftig das BelWü mindestens einen gewissen Grundschutz vor Angriffen aus dem Internet bieten. Zusätzlich soll, soweit möglich, das Internet geschützt werden vor Angriffen, die von Rechnern von BelWü-Teilnehmern ausgehen.

3.2.2 Ermittlung des Schutzbedarfs

Als Schutzziele werden definiert: der Schutz der sicherheitsrelevanten Daten und Anwendungen vor Bedrohungen von außen; der Schutz der Internetteilnehmer außerhalb des BelWü vor Angriffen von BelWü-Teilnehmern; sowie die Vermeidung von unnötiger bzw. übermäßiger Belastung der Internetverbindungen, z.B. durch Spieleserver

oder DDoS-Attacken (letzteres insbesondere aufgrund der Volumentarifierung von den Internet Service Providern Verbindungen).

Der Schutzbedarf hängt von den Anwendungen ab. Ein hoher Schutzbedarf wird z.B. für LVN-Verbindungen, bedeutsame Forschungsergebnisse oder Verwaltungen angenommen. Dieser Schutzbedarf muss durch zusätzliche Schutzvorrichtungen (z.B. zusätzliche äußerst restriktive Firewalls und Verschlüsselung) erfolgen.

3.2.3 Risikoanalyse

Die folgende Risikoanalyse ist nicht vollständig. Sie erfolgt unter dem Blickwinkel des Rechnernetzwerkes. Die Risiken wurden sortiert nach den Bereichen Anwendungen, Systeme/Server, Netzwerk und Sonstiges.

Bei der Einstufung der "Risikobewertung hinsichtlich des Schadens" können immer Fälle konstruiert werden, wo der Schaden sehr hoch ist (z.B. Prüfungsdaten). Im folgenden wird bei der Einstufung aber von einem "durchschnittlichen" Schaden in einer Hochschulumgebung ausgegangen.

3.2.3.1 Anwendungen

Siehe zu den Risiken der Endanwendungen Mail, FTP, WWW (incl. Active-X, Java und Cookies) auch [19], [36] und [37].

3.2.3.1.1 Klartextpasswörter bei Telnet und FTP Das Risiko der Übermittlung von Passwörtern im Klartext bei Telnet und FTP ergibt sich dadurch, dass gemeinsam genutzte Medien wie Ethernet das Abhören durch Dritte ermöglichen. Mit diesen Passwörtern kann dann problemlos in die betreffenden Rechner eingebrochen werden und dort durch oft vorhandene lokale Sicherheitslöcher Root-Rechte erlangt werden. Siehe auch Paragraph 3.2.3.3.5 Ungeschützte Netzwerkverbindungen.
Maßnahmen: Nummer 1, 2, 3, 4, 72.
Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.1.2 Klartextpasswörter bei POP und IMAP Das Risiko der Übermittlung von Passwörtern im Klartext bei POP und IMAP ist geringer als bei Telnet und FTP, da hierdurch "nur" die Mailbox kompromittiert wird. Das Risiko wird allerdings dadurch erhöht, dass teilweise für login und Mailbox dasselbe Passwort verwendet wird. Siehe auch Paragraph 3.2.3.3.5 Ungeschützte Netzwerkverbindungen.
Maßnahmen: Nummer 5, 72.

Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.3 Mailverschlüsselung Das Risiko von unverschlüsselten Mailinhalten ergibt sich dadurch, dass die Mail auf den durchlaufenden Mailrelays von dortigen Verwaltern unbefugt eingesehen und verändert werden kann, sowie auf dem System des Endnutzers ebenfalls für Unbefugte einsehbar sein kann. Die vorgeschlagene Maßnahme (PGP) hilft zudem hinsichtlich der sicheren Authentifizierung des Mailabsenders.
Maßnahmen: Nummer 6, 72.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.4 Spam-Mail und Mailrelaying Das Risiko von Spam-Mail und Mailrelaying ergibt sich zum einen durch die Verbreitung der eigenen Mailadressen über öffentliche Medien wie News oder Web; zum anderen werden ungeschützte Mailhosts und/oder Webserver von Hochschulen von unbefugten Dritten zum Versenden von Spam-Mail verwendet. Im Missbrauchsfall führt Spam-Mail zu einer Belästigung der Endnutzer bzw. zur unbefugten Nutzung von Serverressourcen.
Maßnahmen: Nummer 8, 9, 10, 11.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.5 Mail-Attachment Das Risiko von Mail-Attachments, die z.B. in der Standardkonfiguration vom MS Outlook automatisch geöffnet und ausgeführt werden, ist nicht unerheblich: Attachments können ausführbaren, bösartigen Code enthalten. Durch das OLE-Konzept von Microsoft Betriebssystemen kann dieser Code beim Öffnen des Attachments ausgeführt werden und das betroffene System kompromittieren. Nach diesem Prinzip arbeiten die meisten derzeit in Umlauf befindlichen Viren, Würmer und trojanischen Pferde. Zu den unmittelbaren Folgen der Kompromittierung des betroffenen Systems kommen häufig die nicht unerheblichen mittelbaren Folgen, die durch die Weiterverbreitungsfunktion, v.a. in Internetwürmern, verursacht werden. Erhebliche Belastung, mitunter sogar Überlastung der Mail-Infrastruktur (siehe hierzu die Folgen des "I LOVE YOU"-Wurmes, der ganze Firmennetzwerke lahmlegte) können die Folge sein.
Maßnahmen: Nummer 7, 72.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.6 Viren Das Risiko von Virenbefall ist in einer Microsoft basierenden Umgebung (im Gegensatz zu einer UNIX Umgebung) deutlich höher. Der Viren-

schutz soll auf dem Endsystem erfolgen, da es verschiedene Infizierungswege (Mail, Web, FTP, Diskette, verschlüsselter Zugang) gibt sowie zentrale Virenschutzserver Durchsatzprobleme haben. Für kleinere Einrichtungen kann ein zentraler Virenschutz auf dem Mailhost sowie dem Web-Proxy hilfreich sein. Siehe auch Paragraph 3.2.3.1.5 Mail-Attachment.
Maßnahmen: Nummer 12 und 13.
Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.7 Active-X, JavaScript Das Risiko von Active-X, JavaScript und Ähnlichem ("Active Scripting") ergibt sich aus der inhärenten fehlenden Sicherheit sowie aus der Vielzahl von Webseiten, die das Aktivieren z.B. von JavaScript erfordern. Im Schadensfall kann der Rechner z.B. mit einem trojanischen Pferd (beispielsweise back orifice) infiziert und damit kompromittiert werden. Größer noch ist bei aktiven Inhalten die Gefahr der Ausspähung des angegriffenen Rechners durch bösartigen Scriptcode und die Erlangung wichtiger Daten. Bevorzugtes und leichtes Ziel sind in einem solchen Fall Authentifizierungsdaten, die Zugang zum angegriffenen sowie eventuell weiteren Rechnern erlauben. Dieses Risiko stellt eine Besonderheit dar, da der Angreifer selbst nicht aktiv zu werden braucht. Active-X stellt aufgrund seiner Integration in das Microsoft Betriebssystem eine größere Gefahr dar als JavaScript. Siehe auch Paragraph 3.2.3.1.5 Mail-Attachment sowie [36] und [37].
Maßnahmen: Nummer 15, 72.
Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.1.8 Java Das Risiko von Java ist im Vergleich zu Active-X aufgrund der eingebauten Sicherheit geringer. Prinzipiell sind ähnliche Angriffe, wie bei JavaScript möglich aber i.A. nur bei fehlerhafter Implementierung der JVM (Java Virtual Machine) ausführbar. Fehler in deren Implementierung treten allerdings nicht selten auf. Siehe auch Paragraph 3.2.3.1.5 Mail-Attachment sowie [38], [36] und [37].
Maßnahmen: Nummer 15, 72.
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.1.9 Nicht-jugendfreie Web-Inhalte Das Risiko von nicht-jugendfreien Web-Inhalten besteht im Zugang zu pornographischen, rassistischen oder gewaltverherrlichenden Inhalten und betrifft im Hochschulbereich vor allem die Bibliotheken, ansonsten insbesondere die Schulen.
Maßnahmen: Nummer 14.
Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: gering.

3.2.3.1.10 Squid Proxy und Socks Das Risiko von Squid Proxy und Socks Server, die von außen erreichbar sind, besteht in der Tunnelung einer möglicherweise vorhandenen Firewall. Bei entsprechender Konfiguration können beliebige TCP-Verbindungen weiterleitet werden. Durch die Nutzung von Squid Proxy und Socks Server von außen können unbefugt Ressourcen der Einrichtungen in Anspruch genommen werden und Aussenstehende unbefugt mit der IP-Adresse der betreffenden Einrichtung auftreten.
Maßnahmen: Nummer 16.
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.11 News Das Risiko des Newsdienstes besteht in der Verbreitung von Beiträgen pornographischer, rassistischer oder gewaltverherrlichender Art und der damit verbundenen Rufschädigung bzw. möglichen rechtlichen Problemen. Außerdem entsteht ein nicht unerhebliches Verkehrsaufkommen, wenn Newsgruppen mehrfach parallel von außen in das BelWü übertragen werden.
Maßnahmen: Nummer 17, 18.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.12 SNMP Das Risiko der Ausforschung eines Netzwerkes durch SNMP ergibt sich dadurch, dass der Community String (d.h. das SNMP-Passwort) nur bei der noch nicht verbreiteten, neuen Version 3 verschlüsselt werden kann. Per SNMP kann ein Gerät (z.B. Router) überlastet werden, rebootet werden, oder im Extremfall auch umkonfiguriert werden.
Maßnahmen: Nummer 19, 20.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.1.13 Portmapper Das Risiko von Portmapper liegt im vereinfachten Ausspähen von internen RPC-Services (z.B. NFS).
Maßnahmen: Nummer 21.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: gering.

3.2.3.1.14 X11 Das Risiko von X11 ist die nicht standardmäßig aktivierte Authentisierung, die den unbefugten Zugriff von außen auf lokale X11 Ressourcen (z.B. Tastatureingaben, Bildschirm) ermöglicht.
Maßnahmen: Nummer 22.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.1.15 UUCP Das Risiko von UUCP besteht in dem möglichen Remote-Login und der interaktiven Nutzung von entfernten Rechnern. Hinsichtlich der Übertragung von UUCP-Passwörtern im Klartext gelten dieselben Probleme wie bei POP und IMAP.
Maßnahmen: Nummer 23.
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: gering.

3.2.3.1.16 R-Kommandos Das Risiko von R-Kommandos (rsh, rcp, remsh, rcmd und rlogin) liegt in dem möglichen Zugang ohne Passwort und den damit verbundenen Sicherheits(Authentisierungs)mängeln.
Maßnahmen: Nummer 24.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.1.17 NFS Das Risiko von NFS liegt in Sicherheitslücken im Design, der Implementation oder Konfiguration und den damit verbundenen Angriffen.
Maßnahmen: Nummer 25.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.1.18 lockd Das Risiko von lockd liegt in weit verbreiteten Sicherheitslöchern und wird im Zusammenhang mit NFS verwendet.
Maßnahmen: Nummer 26.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.19 syslogd Das Risiko von syslogd liegt in der fehlenden Authentifizierung, d.h. der Möglichkeit, Logfiles unbefugt von außen zu beschreiben.
Maßnahmen: Nummer 27.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.20 bootp Das Risiko von bootp liegt in der fehlenden Authentifizierung. Zudem ist bootp im Wesentlichen ein nicht geroutetes LAN-Protokoll.
Maßnahmen: Nummer 28.
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: gering.

3.2.3.1.21 lpd Das Risiko von lpd liegt in der fehlerhaften Implementierung und damit verbundenen Sicherheitslöchern. lpd ist ein Dienst, der nur im LAN und nicht von außerhalb benötigt wird.
Maßnahmen: Nummer 29.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.22 ntpd Das Risiko von ntpd liegt in der fehlerhaften Implementierung und damit verbundenen Sicherheitslöchern. ntpd ist ein Dienst, der überwiegend im LAN und nicht von außerhalb benötigt wird.
Maßnahmen: Nummer 30.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.23 TFTP Das Risiko von TFTP liegt in der fehlenden Authentifizierung, d.h. der Möglichkeit, Dateien unbefugt von außen zu lesen und beschreiben. Zudem ist TFTP ein UDP-basierender Dienst, der Ports > 1023 benutzt, d.h. mit einfachen ACLs schlecht zu kontrollieren.
Maßnahmen: Nummer 31.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.24 NeTBIOS/SMB Das Risiko von NeTBIOS/SMB liegt in Sicherheitslücken im Design, der Implementation oder Konfiguration und den damit verbundenen Angriffen.
Maßnahmen: Nummer 32.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.1.25 DNS Das Risiko von DNS besteht in der Fälschung von DNS-Daten (DNS cache contamination), Ausspähung von internen Daten (HINFO, ev. Zonentransfer), sowie in der Kompromittierung des DNS-Servers durch Ausnutzung von Schwächen in der Software.
Maßnahmen: Nummer 33, 34 sowie Maßnahmen des Paragraphen 3.2.3.2.1.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.1.26 Multicast/Multimedia Das Risiko von Multicast/Multimedia besteht in der schlechten Unterstützung durch Firewalls mit der Folge von zu großen Löchern in den Firewalls.

Maßnahmen: Nummer 35.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.2 Systeme/Server

3.2.3.2.1 Ungepflegte Systeme/Anwendungen Das Risiko von ungepflegten Systemen/Anwendungen ergibt sich durch die zunehmenden Angriffsmöglichkeiten aufgrund von Softwaremängel (z.B. bugs im BIND, WU-FTP, mountd, sadmind, sendmail, imapd, qpopper, rpc.statd, rpc.ttdbserverd, rpc.cmsd, IIS oder CGI-Skripten). Ein bekanntes Beispiel hierfür ist der Code Red Wurm. Ein bereits kompromittierter Rechner kann trotz einer moderat restriktiven Firewall (Durchlässigkeit für ICMP, SSH, ident, SAFT) sehr einfach von außen gesteuert werden, indem z.B. über ICMP ein Tunnel aufgebaut oder ein freigeschalteter Port für das "Fernsteuerprotokoll" zweckentfremdet wird.
Maßnahmen: Nummer 57, 58, 59, 60, 61, 62, 72. Weitere Maßnahmen stehen im Anhang C (Betriebshinweise für Server) auf Seite 47.
Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.2.2 Personal Firewall Das Risiko von ungepflegten Arbeitsplatzrechnern ergibt sich ähnlich wie bei den Servern, indem laufend Sicherheitslöcher im Betriebssystem bekannt werden und nicht oder zu spät beseitigt werden. Wenn Arbeitsplatzrechner (wie in der Regel) nicht zentral gewartet werden, werden diese Sicherheitslöcher oftmals nicht beseitigt. Wenn auf dem Arbeitsplatzrechner eingebrochen wurde und ein Trojanisches Pferd installiert wurde, wird dies oftmals nicht bemerkt.
Maßnahmen: Nummer 63.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.2.3 Quellcode Das Risiko von Software, die nicht im Quellcode vorliegt ergibt sich aus absichtlich oder unabsichtlich eingebauten Sicherheitslöchern sowie aus der normalerweise längeren Zeit, entdeckte Sicherheitslöcher zu beseitigen.
Maßnahmen: Nummer 59, 64, 72.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.2.4 Unnötige Dienste Das Risiko von nicht benötigten Diensten (z.B. finger) besteht darin, dass eventuelle Sicherheitsmängel in diesen Diensten für weitergehende Angriffe ausgenutzt werden können.
Maßnahmen: Nummer 65.

Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.2.5 Passwörter Das Risiko von schwachen und/oder gemeinsamen Passwörtern besteht darin, dass ein Angreifer durch bloßes Probieren Zugang zu einem System erlangen kann. Zudem können passwd-Dateien unter UNIX bei schwachen Passwörtern ermittelt werden. Bei gemeinsamen Passwörtern besteht die Gefahr, dass diese zulange beibehalten werden und bei Einbrüchen die Quelle schlecht verfolgbar ist. Siehe hierzu auch [42].
Maßnahmen: Nummer 66, 67, 72.
Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.3 Netzwerk

3.2.3.3.1 DDoS Das Risiko von (D)DoS Attacken ergibt sich dadurch, dass die Hochschulen breitbandig angebunden sind und eine Vielzahl von schlecht gewarteten Rechner beherbergen, d.h. ein ideales Sprungbrett von DDoS Attacken auf andere Einrichtungen darstellen. Hochschulrechner selbst bilden ein Ziel von DoS Attacken insbesondere im Umfeld vom IRC. Der Grundschutz erfolgt i.d.R. auf den BelWü-Routern (ISP-Interfaces und nicht-universitäre BelWü-Zugangsroutern) sowie dem universitären Eingangsrouter bzw. Firewall. Siehe hierzu auch [43], [44].
Maßnahmen: Nummer 36, 37, 38, 39, 40, 41.
Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.3.2 ICMP Das Risiko von ICMP liegt in Denial-of-Service Angriffen sowie im Ausspähen des Netzes.
Maßnahmen: Nummer 42.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.3.3 Routingprotokolle Das Risiko der Kompromittierung von Routingprotokollen (falsche Routingtabelle) ist gering, da dies einen Angreifer im Kernnetz voraussetzt.
Maßnahmen: Nummer 43, 44.
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.3.4 Netzwerkmanagement Das Risiko der Störung des Netzwerkmanagements (z.B. durch Kompromittierung des syslogd, snmp oder Überlastung von zentralen Routern) besteht in Störung des Netzwerkdienstes.
Maßnahmen: siehe syslogd, SNMP.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.3.5 Ungeschützte Netzwerkverbindungen Das Risiko der ungeschützten Netzwerkverbindungen über gemeinsam genutzte Medien wie Ethernet oder Funk ergibt sich durch die einfache Möglichkeit von Externen, den Verkehr abzuhören. Dadurch können Klartextpasswörter, Kommunikationsinhalte (z.B. Mail) aber auch Verkehrsbeziehungen in unbefugte Hände gelangen. Bei Funkzellen können sich ggf. Unbefugte einbuchen (siehe hierzu z.B. [47]). Maßnahmen: Nummer 45, 46, 47, 48.
Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.3.6 VLAN Das Risiko von VLAN besteht in einem Sicherheitsloch in bestimmten Switches, das das Abhören des Verkehrs von anderen VLANs erlaubt.
Maßnahmen: Nummer 49.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.3.7 Tunnel Das Risiko der Kompromittierung des Firewallschutzes durch Tunnel (GRE, IPSec, IPv6, SSH, SSL, PPTP, L2TP) ergibt sich aus der Vielzahl solcher Tunnel sowie aus der Vertrauenswürdigkeit der jeweiligen Tunnelenden. Grundsätzlich ist jedes Loch in einer Firewall riskant und möglichst zu vermeiden. Es wird jedoch erwartet, dass die Verwendung von Tunnelprotokollen als Mittel für verschlüsselte Datenkommunikation zunehmen wird.
Maßnahmen: Nummer 52, 53, 72.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.3.8 Direktverbindungen zwischen Rechnern (z.B. über SDH, ATM) Das Risiko von SDH, ATM, Großrechnerkoppelungen, QoS-Interfaces besteht in der Kompromittierung des Firewallschutzes. Dies steht im Gegensatz zur Anforderung an qualitativ hochwertige Netzwerkverbindungen.
Maßnahmen: Nummer 53, 54, 55.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.3.9 Verschlüsselte Datenverbindung Das Risiko von verschlüsselten Datenverbindungen besteht darin, dass diese für unkontrollierbare Tunnel durch die Firewall verwendet werden können.
Maßnahmen: 72.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.3.10 Einwahl Das Risiko der Kompromittierung des Firewallschutzes durch unbefugte Einwahlmöglichkeiten innerhalb des geschützten Netzes ergibt sich durch die Vielzahl der Netzanwender sowie aus dem dezentralen Charakter einer Hochschule und ist durch organisatorische Maßnahmen nur schwer in den Griff zu bekommen.
Maßnahmen: Nummer 53, 56, 72.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.3.11 Zugang von zu hause per DSL, Modem o.ä. Das Risiko des Zugang von zu hause per DSL o.ä. besteht darin, dass der Rechner zu hause kompromittiert ist und ein Hacker über den Zwischenschritt Heimrechner eines unbescholtenen Hochschulangehörigen Zugang in das Hochschulnetz erhält. Ein weiteres Risiko besteht darin, dass der Zugang nicht mehr direkt in das Hochschulrechenzentrum erfolgt, sondern über einen ISP und damit über das öffentliche Internet - wodurch die Datenverbindung potentiell unsicher wird. Diese Risiken werden mit der Verbreitung von DSL oder Kabelmodem Zugängen zunehmen, insbesondere wenn die Heimrechner lange am Netz sind.
Maßnahmen: Nummer 1, 3, 5, 12, 46, 63, 72.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.4 Sonstiges

3.2.3.4.1 Firewall Das Risiko von unzureichenden Firewalls besteht in der zu hohen Anzahl von Löchern sowie in dem Vortäuschen eines ausreichenden Schutzes. Andererseits genügen oft hochwertige Firewalls nicht den Durchsatzanforderungen im Wissenschaftsbereich.
Maßnahmen: Nummer 50.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.4.2 Whitelist/Blacklist Das Risiko der Blacklist (Verbotsliste) im Vergleich zur Whitelist (Erlaubnisliste/Positivliste) sind die vielen Löcher, die hierbei bestehen bleiben.

Maßnahmen: Nummer 51.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: mittel.

3.2.3.4.3 Interne Informationen Das Risiko der Erlangung von internen Informationen ("social engineering") durch einen Angreifer um damit in ein System einzubrechen, ist in einer eher offenen Arbeitsumgebung wie in einer Hochschule nicht unerheblich.
Maßnahmen: Nummer 68.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.4.4 Interne Angreifer Das Risiko von internen Angriffen ist laut Statistik sehr hoch und besteht insbesondere darin, dass kein Firewallschutz überwunden werden muss.
Maßnahmen: siehe Schutz von Servern.
Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.4.5 Mobile Geräte (Laptops) Das Risiko von mobilen Geräten besteht bei einem Wechsel von Anschlüssen im ungeschützten und geschützten Bereich darin, dass sie von außen kompromittiert werden und dann im geschützten Bereich selbst zu Gefahr werden.
Maßnahmen: Nummer 63, 69, 72.
Risikobewertung hinsichtlich des Auftretens: mittel.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.4.6 Konsolzugang Das Risiko des physikalischen Zugriffs auf die Konsole von Systemen besteht darin, dass dadurch meistens ein privilegierter Zugang (z.B. root unter UNIX) möglich wird.
Maßnahmen: Nummer 70.
Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.4.7 LVN Das Risiko des LVN-Zugangs aus dem BelWü-Netz besteht in der zunächst unsicheren Datenübertragung von sensitiven Daten. Hierfür existiert ein gesondertes Sicherheitskonzept, welches bei der BelWü-Koordination angefordert werden kann.
Maßnahmen: Nummer 71.

Risikobewertung hinsichtlich des Auftretens: hoch.
Risikobewertung hinsichtlich des Schadens: hoch.

3.2.3.5 Restrisiko

Das **Restrisiko** besteht in der höchsten Sicherheitsstufe

- in Tunneln wenn ein Komplize innerhalb des Hochschulnetzes sitzt und dort Kontrolle über ein Rechnersystem besitzt;
- wenn nach erfolgreicher Kompromittierung von Rechnern die Kommunikation der Angreifer zu diesen über Tunnel stattfindet;
- in verschlüsselten Datenverbindungen, die nicht kontrolliert werden können (z.B. Übertragung von Viren über eine HTTPS Verbindung).

Risikobewertung hinsichtlich des Auftretens: gering.
Risikobewertung hinsichtlich des Schadens: mittel bis groß.

3.3 Maßnahmenkatalog

Der folgende Maßnahmenkatalog bezieht sich auf die obige Risikoanalyse und stellt die wichtigsten Gegenmaßnahmen vor.

Siehe zu weiteren Maßnahmen der Endanwendungen Mail, FTP, WWW (incl. ActiveX, Java und Cookies) auch [19]. Die Nummern in der eckigen Klammer beziehen sich auf das Literaturverzeichnis, nicht auf die laufenden Nummern der Maßnahmen.

1. Zum interaktiven login nur SSH verwenden. Bei besonders sicherheitskritischen Zielen sollte SSH mit Einmalpasswörtern verwendet werden (wegen der Gefahr des Auslesens der Tastaturausgaben durch Trojanische Pferde). Siehe zu SSH [26] und [27].

2. Telnet von außen nur als Ausnahme und nur mit Ziel/Quellenpaar zulassen und dann vorzugsweise mit one time passwords.

3. SSH Protokolle (z.B. scp) und sendfile für Datenübertragungen verwenden.

4. FTP von außen nur zu AFTP Servern zulassen; darüberhinaus nur als Ausnahme und nur mit Ziel/Quellenpaar zulassen und dann vorzugsweise mit one time passwords.

5. Einsatz von verschlüsselten Verbindungen zwischen Mailboxserver und Mailclient (Secure POP3 und Secure IMAP).

6. Verschlüsselung von vertraulichen Mails mittels PGP.

7. Auf Mailserver ausführbare Attachments prüfen (diese Maßnahme dient der Gefahrenabwehr, deren Zulässigkeit ist jedoch umstritten).

8. ACL für SMTP-Verbindungen von außen am Eingangsrouter nur auf ausgewählte Mailhosts.

9. Relayfeste Mailhosts gemäß RFC2505 plus Unterstützung von authenticated SMTP. Siehe hierzu [30]. Relayfester Standard-CGI zum Mailversand (i.d.R. FormMail); siehe hierzu [31].

10. Bereitstellung von Spam-Filter (auf Anfrage von Nutzern). Siehe hierzu [32] und RFC2505.

11. Einsatz von DUL und RBL beim Mailhost (keine SMTP-Verbindungen von Spammern). Diese Maßnahme ist jedoch umstritten, insbesondere RBL. Siehe hierzu auch [33].

12. Unterstützung der Anwender hinsichtlich Virenschutz auf dem Endsystem. Besondere Bedeutung kommt hier einem regelmäßigen (mindestens wöchentlichen, automatischen) Update der Virensignaturen und der Einbeziehung wirklich aller Rechner zu.

13. Bereitstellung von Virenchecks im Mailhost und Web-Proxy.

14. Bei Bedarf für jugendfreie Web-Inhalte Negativ-Filterliste (URL, IP-Adresse) im Web-Proxy oder transparenten Proxy) verwenden. Siehe hierzu [35].

15. Active-X bzw. Java filtern. Dies ist bei HTTPS nicht möglich. Wenn eine generelle Filterung nicht durchsetzbar ist: Filter mit Ausnahmen; oder Benutzer auffordern, Active-X bzw. Java im Browser zu deaktivieren; oder Browser-Proxy (Zugang mittels X11) in der DMZ.

16. Squid und Socks von außen am Upstream Interface sperren.

17. Ungeeignete Newsgruppen (insbesondere Binary-Newsgruppen) nicht transportieren.

18. Ev. NNTP am Upstream Interface nur für ausgewählte interne Server und ggf. externe Clienten zulassen.

19. SNMP von außen am Upstream Interface sperren; wenn dies nicht möglich ist, soll SNMP in beiden Richtungen gesperrt werden.

20. SNMP community strings dürfen nicht "public" oder "private" heißen und dürfen nicht einfach zu erraten sein. Zusätzlich sollte der SNMP Zugang auf Router per Accessliste nur von wenigen berechtigten Rechnern aus erlaubt sein.

21. Portmapper von außen am Upstream Interface sperren (dies ist unzureichend für RPC Anwendungen). Siehe auch [40].

22. X11 in beiden Richtungen am Upstream Interface sperren. Ersatzlösung: X11 über SSH.

23. UUCP von außen am Upstream Interface sperren.

24. rsh, rcp, remsh, rcmd und rlogin von außen am Upstream Interface sperren.

25. NFS in beiden Richtungen am Upstream Interface sperren (Achtung: NFS verwendet teilweise auch dynamische Ports).

26. lockd in beiden Richtungen am Upstream Interface sperren.

27. syslogd von außen am Upstream Interface sperren.

28. bootp von außen am Upstream Interface sperren.

29. lpd von außen am Upstream Interface sperren.

30. ntpd von außen am Upstream Interface sperren.

31. TFTP von außen am Upstream Interface sperren.

32. NeTBIOS in beiden Richtungen am Upstream Interface sperren.

33. Keine HINFO Records benutzen. Ev. den Zonentransfer unterbinden. Letzteres ist eine umstrittene Maßnahme. Ev. den Einsatz von "splitted DNS" prüfen.

34. Einsatz von DNSSEC (für Signaturen) prüfen. Siehe auch [34].

35. Einsatz von neuesten statefull Firewalls für Multicastanwendungen. Ggf. Multicast-Proxy einsetzen. Zu netmeeting siehe [39].

36. ACL hinsichtlich IP Spoofing (in beiden Richtungen) und privaten IP-Adressen.

37. Sperren von Source Routing.

38. Sperren von "directed broadcast".

39. Sperren von *.*.*.0 und *.*.*.255 für IP von außen am Upstream Interface.

40. Traffic Shaping auf ICMP/UDP echo reply (ca. 5% der genutzten Bandbreite).

41. TCP Syn (TCP Intercept) in Betracht ziehen, insbesondere für bestimmte interne Server. Siehe hierzu [48].

42. Sperren von ICMP/UDP echo für BelWü IRC Server von außen am Upstream Interface. Whitelist für bestimmte ICMP Typen in der mittleren Sicherheitsstufe am Eingangsrouter bzw. Firewall einer Einrichtung. In den drei höchsten Sicherheitsstufen wird nur ICMP packet-to-big (3,4) durchgelassen. Siehe hierzu [46].

43. Einsatz von Passwörtern bei Routingprotokollen oder verschlüsselten Routingprotokollen.

44. Routingprotokolle auf Endnetzinterfaces (im Router) sperren.

45. Strukturierte Verkabelung um das Abhören zu erschweren.

46. Einsatz von IPSec zur Verschlüsselung von IP Datenpaketen.

47. Keine unverschlüsselten Funkverbindungen.

48. Abschottung von Funkzellen gegen Einbuchen Unbefugter, z.B. durch Kontrolle der MAC Adresse oder nach 802.1X sowie durch Konfiguration als "hidden network". Siehe hierzu auch [47].

49. Einsatz von sicheren VLAN-Switches.

50. Einsatz einer zumindest statefull Firewall, d.h. Verzicht einer stateless Firewall bzw. ACL. Vorzuziehen wäre allerdings eine Application Firewall, sofern sie den gewünschten Durchsatz bietet.

51. Einsatz einer Whitelist anstelle einer Blacklist bei hohen Sicherheitsanforderungen.

52. Tunnel (GRE, IPSec, IPv6) nur als Ausnahme und nur mit Ziel/Quellenpaar zulassen. Tunnelenden im geschützten Bereich müssen besonders geschützt werden, der Zugriff über Tunnelprotokolle darf nur von Sicherheitsbeauftragten freigegeben werden. Dies bedeutet u.U. auch Einschränkungen für SSH. Die Geräte auf der nicht geschützten Seite müssen unbedingt durch persönliche Firewalls geschützt werden.

53. Keine Weiterleitung von Datenpaketen in das LAN (IP Forwarding).

54. Nur wenige SDH, ATM, Großrechnerkoppelungen, QoS-Interfaces an der zentralen Firewall vorbei zulassen.

55. SDH, ATM, Großrechnerkoppelungen, QoS-Endpunkte in der Hochschule nur auf Rechner, die nicht im LAN der Hochschule hängen.

56. Einwahl von außen nur in die zentrale DMZ (getrenntes Servernetz) zulassen.

57. Aktuelle Systemsoftware (Betriebssystem, Anwendungsprogramm) sowie ständig aktuelle Sicherheitspatches benutzen. Dies gilt insbesondere für von außen erreichbare Systeme, d.h. Server. Zusätzlich ist eine TOP10 Liste der aktuellen kritischsten Sicherheitsbedrohungen zu verfolgen (z.B. [11]) oder besser noch selbst für die eigene Einrichtung aufzustellen und zu pflegen.

58. Sorgfältiger Einsatz von CGI-Skripten auf Webservern.

59. Von außen erreichbare Systeme nur in der DMZ (Servernetz) betreiben.

60. Verbindungen von außen nur als Ausnahme zulassen.

61. IDS System um Angriffe auf Server mitzuloggen, zu warnen und ggf. abzublocken.

62. ACL für HTTP/HTTPS Verbindungen von außen am Eingangsrouter nur auf ausgewählte Web-Server. Diese Web-Server sollten bevorzugt in der DMZ stehen. Ggf. kann mittels Portumlenkung der gesamte HTTP-Verkehr auf den zentralen Web-Server zwangsumgeleitet werden.

63. Personal Firewall Software bzw. Paketfilter auf Arbeitsplatzrechner installieren. Konfigurationsempfehlungen für die wichtigsten Produkte sollen vom Rechenzentrum den Benutzern bereitgestellt werden.

64. Open Source Anwendungen wenn möglich.

65. Nicht benötigte Dienste auf Endsystemen deaktivieren und in der Firewall sperren.

66. Der Rechner darf keine schwachen Passwörter erlauben. Passwort-Crackprogramme sind bei Servern regelmäßig anzuwenden.

67. Keine Sammelnutzeraccounts, d.h. mehrere Nutzer haben dasselbe Passwort.

68. Personalaufklärung hinsichtlich "social engineering".

69. Mobile Geräte (z.B. Laptops) dürfen nicht zwischen Anschlüssen im ungeschützten und im geschützten Bereich wechseln.

70. Unbeaufsichtigte Rechner nur in gesicherten Räumen.

71. Verschlüsselter LVN-Zugang per Einzelplatz-PC oder LAN Anbindung. Siehe hierzu [23].

72. Benutzer auf Risiko hinweisen.

Transport	Port	Protokoll	Beschreibung	gesperrte Richtung
ICMP	0 und 8	echo / echo reply	Schutz für IRC Server	von außen
UDP	7	echo	Schutz für IRC Server	von außen
UDP	67	bootps	bootp/DHCP Server	von außen
UDP	68	bootpc	bootp/DHCP Client	von außen
UDP	69	TFTP	Filetransfer (ohne Passwörter)	von außen
UDP, TCP	111	Portmapper	Portmapper	von außen
UDP	123	ntpd	Time Service	von außen
UDP, TCP	137-139,445	NeTBIOS	SMB	beide
UDP, TCP	161-162	SNMP	Netzwerkmanagement	von außen
TCP	512	rexec	R-Kommando	von außen
TCP	513	rlogin	R-Kommando	von außen
TCP	514	rsh, rcp, rdump, rrestore, rdist	R-Kommandos	von außen
UDP	514	syslogd	Logdateien	von außen
TCP	515	lpd	Drucker	von außen
TCP	540	UUCP	Mail (zu Mailhosts durchlassen)	von außen
TCP	1080	Socks	Anwendungsproxy	von außen
UDP, TCP	2049	NFS	Filesystem (auch andere Ports mögl.)	beide
TCP	3128	Squid	Web-Proxy	von außen
UDP, TCP	4045	lockd	NFS lock manager	beide
TCP	6000-6063	X11	entferntes Terminal	beide

Tabelle 3.1: Grundschutz an Peering und Upstream ISP Interfaces (Verbotsliste)

3.3.1 Sperrung von bestimmten Ports auf den ISP-Interfaces (Verbotsliste)

Die folgende Liste wurde aufgrund der Maßnahmen 42, 28, 31, 21, 30, 32, 19, 24, 27, 29, 23, 16, 25, 26 und 22 zusammengestellt. Erfahrungsgemäß basiert die Mehrheit der Einbrüche auf wenigen, teilweise sehr alten Sicherheitslöchern. Die Sperrung auf den ISP-Interfaces soll keine BelWü-zentrale Firewall darstellen sondern nach dem Zwiebelschalenprinzip den gröbsten Unfug an den Außengrenzen des BelWü herausfiltern. Bei Bedarf können Ausnahmen zugelassen werden (wenn z.B. rlogin von außen zu einem bestimmten Rechner in einer Hochschule notwendig ist); wenn die Ausnahmen zu umfangreich werden, muss der betreffenden Port jedoch wieder aufgemacht werden. Weitere zu sperrende Ports können auf Vorschlag des BelWü-AK1 und Zustimmung des Universitätsrechenzentrumsleiterkreises (Achern) hinzugenommen werden.

Neben ICMP und UDP echo/echo-reply für IRC Server innerhalb des BelWü sollen die Ports gemäß der Tabelle 3.1 auf den Peering und Upstream ISP Interfaces gesperrt werden.

Von einer Sperrung von Spieleservern, back orifice u.ä. wurde abgesehen, da diese Ports teilweise auch von anderen Anwendungen verwendet werden. Vor der aktuellen Sperrung sollte durch ein entsprechendes mitloggen Daten erfasst werden, wieviel Verkehr hierdurch betroffen wird. Eine entsprechende Benachrichtigung der Nutzer erfolgt durch die jeweiligen Rechenzentren.

Server	Transport	Port	Protokoll	Beschreibung
	ICMP	3,4	packet-too-big	MTU Aushandlung
	TCP	113	Ident	Authentifizierungsservice
	TCP	22	SSH	interaktiver Zugang, verschlüsselt
	TCP	487	SAFT	Filetransfer (ohne Passwörter)
S	UDP	53	DNS	Domain Service
S	TCP	53	DNS	Domain Service, Zonentransfer
S	TCP	389	LDAP	Verzeichnisdienst
S	TCP	119	NNTP	Newsservice
S	UDP	123	NTP	Timeservice
S	TCP	25	SMTP	Mailtransport
S	TCP	21	FTP	Filetransfer
S	TCP	80	HTTP	Web-Server
S	TCP	443	HTTPS	Web-Server
S	TCP	995	POP3S	Secure POP3
S	TCP	993	IMAPS	Secure IMAP
S	UDP	dynamisch	IGMP, RTP, RTCP	MBone

Tabelle 3.2: Erlaubnisliste für die hohe Sicherheitsstufe

Server	Transport	Port	Protokoll	Beschreibung
	TCP	23	Telnet	interaktiver Zugang
	TCP	21	FTP	Filetransfer (plus Ports > 1023 für passive ftp)
S	TCP	110	POP3	Mailbox
S	TCP	143	IMAP	Mailbox

Tabelle 3.3: Erweiterung um Anwendungen mit Klartextpasswörter

3.3.2 Zugelassene Anwendungen (Erlaubnisliste)

Bei einer restriktiven Sicherheitsrichtlinie können auf dem Eingangsrouter bzw. Firewall einer Einrichtung die Ports gemäß der Tabelle 3.2 mittels einer Whitelist von außerhalb zugelassen werden. Dabei bedeutet ein "S" in der ersten Spalte, dass der Port nur auf bestimmte Server bei der Einrichtung freigeschaltet wird. Naturgemäß verbessert sich der Schutz erheblich, je weniger Verbindungen von außen zugelassen werden - dies betrifft insbesondere die Ports ohne ein "S" in der ersten Spalte. Hinsichtlich ICMP soll generell nur packet-too-big (3,4) von außen erlaubt sein, wobei für einzelne Rechner/Server mehr ICMP Typen zugelassen werden können.

Bei geringeren Sicherheitsanforderungen können zusätzlich die Ports gemäß der Tabelle 3.3 von außerhalb zugelassen werden (dabei besteht die Gefahr der Übermittlung von unverschlüsselten Passwörtern über das Netz).

Bei noch geringeren Sicherheitsanforderungen können zusätzlich die Ports gemäß der Tabelle 3.4 von außerhalb zugelassen werden.

Hinsichtlich ICMP sollen von außen durchgelassen werden (in Klammern Type und Code): net-unreachable (3,0), host-unreachable (3,1), port-unreachable (3,3), packet-too-big (3,4), administratively-prohibited (3,13), ttl-exceeded (11,0), echo-request (8), echo-reply (0) (letztere zwei nicht für IRC Server). Der Rest von ICMP soll gesperrt werden.

Server	Transport	Port	Protokoll	Beschreibung
	ICMP	0 3,0 3,1 3,3 3,4 3,13 8 11,0	diverse	diverse ICMP
	UDP, TCP	dynamisch	H.323-Suite	Multimedia (Netmeeting)
S	TCP	dynamisch	ADSM	Datenbackup
S	UDP	1645	RADIUS	Authentifizierungsdatenbank
S	UDP	1646	RADIUS	Accountingdatenbank
S	UDP	6970-7170	Real Audio	Multimedia (Real Audio)
S	TCP	607	NQS	Network Queueing System (Batch)
S	TCP	dynamisch	SQL	Datenbank
S	GRE	4	GRE, IPIP	IP/IP Tunnel
S	IPSec	50,51	IPSec	IPsec
S	IPv6		IPv6	IPv6 Tunnel

Tabelle 3.4: Erweiterung der Erlaubnisliste um weitere Anwendungen

Sicherheitsstufe	Grobe Ausprägung
extrem hoch	kein Zugang von außen, Java/Active-X/Mailattachments filtern
sehr hoch	Zugang von außen nur auf wenige Server
hoch	Whitelist gemäß Kapitel 3.3.2, Tabelle 3.2
mittel	Whitelist gemäß Kapitel 3.3.2, Tabelle 3.2, 3.3 und 3.4
gering	Blacklist

Tabelle 3.5: Sicherheitsstufen

3.4 Sicherheitsstufen

Aufgrund der obigen Maßnahmen werden fünf Sicherheitsstufen gemäß der Tabelle 3.5 definiert.

Die hohen Sicherheitsstufen haben große Einschränkungen der nutzbaren Internetdienste zur Folge. Dies stellt insbesondere für größere Hochschulen ein Problem dar. Eine mögliche Lösung ist, dass die Hochschule zwei Internetzugänge zur Verfügung stellt: ein gesicherter und ein ungesicherter. Allerdings darf dann keine interne Verbindung ohne Firewall zwischen diesen beiden Bereichen bestehen.

Zu den fünf Sicherheitsstufen ist im einzelnen folgendes zu sagen:

extrem hoch Diese höchste Sicherheitsstufe ist für Einrichtungen gedacht, die keine Studenten zu versorgen haben und keine/kaum Forschungs- und Lehre-Aufgaben erfüllen müssen. Ein Beispiel hierfür wären Museen.
Der entscheidende Unterschied zur nächstniedrigen Stufe ("sehr hoch") liegt darin, dass grundsätzlich kein Zugang von außen zulässig ist sowie im Filtern von Java, Active-X und JavaScript. Durch den ersten Punkt ergibt sich, dass die Mailboxen auf einem externen Mailhost liegen, ebenso befinden sich die Webseiten auf einem externen Rechner.

sehr hoch Diese zweithöchste Sicherheitsstufe ist für Einrichtungen gedacht, die einen sehr hohen Schutzbedarf haben aber z.B. aufgrund ihrer Größe oder Funktionalität Verbindungen von außen benötigen - diese aber auf ein paar wenige Server begrenzen können. Ein Beispiel hierfür kann eine kleine Fachhochschule oder Berufsakademie sein.

Der Unterschied zur nächstniedrigen Stufe ("hoch") liegt darin, dass Server nur in der DMZ stehen, Mailattachments auf Viren überprüft werden und Spamfilter bereitgestellt werden.

hoch Diese dritthöchste Sicherheitsstufe ist für Einrichtungen gedacht, die von außen vielfach erreichbar sind, diese Zugänge jedoch auf eine gewisse Anzahl definierter Dienste und sicherer Anwendungen gemäß Tabelle 3.2 auf Seite 31 begrenzen. Ein Beispiel hierfür kann eine Universität mit einer restriktiven Sicherheitspolitik sein.
Der Unterschied zur nächstniedrigen Stufe ("mittel") liegt darin, dass Einwahlknoten nur in DMZ stehen, ssh und scp anstelle von Telnet und FTP verwendet wird, und POP/IMAP verschlüsselt benutzt.

mittel Diese vierthöchste Sicherheitsstufe ist für Einrichtungen gedacht, die von außen vielfach erreichbar sind und hierbei auch Risiken hinsichtlich Klartextpasswörter und einer erhöhten Anzahl von Anwendungen gemäß den Tabellen 3.2, 3.3 und 3.4 auf Seite 31 hinnehmen. Ein Beispiel hierfür ist eine Hochschule, die aufgrund von gewachsenen Strukturen, Gewohnheiten und/oder schlechter Personalsituation mit diesen Risiken leben muss.
Der Unterschied zur nächstniedrigen Stufe ("gering") liegt darin, dass eine Positivliste ("Whitelist") verwendet wird, Server besser gepflegt sind, SMTP von außen nur auf Server zugelassen ist und dass Benutzer hinsichtlich Viren unterstützt werden.

gering In dieser niedrigsten Sicherheitsstufe sind diejenigen Einrichtungen, die aufgrund von gewachsenen Strukturen, Gewohnheiten und/oder schlechter Personalsituation keine Positivliste ("Whitelist") benutzen können und keine oder sehr wenig Zeit in Maßnahmen der Rechnersicherheit stecken können. Diese Einrichtungen profitieren am meisten durch den BelWü-Grundschutz an den Upstream-ISP Interfaces gemäß Tabelle 3.1 auf Seite 30. Allerdings sollte das Rechenzentrum bzw. der EDV-Beauftragte beim nächsten größeren Sicherheitsvorfall intern auf eine höhere Sicherheitsstufe drängen.

Im einzelnen können die behandelten Risiken und Maßnahmen den 5 Sicherheitsstufen wie folgt zugewiesen werden (U = Upstream ISP Interface Filter; min. = minimal; empf. = empfohlen; "-" = trifft nicht zu oder ist nicht notwendig):

Risiko Nr.	Beschreibung	Nr.	Maßnahme Beschreibung	U	extr. min	hoch empf	Nr.	sehr min	hoch empf	hoch min	empf	Nr.	mit min	tel empf	ger min	ing empf
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	1	SSH benutzen		x		1	x		x		1		x		x
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	2	Telnet nur ausnahmsweise		-	-	2	x		x		2	-	-	-	-
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	3	scp benutzen		x		3	x		x		3	-	-	-	-
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	4	FTP nur ausnahmsweise		-	-	4	x		x		4	-	-	-	-
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.1.2	Klartextpasswörter bei POP/IMAP	5	Verschlüsseltes POP/IMAP		x		5	x		x		5		x	-	-
3.2.3.1.2	Klartextpasswörter bei POP/IMAP	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.1.3	unverschlüsselte Mailinhalte	6	Mail verschlüsseln		x		6	x		x		6	x		x	
3.2.3.1.3	unverschlüsselte Mailinhalte	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.1.4	Spam-Mail und Mailrelaying	8	SMTP von außen nur auf Server		-	-	8	x		x		8	x			x
3.2.3.1.4	Spam-Mail und Mailrelaying	9	Relayfeste Mailhosts		-	-	9	x		x		9	x		x	
3.2.3.1.4	Spam-Mail und Mailrelaying	10	Spam-Filter		-	-	10		x		x	10		x		-
3.2.3.1.4	Spam-Mail und Mailrelaying	11	DUL/RBL einsetzen		-	-	11		x		x	11		-		-
3.2.3.1.5	Mail-Attachment	7	Attachments prüfen		x		7	x			x	7		x		-
3.2.3.1.5	Mail-Attachment	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.1.6	Viren	12	Virenschutz PC		x		12	x		x		12	x			x
3.2.3.1.6	Viren	13	Virenschutz Mailhost/Web-Proxy		x		13	x			x	13		x		x
3.2.3.1.7	Active-X, JavaScript u. ähnliches	15	Active-X u.ä. filtern		x		15		x		x	15		-		-
3.2.3.1.7	Active-X, JavaScript u. ähnliches	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.1.8	Java	15	Java filtern		x		15		x		x	15		-		-
3.2.3.1.8	Java	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.1.9	Nicht-jugendfreie Web-Inhalte	14	Webinhalte filtern	-	-	-	14	-	-	-	-	14	-	-	-	-
3.2.3.1.10	Squid und Socks	16	Squid/Socks am Upstream filtern	x	-	-	16	-	-	-	-	16	-	-	-	-
3.2.3.1.11	Newsdienst	17	Newsgruppen filtern	x	-	-	17	-	-	-	-	17	-	-	-	-
3.2.3.1.11	Newsdienst	18	nur wenige Newsfeeds am Upstream	-	-	-	18	-	-	-	-	18	-	-	-	-
3.2.3.1.12	SNMP	19	SNMP am Upstream filtern	x	-	-	19	-	-	-	-	19	-	-	-	-
3.2.3.1.12	SNMP	20	SNMP Passwort/Zugang		x	-	20	x	-	x	-	20	x	-	x	-
3.2.3.1.13	Portmapper	21	Portmapper am Upstream filtern	x	-	-	21	-	-	-	-	21	-	-	-	-
3.2.3.1.14	X11	22	X11 am Upstream filtern	x	-	-	22	-	-	-	-	22	-	-	-	-
3.2.3.1.15	UUCP	23	UUCP am Upstream filtern	x	-	-	23	-	-	-	-	23	-	-	-	-
3.2.3.1.16	R-Kommandos	24	R-Kommandos am Upstream filtern	x	-	-	24	-	-	-	-	24	-	-	-	-
3.2.3.1.17	NFS	25	NFS am Upstream filtern	x	-	-	25	-	-	-	-	25	-	-	-	-
3.2.3.1.19	syslogd	27	syslogd am Upstream filtern	x	-	-	27	-	-	-	-	27	-	-	-	-
3.2.3.1.20	bootp/DHCP	28	bootp am Upstream filtern	x	-	-	28	-	-	-	-	28	-	-	-	-
3.2.3.1.21	lpd	29	lpd am Upstream filtern	x	-	-	29	-	-	-	-	29	-	-	-	-
3.2.3.1.22	ntpd	30	ntpd am Upstream filtern	x	-	-	30	-	-	-	-	30	-	-	-	-
3.2.3.1.23	TFTP	31	TFTP am Upstream filtern	x	-	-	31	-	-	-	-	31	-	-	-	-
3.2.3.1.24	NeTBIOS/SMB	32	NeTBIOS am Upstream filtern	x	x	-	32	x	-	x	-	32	x	-	x	-
3.2.3.1.25	DNS	33	keine HINFO Records		x		33	x		x		33		x		x
3.2.3.1.25	DNS	34	DNSSEC prüfen			x	33		x		x	34		x		x
3.2.3.1.26	Multicast/Multimedia	35	Neueste Firewalls benutzen		x		35					35		x	-	-

Risiko Nr.	Beschreibung	Nr.	Maßnahme Beschreibung	U	extr. min	hoch empf	Nr.	sehr min	hoch empf	hoch min	empf	Nr.	mit min	tel empf	ger min	ing empf
3.2.3.2.1	ungepflegte Systeme/Anwendungen	57	Sicherheitspatches		x		57	x		x		57	x		x	
3.2.3.2.1	ungepflegte Systeme/Anwendungen	58	sorgfältige CGI-Skripte		x		58	x		x		58	x		x	
3.2.3.2.1	ungepflegte Systeme/Anwendungen	59	Server in DMZ		-		59	x			x	59		x	-	-
3.2.3.2.1	ungepflegte Systeme/Anwendungen	60	ausnahmsweise Verbindungen von außen		-		60	x		x		60	x		-	-
3.2.3.2.1	ungepflegte Systeme/Anwendungen	61	IDS System einsetzen		-	x	61	x			x	61		x	-	-
3.2.3.2.1	ungepflegte Systeme/Anwendungen	62	Web von außen nur auf Server		-		62	x		x		62	x		-	-
3.2.3.2.1	ungepflegte Systeme/Anwendungen	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.2.2	Personal Firewall	63	Personal Firewall einsetzen		x		63		x		x	63		x		x
3.2.3.2.3	Software ohne Quellcode	59	Server in DMZ		-	-	59	x			x	59		x	-	-
3.2.3.2.3	Software ohne Quellcode	64	Opensource einsetzen		-	x	64		x		x	64		x		x
3.2.3.2.3	Software ohne Quellcode	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.2.4	Unnötige Dienste	65	Unnötige Dienste sperren		x		65	x		x		65	x		x	
3.2.3.2.5	schwache/gemeinsame Passwörter	66	Starke Passwörter		x		66	x		x		66	x		x	
3.2.3.2.5	schwache/gemeinsame Passwörter	67	Keine Sammelaccounts		x		67	x		x		67	x		x	
3.2.3.2.5	schwache/gemeinsame Passwörter	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.3.1	(D)DoS Attacken	36	IP Spoofing sperren	x	x		36	x		x		36	x		x	
3.2.3.3.1	(D)DoS Attacken	37	Source Routing sperren	x	x		37	x		x		37	x		x	
3.2.3.3.1	(D)DoS Attacken	38	directed broadcast sperren		x		38	x		x		38	x		x	
3.2.3.3.1	(D)DoS Attacken	39	*.*.*.0 und *.*.*.255 sperren	x	x		39	x		x		39	x		x	
3.2.3.3.1	(D)DoS Attacken	40	ICMP/UDP Echo Reply begrenzen	x	x		40	x		x		40	x			x
3.2.3.3.1	(D)DoS Attacken	41	TCP Intercept einsetzen		-	-	41		x		x	41		x	-	-
3.2.3.3.2	ICMP	42	manche ICMP-Typen sperren	x	x		42	x		x		42	x		-	-
3.2.3.3.3	Routingprotokolle	43	sichere Routingprotokolle	x	x		43	x			x	43		x	-	-
3.2.3.3.3	Routingprotokolle	44	Routingprotokolle begrenzen	x	x		44	x		x		44	x			x
3.2.3.3.5	Ungeschützte Netzwerkverbindungen	45	Strukturierte Verkabelung		x		45	x		x		45	x			x
3.2.3.3.5	Ungeschützte Netzwerkverbindungen	47	Verschlüsselte Funkverbindungen		x		47	x		x		47	x		x	
3.2.3.3.5	Ungeschützte Netzwerkverbindungen	48	Kein Einbuchen Unbefugter		x		48	x		x		48	x		x	
3.2.3.3.6	VLAN	49	Sichere VLAN-Switches einsetzen		x		49	x		x		49	x			x
3.2.3.3.7	Tunnel	52	Tunnel nur ausnahmsweise		-	-	52	x		x		52	x		-	-
3.2.3.3.7	Tunnel	53	Tunnelendpunkte routen nicht		-	-	53	x		x		53	x		-	-
3.2.3.3.7	Tunnel	72	Benutzer schulen		x		72	x		x		72	x		x	
3.2.3.3.8	SDH, ATM, etc.	53	SDH etc. Endpunkte routen nicht		-	-	53	x		x		53	x		-	-
3.2.3.3.8	SDH, ATM, etc.	54	SDH etc. nur ausnahmsweise		-	-	54	x		x		54	x		-	-
3.2.3.3.8	SDH, ATM, etc.	55	SDH etc. Endpunkte nicht im LAN		-	-	55	x		x		55		x	-	-
3.2.3.3.10	Einwahl	53	Einwahlknoten routen nicht		-		53	x		x		53		x	-	-
3.2.3.3.10	Einwahl	56	Einwahlknoten nur in DMZ		-		56	x		x		56		x	-	-
3.2.3.3.10	Einwahl	72	Benutzer schulen		-		72	x		x		72	x		x	
3.2.3.3.11	DSL, Modem	1	SSH benutzen		-		1	x		x		1		x		x
3.2.3.3.11	DSL, Modem	3	scp benutzen		-		3	x		x		3	-	-	-	-
3.2.3.3.11	DSL, Modem	5	Verschlüsseltes POP/IMAP		-		5	x		x		5		x	-	-
3.2.3.3.11	DSL, Modem	12	Virenschutz PC		-		12	x		x		12	x			x
3.2.3.3.11	DSL, Modem	46	IPSec einsetzen		-		46	x		x		46	x		x	
3.2.3.3.11	DSL, Modem	63	Personal Firewall einsetzen		-		63		x		x	63		x		x
3.2.3.3.11	DSL, Modem	72	Benutzer schulen		-		72	x		x		72	x		x	
3.2.3.4.1	Unzureichender Firewall	50	Starker Firewall (statefull)		x		50	x		x		50		x		x
3.2.3.4.2	Blacklist (Verbotsliste)	51	Whitelist einsetzen		x		51	x		x		51	x		-	-
3.2.3.4.3	Interne Informationen	68	Benutzer schulen		x		68	x		x		68	x		x	
3.2.3.4.5	Mobile Geräte (Laptop)	69	Laptop vor/hinter Firewall		-		69	x		x		69		x		x
3.2.3.4.5	Mobile Geräte (Laptop)	63	Personal Firewall einsetzen		-		63	x		x		63		x		x
3.2.3.4.5	Mobile Geräte (Laptop)	72	Benutzer schulen		-		72	x		x		72	x		x	
3.2.3.4.6	Konsolzugang	70	Rechner in sichere Räume		x		70	x		x		70		x		x
3.2.3.4.7	LVN-Zugang	71	Verschlüsselter LVN-Zugang	x	x		71	x		x		71	x		x	

Tabelle 3.6: Maßnahmenkatalog

3.5 Phasenkonzept Realisierung

1. Die ISP Interface Konfiguration kann sofort umgesetzt werden.
2. Bei den 21 nicht-universitären Einrichtungen, die ab 2001 bzw. 2002 über schnelle Tesion-Zugänge verfügen werden, ist ein Schutz mittels Firewall Feature Set und IDS auf den Ciscoroutern vorgesehen. Bei den anderen nicht-universitären Einrichtungen erfolgt der Schutz ggf. mittels den im normalen IOS vorhandenen ACLs. Die Einrichtung der Zugangskontrollen erfolgt immer in Absprache mit der jeweiligen Einrichtung.
3. Anpassung der universitären RZ-Firewall.
4. Zum Erkennen von Angriffen soll ein IDS testweise betrieben werden um die Möglichkeiten eines solchen Systems zu erkunden. Siehe hierzu auch [18].
5. Ggf. soll eine Authentifizierungsstudie die Möglichkeiten von Chipkarten untersuchen und entsprechende Empfehlungen aussprechen.

3.6 Regelungen (technisch und organisatorisch)

3.6.1 Maßnahmen BelWü-Einrichtungen

Folgendes gilt für die Universitäten:

- Installation einer FW/ACL Whitelist am RZ-Router bzw. RZ-Firewall.

Folgendes gilt für alle Einrichtungen:

- Verabschiedung einer Sicherheitsrichtlinie (Policy). Hierzu wird neben dem vorliegenden BelWü-Sicherheitskonzept noch [12] empfohlen.

3.6.2 Maßnahmen BelWü-Koordination

- Installation eines Grundschutzes sowie FW/ACL Whitelist auf den nicht-universitären BelWü-Zugangsroutern in Absprache mit den jeweiligen Einrichtungen.
- Installation eines Grundschutzes auf den ISP Interfaces.

3.6.3 Vorfallbearbeitung

Bei einem aktuellen Angriff ist die BelWü-Koordination ermächtigt, angemessene Gegenmaßnahmen zu ergreifen (z.B. Sperrung von Ports oder IP-Adressen). Diese Maßnahmen müssen immer mit dem lokalen BelWü-Beauftragten abgestimmt sein; wenn dieser nicht erreichbar ist (insbesondere außerhalb der üblichen Arbeitszeiten), kann die Maßnahme auch ohne Absprache erfolgen.
Die Netzordnungen der jeweiligen Hochschulen regeln die Verantwortlichkeit der Rechenzentren hinsichtlich des Hochschul-LAN.

Aktuelle oder erfolgte Angriffe werden über die Mailliste incident@belwue.de verbreitet. Hierfür steht ein Archiv zur Verfügung.

In der RIPE Datenbasis sollen Role Accounts ("security@" und "abuse@") der Hochschulen aufgeführt sein.

Bei Anfragen einer Ermittlungsbehörde ist zu beachten, dass der Anfrage eine entsprechende Rechtsgrundlage zugrundeliegt. Bei einer Anfrage muss immer der Leiter der Einrichtung (bei einer Universität der Kanzler/Rektor/Präsident) eingeschaltet werden bzw. über ihn die Auskunft erteilt werden oder es muss eine Prozedur durch diese Person/Funktion festgelegt worden sein, die diese Kompetenz an einen Beauftragten delegiert hat. Da dies zu keiner Zeitverzögerung führen darf, sind relevante Log-Dateien zum Zeitpunkt der Anfrage zu sichern.

Für verschiedene Sicherheitsvorfälle ist ein Verfahren festzulegen, nach dem im Sicherheitsvorfall vorzugehen ist. Ein Beispiel hierfür ist eine Prozedur bei DDoS-Angriffen.

3.6.4 Management

Bei nicht-universitären Einrichtungen, deren Zugangsschutz auf dem BelWü-Router basiert, erfolgt die Erstellung und Änderung der ACL im Einvernehmen mit dem lokalen BelWü-Beauftragten. Die Konfiguration der ACL kann auch direkt durch den lokalen BelWü-Beauftragten erfolgen. Die relevanten Log-Dateien werden durch den lokalen BelWü-Beauftragten und die BelWü-Koordination ausgewertet.

Wenn Ausnahmen ("Löcher") in einer ACL einen solchen Umfang annehmen, dass sie nicht mehr handhabbar sind, muss der betroffene Dienst auf dem Firewall freigeschaltet werden und der Schutz auf andere Art und Weise (z.B. auf den Endsystemen) erreicht werden.

Servertests (z.B. bei neuem WU-FTP Loch) durch die BelWü-Koordination mit anschließender Benachrichtigung der Betreibern von löchrigen Servern sind anzustreben. Dies erfordert ein automatisiertes Verfahren mittels einer "network based vulnerability test software" (z.B. Nessus, Nmap oder Cisco Secure Scanner).

Kapitel 4

Konzepte (Intranet, DMZ, Firewall, NAT, Authentifizierung)

4.1 Intranet

Ein Intranet ist ein abgeschlossenes Netz einer organisatorischen Einheit. Es hat einen kontrollierten Übergang (z.B. Firewall) zum Internet. Die Konnektivitäts- und Schutzanforderung für die angeschlossenen Systeme sind weitgehend einheitlich und können deshalb einer gemeinsamen Sicherheitsrichtlinie (Policy) unterworfen werden. Innerhalb des Intranet besteht nach landläufiger Auffassung gegenseitiges Vertrauen, so dass in diesem Bereich i.d.R. keine weiteren Schutzmaßnahmen erforderlich sein sollten.

Ein solches Intranet ist bei schon größeren BelWü-Einrichtung oft nicht möglich. Beispielsweise planen die Universitäten Heidelberg und Karlsruhe dezentrale Firewallsysteme und haben solche zum Teil schon eingerichtet. Im weit größeren BelWü ist ein Intranet erst recht nicht möglich. Die Interessenlage der einzelnen Einrichtungen ist zu verschieden. Auch schließt die Größe des Bereiches gegenseitiges Vertrauen aus, da sonst die Gefahr von Angriffen von Insidern viel zu groß wird.

Eine zentrale BelWü-Firewall wird als nicht praktikabel angesehen: Es fehlt eine gemeinsame Policy bzw. ein gemeinsames Intranet; die Selbständigkeit der Universitäten steht dem entgegen wie auch potentielle Performance- und Managementprobleme (letztere wegen der Komplexität der vielen Ausnahmeregeln, wenn alle Einrichtungen durch eine einzige Firewall gehen).

4.2 Sicherung von öffentlichen Servern

Zur Sicherung von öffentlichen Servern bieten sich verschiedene Techniken an:

Zu einen können diese Server in einem relativ offenen Bereich hinter dem Eingangsrouter untergebracht werden. Die Server selbst werden durch konsequente Beseitigung von Schwachstellen im Betriebssystem und den Anwendungen gegen Angriffe geschützt. Zusätzlich bietet sich die Anwendung von internen Firewalltechniken an. Bei einer kleinen Anzahl von Servern ist ein solches Vorgehen sinnvoll.

Zum andern können vorgeschaltete Firewallsysteme den Schutz übernehmen. Diese müssen dann sowohl Angriffe aus dem Internet wie auch aus der eigenen Einrichtung abwehren. Die Server liegen dann in einer DMZ oder einem SSN (Sicheren Server Netz). Auch bei dieser Lösung sollten zusätzliche Schutzmaßnahmen auf den Servern vorgenommen werden.

4.3 Firewall

Zum Schutz der Einrichtungen werden statefull Firewalls empfohlen. Dies können dedizierte Firewalls sein, aber auch ein Cisco IOS mit Firewall Feature Set. Letzteres ermöglicht context-based ACLs; bei normalem Cisco IOS sind reflexive ACLs den "normalen" ACLs vorzuziehen. Siehe Seite 50 zu reflexiven ACLs und Seite 51 zu context-based ACLs. Grundsätzlich sollten vermehrt Positivlisten (Whitelist) anstelle von Verbotslisten (Blacklist) verwendet werden.

4.4 NAT

Private IP-Adressen haben den Vorteil des zusätzlichen Schutzes vor Angriffen von außen. Der Nachteil ist, dass die ggf. notwendige Adressumsetzung (NAT) manche Anwendungen nicht ermöglicht (siehe hierzu RFC1631, RFC2663 und RFC2775). NAT bzw. private IP-Adressen werden für Studentenwohnheime und Verwaltungen empfohlen, aber auch für kleinere Einrichtungen und bestimmte Uni-Subnetze können sie sinnvoll sein. Bei Verwaltungen ist zu beachten, dass der vom LVN für den MWK-Bereich vorgesehene Adressraum verwendet wird.

4.5 Chipkarte

In Baden Württemberg ist im Jahr 2000 das Projekt "BW-CARD" angelaufen, das die flächendeckende Versorgung der Bevölkerung mit kryptographischen Zertifikaten zur sicheren Authentifizierung bei elektronischen Transaktionen (E-Business, elektronische Behördengänge, usw.) zum Ziel hat. Dabei sollen die zertifizierten Schlüsselpaare, die auf Chipkarten gespeichert und zunächst an Interessierte ausgegeben werden, auch zur Leistung einer digitalen Unterschrift in zunächst ausgewählten Anwen-

dungen verwendet werden können. Zu den ausgewählten Anwendungen zählen hierbei vor allem Verwaltungsvorgänge. Der Landtag hat ein entsprechendes Gesetz verabschiedet und die rechtlichen Grundlagen für einen solchen Versuch geschaffen. Zur Zeit werden die technischen und organisatorischen Voraussetzungen, die für den Beginn des Versuches geschaffen werden müssen untersucht. Die Universität Stuttgart beteiligt sich an diesem Versuch und wird im Bereich der studentischen Anwendungen Pilotfunktion übernehmen.
Da die auszugebenden Zertifikate bestehenden Standards entsprechen werden, sind sie geeignet neben o.g. Anwendungen auch für eine kryptographisch starke Benutzerauthentifizierung verwendet zu werden. In einem ersten Szenario könnte sich das BelWü als Pilot für die Anwendung der BW-CARD zur Authentifizierung von BelWü-Benutzern (die lediglich eine BW-CARD besitzen müssten) gegenüber ausgewählten Diensten im BelWü zur Verfügung stellen. Auch die Authentifizierung von BelWü-Mitarbeitern gegenüber der eigenen Infrastruktur könnte mit moderatem Aufwand implementiert werden. In einem fortgeschrittenen Stadium, wenn bereits Studenten mit der BW-CARD ausgerüstet sind kann die Benutzerverwaltung (zumindest beim Piloten Universität Stuttgart) mittels der BW-CARD-Zertifikate erfolgen.

In Baden-Württemberg existieren bereits an einigen Universitäten Chip-Karten-Projekte, die die Realisierung des elektronischen Studentenausweises zum Ziel haben. Aufgrund der bis dato noch nicht erfolgten industriellen Standardisierung der eingesetzten Hardware, steht zu befürchten, dass nicht alle der bereits laufenden Projekte mit dem BW-CARD-Projekt in Einklang zu bringen sein werden. Es muss daher damit gerechnet werden, dass an den Hochschulen in Baden-Württemberg unterschiedliche Chip-Karten-Projekte nebeneinander existieren werden. Eine eigene Chip-Karte für Studenten gibt es derzeit an den Universitäten Freiburg (http://www.verwaltung.uni-freiburg.de/chipkarte/), Mannheim (http://www.uni-mannheim.de/rum/NAT/ecUM/), Tübingen (http://www.uni-tuebingen.de/zdv/bi/bi00/bi001v1-chip.html).

Erklärtes Ziel des BW-CARD-Projektes ist es jedoch, einheitliche Standards zur Einführung und zum Betrieb einer landesweiten PKI (Public Key Infrastructure) zu entwickeln und in den Pilotbetrieb zu gehen.

Kapitel 5

Änderungshistorie

Version	Datum	Änderungen
0.1	4.12.2000	Erster Entwurf aufgrund des Treffens vom 1.12.00
0.4	14.12.2000	Ausformulierungen
0.5	19.01.2001	Verbesserung aufgrund des Treffens vom 14.12.00
0.6	23.01.2001	Chipkarte, Abkürzungsverzeichnis, weitere kleinere Verbesserungen
0.7	30.01.2001	Verbesserung aufgrund des Treffens vom 25.1.01
0.8	12.03.2001	Verbesserung aufgrund der Universitätsrechenzentrumsleiter sowie Ausformulierung Sicherheitsstufen
0.9	30.03.2001	Ergänzungen u.a. hinsichtlich Funk-LAN, lockd, Web-Virencheck.
0.95	15.05.2001	Ergänzungen u.a. hinsichtlich lpd, Ethernet, ICMP, DSL von zu hause, Passwörter, Endnutzerempfehlungen, Anhang Sicherheitsrichtlinien.
0.96	21.05.2001	Upstream/Peering Spoofing/Broadcast ACL Beispiel im Anhang, ssh idle, Sicherheits-URL mehrerer Universitäten.
0.97	26.06.2001	Virenschutzergänzung; Verbesserungen aufgrund des Treffens vom 31.5.01, u.a. Squid, Socks, Laptop neu und ICMP Filter bei Grundschutz reduziert.
1.0	14.08.2001	Relayfestes Mail-CGI.

Anhang A

Anwenderunterstützung

A.1 Benutzerempfehlungen

Einige Empfehlungen für Endnutzer mit einer Beschreibungen von Risiken und geeigneten Maßnahmen hinsichtlich der sicheren Internetnutzung finden sich im Web unter http://www.BelWue.DE/aktivitaeten/security/empfehlungen.html.
Diese umfassen:
- Klartextpasswörter bei Telnet, FTP, POP und IMAP
- unverschlüsselte Mail
- Gefahr von Mailattachments
- Gefahr von Active-X, JavaScript und Java
- schwache/gemeinsame Passwörter
- Gefahr von Hintertüren ins geschützte LAN (Modemeinwahl z.B.)
- keine internen sicherheitsrelevanten Informationen unbedarft weitergeben
- Gefahr von ungepflegten Servern/Arbeitsplatzrechnern
- Gefahr von Software, die nicht im Quellcode vorliegt

A.2 Info über Filter der BelWü-Teilnehmer

Unter folgender URL findet man eine kurze Beschreibung der BelWü Sicherheitsmaßnahmen und deren Auswirkungen auf die Datenkommunikation:
http://www.BelWue.DE/aktivitaeten/security/filter-kurz.html.

Folgende URLs von Hochschulen in Baden-Württemberg bieten Informationen über lokale Sicherheitsmaßnahmen:

http://www.uni-freiburg.de/rz/security
http://web.urz.uni-heidelberg.de/Netzdienste/firewall

http://www.rz.uni-hohenheim.de/mitteilungen/rz-telegramm/2000/rzt00_01_07.htm
http://www.systems.uni-konstanz.de/CERT/Netz.php3
http://cert.uni-stuttgart.de/router.php

A.3 Konfigurationsempfehlung Personal Firewall

http://www-ks.rus.uni-stuttgart.de/PKB/People/Rozek/ZoneAlarm

Anhang B

Tabelle Zuordnung Risiken und Maßnahmen

Risiko Nr.	Beschreibung	Maßnahme Nr.	Beschreibung
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	1	SSH benutzen
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	2	Telnet nur ausnahmsweise
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	3	scp benutzen
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	4	FTP nur ausnahmsweise
3.2.3.1.1	Klartextpasswörter bei Telnet/FTP	72	Benutzer schulen
3.2.3.1.2	Klartextpasswörter bei POP/IMAP	5	Verschlüsseltes POP/IMAP
3.2.3.1.2	Klartextpasswörter bei POP/IMAP	72	Benutzer schulen
3.2.3.1.3	unverschlüsselte Mailinhalte	6	Mail verschlüsseln
3.2.3.1.3	unverschlüsselte Mailinhalte	72	Benutzer schulen
3.2.3.1.4	Spam-Mail und Mailrelaying	8	SMTP von außen nur auf Server
3.2.3.1.4	Spam-Mail und Mailrelaying	9	Relayfeste Mailhosts
3.2.3.1.4	Spam-Mail und Mailrelaying	10	Spam-Filter
3.2.3.1.4	Spam-Mail und Mailrelaying	11	DUL/RBL einsetzen
3.2.3.1.5	Mail-Attachment	7	Attachments prüfen
3.2.3.1.5	Mail-Attachment	72	Benutzer schulen
3.2.3.1.6	Viren	12	Virenschutz PC
3.2.3.1.6	Viren	13	Virenschutz Mailhost/Web-Proxy
3.2.3.1.7	Active-X, JavaScript u. ähnliches	15	Active-X u.ä. filtern
3.2.3.1.7	Active-X, JavaScript u. ähnliches	72	Benutzer schulen
3.2.3.1.8	Java	15	Java filtern
3.2.3.1.8	Java	72	Benutzer schulen
3.2.3.1.9	Nicht-jugendfreie Web-Inhalte	14	Webinhalte filtern
3.2.3.1.10	Squid und Socks	16	Squid/Socks am Upstream filtern
3.2.3.1.11	Newsdienst	17	Newsgruppen filtern
3.2.3.1.11	Newsdienst	18	nur wenige Newsfeeds am Upstream
3.2.3.1.12	SNMP	19	SNMP am Upstream filtern
3.2.3.1.12	SNMP	20	SNMP Passwort/Zugang
3.2.3.1.13	Portmapper	21	Portmapper am Upstream filtern
3.2.3.1.14	X11	22	X11 am Upstream filtern
3.2.3.1.15	UUCP	23	UUCP am Upstream filtern
3.2.3.1.16	R-Kommandos	24	R-Kommandos am Upstream filtern
3.2.3.1.17	NFS	25	NFS am Upstream filtern
3.2.3.1.19	syslogd	27	syslogd am Upstream filtern
3.2.3.1.20	bootp/DHCP	28	bootp am Upstream filtern
3.2.3.1.21	lpd	29	lpd am Upstream filtern
3.2.3.1.22	ntpd	30	ntpd am Upstream filtern
3.2.3.1.23	TFTP	31	TFTP am Upstream filtern
3.2.3.1.24	NeTBIOS/SMB	32	NeTBIOS am Upstream filtern
3.2.3.1.25	DNS	33	keine HINFO Records
3.2.3.1.25	DNS	34	DNSSEC prüfen
3.2.3.1.26	Multicast/Multimedia	35	Neueste Firewalls benutzen

Risiko Nr.	Beschreibung	Maßnahme Nr.	Beschreibung
3.2.3.2.1	ungepflegte Systeme/Anwendungen	57	Sicherheitspatches
3.2.3.2.1	ungepflegte Systeme/Anwendungen	58	sorgfältige CGI-Skripte
3.2.3.2.1	ungepflegte Systeme/Anwendungen	59	Server in DMZ
3.2.3.2.1	ungepflegte Systeme/Anwendungen	60	ausnahmsweise Verbindungen von außen
3.2.3.2.1	ungepflegte Systeme/Anwendungen	61	IDS System einsetzen
3.2.3.2.1	ungepflegte Systeme/Anwendungen	62	Web von außen nur auf Server
3.2.3.2.1	ungepflegte Systeme/Anwendungen	72	Benutzer schulen
3.2.3.2.2	Personal Firewall	63	Personal Firewall einsetzen
3.2.3.2.3	Software ohne Quellcode	59	Server in DMZ
3.2.3.2.3	Software ohne Quellcode	64	Opensource einsetzen
3.2.3.2.3	Software ohne Quellcode	72	Benutzer schulen
3.2.3.2.4	Unnötige Dienste	65	Unnötige Dienste sperren
3.2.3.2.5	schwache/gemeinsame Passwörter	66	Starke Passwörter
3.2.3.2.5	schwache/gemeinsame Passwörter	67	Keine Sammelaccounts
3.2.3.2.5	schwache/gemeinsame Passwörter	72	Benutzer schulen
3.2.3.3.1	(D)DoS Attacken	36	IP Spoofing sperren
3.2.3.3.1	(D)DoS Attacken	37	Source Routing sperren
3.2.3.3.1	(D)DoS Attacken	38	directed broadcast sperren
3.2.3.3.1	(D)DoS Attacken	39	*.*.*.0 und *.*.*.255 sperren
3.2.3.3.1	(D)DoS Attacken	40	ICMP/UDP Echo Reply begrenzen
3.2.3.3.1	(D)DoS Attacken	41	TCP Intercept einsetzen
3.2.3.3.2	ICMP	42	manche ICMP-Typen sperren
3.2.3.3.3	Routingprotokolle	43	sichere Routingprotokolle
3.2.3.3.3	Routingprotokolle	44	Routingprotokolle begrenzen
3.2.3.3.4	Störung des Netzwerkmanagements	siehe snmp, syslogd	
3.2.3.3.5	Ungeschützte Netzwerkverbindungen	45	Strukturierte Verkabelung
3.2.3.3.5	Ungeschützte Netzwerkverbindungen	47	Verschlüsselte Funkverbindungen
3.2.3.3.5	Ungeschützte Netzwerkverbindungen	48	Kein Einbuchen Unbefugter
3.2.3.3.6	VLAN	49	Sichere VLAN-Switches einsetzen
3.2.3.3.7	Tunnel	52	Tunnel nur ausnahmsweise
3.2.3.3.7	Tunnel	53	Tunnelpunkte routen nicht
3.2.3.3.7	Tunnel	72	Benutzer schulen
3.2.3.3.8	SDH, ATM, etc.	53	SDH etc. Endpunkte routen nicht
3.2.3.3.8	SDH, ATM, etc.	54	SDH etc. nur ausnahmsweise
3.2.3.3.8	SDH, ATM, etc.	55	SDH etc. Endpunkte nicht im LAN
3.2.3.3.9	Verschlüsselte Datenverbindungen	keine	
3.2.3.3.10	Einwahl	53	Einwahlknoten routen nicht
3.2.3.3.10	Einwahl	56	Einwahlknoten nur in DMZ
3.2.3.3.10	Einwahl	72	Benutzer schulen
3.2.3.3.11	DSL, Modem	1	SSH benutzen
3.2.3.3.11	DSL, Modem	3	scp benutzen
3.2.3.3.11	DSL, Modem	5	Verschlüsseltes POP/IMAP
3.2.3.3.11	DSL, Modem	12	Virenschutz PC
3.2.3.3.11	DSL, Modem	46	IPSec einsetzen
3.2.3.3.11	DSL, Modem	63	Personal Firewall einsetzen
3.2.3.3.11	DSL, Modem	72	Benutzer schulen
3.2.3.4.1	Unzureichender Firewall	50	Starker Firewall (statefull)
3.2.3.4.2	Blacklist (Verbotsliste)	51	Whitelist einsetzen
3.2.3.4.3	Interne Informationen	68	Benutzer schulen
3.2.3.4.4	Interne Angreifer	siehe Risiko Server	
3.2.3.4.5	Mobile Geräte (Laptop)	69	Laptop vor/hinter Firewall
3.2.3.4.6	Konsolzugang	70	Rechner in sichere Räume
3.2.3.4.7	LVN-Zugang	71	Verschlüsselter LVN-Zugang

Tabelle B.1: Zuordnung Risiken und Maßnahmen

Anhang C

Betriebshinweise für Server

Folgende Maßnahmen sollten beim Betrieb von Servern beachtet werden. Siehe hierzu auch Paragraph 3.2.3.2.1 (Ungepflegte Systeme/Anwendungen) auf Seite 19 sowie [9], [25], [11] und [12].

- IP Filter
- SSH Zugang anstelle von Telnet
- kein FTP-Zugang (Ausnahme: Anonymous FTP)
- keine Nutzeraccounts
- Accounts von ausscheidenden Hochschulmitgliedern prinzipiell umgehend deaktivieren
- Online Warnung im Banner, dass der Zugang nicht erlaubt ist (damit gefasste Hacker bei Bedarf bestraft werden können)
- Verfolgung von relevanten Sicherheitsquellen (Mail, News, Ticker)
- umgehendes Einspielen von Sicherheitspatches
- unnötige Dienste abstellen, Minimal-Betriebssystem
- Server-Prozesse unprivilegiert betreiben, wenn möglich
- kein anonyme Schreib-Benutzungsmöglichkeit von Services
- regelmäßige Integritätskontrolle des File Systems (z.B. tripwire)
- alle Services müssen Logfiles schreiben, dabei Bundesdatenschutzgesetz beachten

- Log-Dateien überwachen
- regelmäßige Backups und periodische Testrestaurationen
- postmaster@servername und andere Role Account nach RFC 2142 müssen erreichbar sein und auf Anfragen reagieren
- alle Services müssen RFC konform sein, insbesondere was Fehlermeldungen betrifft
- kompromittierte Maschinen müssen neu installiert werden
- Vertretung des System-Administrator muss geregelt sein

Anhang D

Cisco-Konfigurationsbeispiele

Siehe hierzu auch [50] und [49].

D.1 Traffic Shaping mit CAR

```
Cisco7500:
interface FastEthernet 0/0
 rate-limit input access-group 120 512000 9180 9180 conform-action transmit exceed-action drop

Cisco12400:
interface GigabitEthernet 0/0
 rate-limit input 2000000 128000 128000 conform-action transmit exceed-action drop protocol icmp echo-reply
```

D.2 TCP Intercept (SYN-Flooding Attacke)

```
ip tcp intercept acl
```

Siehe hierzu [48].

D.3 Sperren verschiedener Dienste für Router

```
no cdp run                      ! Cisco Discovery Protocol
no service tcp-small-servers    ! Echo (7), Discard (9), Daytime (13), Chargen (19), Finger (79)
no service udp-small-servers    ! Echo (7), Discard (9), Daytime (13), Chargen (19)
no ip source-route
.....
```

```
interface xx
no ip unreachables
no ip redirects
.....
```

D.4 Reflexive ACL

Hierbei ist wichtig, für Verbindungen, die länger idle sind (wie z.B. ssh) einen höheren timeout zu konfigurieren (im folgenden Beispiel "servertraffic").

```
interface Ethernet 0/0                      ! Mosbach lokal
 ip address 129.143.204.13 255.255.255.252
 description Ethernet zum RZ-Router
 no ip directed-broadcast                   ! wg. Hacker (denial of service)
 ip access-group in-filter  in              ! RZ-Router -> Welt
 ip access-group out-filter out             ! Reflexive extended Access-list
 no shutdown
!
no ip access-list extended in-filter
 ip access-list extended in-filter
!Eigene 'Reflexive IP access list' wegen dem hohen Timeout:
 permit ip  host 193.196.5.105 host 123.256.78.9 reflect servertraffic timeout 7200
 permit  ip 193.196.5.0  0.0.0.255 any reflect alltraffic
!
no ip access-list extended out-filter
 ip access-list extended out-filter
!
 permit tcp any any eq 22                           ! SSH
 permit tcp any any eq 113                          ! Ident
 permit tcp any any eq 487                          ! SAFT
!
 evaluate alltraffic                                ! temp. Loecher
 evaluate servertraffic                             ! temp. Loecher mit hohen Timeout
!
 permit tcp any gt 1023 host 193.196.5.107 eq 21    ! FTP-Commands (fuer PASV FTP)
 permit tcp any gt 1023 host 193.196.5.105 eq 21    ! FTP-Commands (fuer PASV FTP)
 permit tcp any gt 1023 host 193.196.5.105 gt 1023  ! FTP-Commands (fuer PASV FTP)
 permit tcp any gt 1023 host 193.196.5.107 gt 1023  ! FTP-Commands (fuer PASV FTP)
 permit tcp any eq 21 any gt 1023 established log   ! FTP timeout Activ-FTP
!
 permit tcp any host 193.196.5.107 eq 25            ! SMTP
 permit tcp any host 193.196.5.105 eq 25            ! SMTP
!
 permit tcp host 129.143.2.1     host 193.196.5.107 eq 53  ! DNS Zone-Transfer
 permit tcp host 129.206.100.126 host 193.196.5.107 eq 53  ! DNS Zone-Transfer
 permit tcp host 129.206.100.127 host 193.196.5.107 eq 53  ! DNS Zone-Transfer
 permit tcp host 129.143.2.1     host 193.196.5.105 eq 53  ! DNS Zone-Transfer
 permit tcp host 129.206.100.126 host 193.196.5.105 eq 53  ! DNS Zone-Transfer
 permit tcp host 129.206.100.127 host 193.196.5.105 eq 53  ! DNS Zone-Transfer
!
 permit tcp any host 193.196.5.107 eq 80            ! WWW
 permit tcp any host 193.196.5.105 eq 80            ! WWW
!
 permit tcp any host 193.196.5.107 eq 119           ! nntp
 permit tcp any host 193.196.5.105 eq 119           ! nntp
!
 permit udp any host 193.196.5.107 eq 123           ! ntp
 permit udp any host 193.196.5.105 eq 123           ! ntp
```

```
!
 permit tcp any host 193.196.5.107 eq 389            ! ldap
 permit tcp any host 193.196.5.105 eq 389            ! ldap
!
 permit tcp any host 193.196.5.107 eq 443            ! https
 permit tcp any host 193.196.5.105 eq 443            ! https
!
 permit tcp any host 193.196.5.107 eq 993            ! Secure-IMAP
 permit tcp any host 193.196.5.105 eq 993            ! Secure-IMAP
!
 permit tcp any host 193.196.5.107 eq 995            ! Secure-POP3
 permit tcp any host 193.196.5.105 eq 995            ! Secure-POP3
!
! bei geringeren Sicherheitsanforderungen:
 permit tcp any host 193.196.5.107 eq 110            ! POP3 zulassen
 permit tcp any host 193.196.5.105 eq 110            ! POP3 zulassen
 permit udp any host 193.196.5.105 eq 53             ! DNS-Anfragen
 permit udp any host 193.196.5.107 eq 53             ! DNS-Anfragen
!
 permit icmp any host 193.196.5.107     8            ! Server soll Ping-Echos geben
 permit icmp any 193.196.5.0  0.0.0.255 3 1          ! host-unreachable
 permit icmp any 193.196.5.0  0.0.0.255 3 3          ! port-unreachable
 permit icmp any 193.196.5.0  0.0.0.255 3 4          ! packet-too-big
 permit icmp any 193.196.5.0  0.0.0.255 3 13         ! administratively-prohibited
 permit icmp any 193.196.5.0  0.0.0.255 4            ! source-quench
 permit icmp any 193.196.5.0  0.0.0.255 11 0         ! ttl-exceeded
 permit tcp any any eq ssh                           ! ssh auf lokales Netz zulassen
!
 deny udp any any eq 138                             ! NeTBIOS nicht in das Logfile
 deny udp any any eq 137                             ! NeTBIOS nicht in das Logfile
!
 deny ip any any log
```

D.5 Context-Based ACL

Folgendes erfordert ein Firewall Feature Set IOS.

```
Es gibt da mehrere Moeglichkeiten CBAC (Context-Based-Access-Control) zu
konfigurieren:

a) auf dem internen interface Ethernet 0/0
b) auf dem externen interface Serial 0/0 (was ist der Theorie nach das Beste ist!)
c) auf beiden gemischt ('ACL 101 in' auf dem e0/0 und 'ACL 111 in' auf dem s0/0)

Aehnlich wie bei einer reflexiven ACL werden temporaere Loecher
fuer den Durchgang durch die Firewall 'gebohrt'.
Die Default-Timeouts werden zunaechst belassen

Moeglichkeit a):

interface Ethernet 0/0                      ! Mosbach lokal
 ip address 129.143.204.13 255.255.255.252
 description Ethernet zum RZ-Router
 no ip directed-broadcast                   ! wg. Hacker (denial of service)
 ip inspect FIWA in                         ! Ueberpruefung des IP-Verkehrs
 ip access-group 101 in                     ! Anti-Spoofing
 ip access-group 102 out                    ! zusaetzliches Welt-LAN-Filter wegen Servern
 no shutdown
!
```

```
no access-list 101
access-list 101 permit tcp  129.143.204.12 0.0.0.3   any  ! RZ-Router Anti-Spoofing
access-list 101 permit udp  129.143.204.12 0.0.0.3   any  ! RZ-Router Anti-Spoofing
access-list 101 permit icmp 129.143.204.12 0.0.0.3   any  ! RZ-Router Anti-Spoofing
access-list 101 permit tcp  193.196.5.0 0.0.0.255    any  ! Netz der BA-Mo Anti-Spoofing
access-list 101 permit udp  193.196.5.0 0.0.0.255    any  ! Netz der BA-Mo Anti-Spoofing
access-list 101 permit icmp 193.196.5.0 0.0.0.255    any  ! Netz der BA-Mo Anti-Spoofing
access-list 101 deny ip any any
!
! Zulassen von gewissen Diensten auf die Server
no access-list 102
!
access-list 102 permit tcp any any eq 22                          ! SSH
access-list 102 permit tcp any any eq 113                         ! Ident
access-list 102 permit tcp any any eq 487                         ! SAFT
!
permit tcp any gt 1023 host 193.196.5.107 eq 21                   ! FTP-Commands (fuer PASV FTP)
permit tcp any gt 1023 host 193.196.5.105 eq 21                   ! FTP-Commands (fuer PASV FTP)
!
access-list 102 permit tcp any host 193.196.5.107 eq 25           ! SMTP zulassen
access-list 102 permit tcp any host 193.196.5.105 eq 25           ! SMTP zulassen
!
access-list 102 permit tcp host 129.143.2.1     host 193.196.5.107 eq 53  ! DNS Zone-Transfer
access-list 102 permit tcp host 129.206.100.126 host 193.196.5.107 eq 53  ! DNS Zone-Transfer
access-list 102 permit tcp host 129.206.100.127 host 193.196.5.107 eq 53  ! DNS Zone-Transfer
access-list 102 permit tcp host 129.143.2.1     host 193.196.5.105 eq 53  ! DNS Zone-Transfer
access-list 102 permit tcp host 129.206.100.126 host 193.196.5.105 eq 53  ! DNS Zone-Transfer
access-list 102 permit tcp host 129.206.100.127 host 193.196.5.105 eq 53  ! DNS Zone-Transfer

access-list 102 permit permit tcp any host 193.196.5.107 eq 80    ! WWW
access-list 102 permit permit tcp any host 193.196.5.105 eq 80    ! WWW
!
access-list 102 permit tcp any host 193.196.5.107 eq 119          ! nntp
access-list 102 permit tcp any host 193.196.5.105 eq 119          ! nntp
!
access-list 102 permit udp any host 193.196.5.107 eq 123          ! ntp
access-list 102 permit udp any host 193.196.5.105 eq 123          ! ntp
!
access-list 102 permit tcp any host 193.196.5.107 eq 389          ! ldap
access-list 102 permit tcp any host 193.196.5.105 eq 389          ! ldap
!
access-list 102 permit tcp any host 193.196.5.107 eq 443          ! https
access-list 102 permit tcp any host 193.196.5.105 eq 443          ! https
!
access-list 102 permit tcp any host 193.196.5.107 eq 993          ! Secure-IMAP
access-list 102 permit tcp any host 193.196.5.105 eq 993          ! Secure-IMAP
!
access-list 102 permit tcp any host 193.196.5.107 eq 995          ! Secure-POP3
access-list 102 permit tcp any host 193.196.5.105 eq 995          ! Secure-POP3
!
! bei geringeren Sicherheitsanforderungen:
!
access-list 102 permit tcp any host 193.196.5.107 eq 110          ! POP3 zulassen
access-list 102 permit tcp any host 193.196.5.105 eq 110          ! POP3 zulassen
access-list 102 permit udp any host 193.196.5.105 eq 53           ! DNS-Anfragen
access-list 102 permit udp any host 193.196.5.107 eq 53           ! DNS-Anfragen
!
!
access-list 102 permit icmp any host 193.196.5.107  administratively-prohibited
access-list 102 permit icmp any host 193.196.5.107  echo
access-list 102 permit icmp any host 193.196.5.107  echo-reply
access-list 102 permit icmp any host 193.196.5.107  packet-too-big
access-list 102 permit icmp any host 193.196.5.107  time-exceeded
access-list 102 permit icmp any host 193.196.5.107  traceroute
access-list 102 permit icmp any host 193.196.5.107  unreachable
```

```
access-list 102 deny ip any any
!
ip inspect name FIWA http java-list 50     ! JavaScript ablehnen nach ACL 50
ip inspect name FIWA realaudio timeout 3600
ip inspect name FIWA smtp timeout 3600
ip inspect name FIWA tftp timeout 30
ip inspect name FIWA ftp  timeout 3600
ip inspect name FIWA udp  timeout 15
ip inspect name FIWA tcp  timeout 3600
!
no access-list 50
access-list 50 permit any log              ! Hier koennten IP-Adressen stehen
```

D.6 Upstream/Peering ACL

```
interface POS 10/0/0
 description Upstream/Peering Interface
 ip access-group 121 in   ! IP Spoofing (vom ISP keine BelWue Netze / priv. Adressen)
 ip access-group 122 out  ! IP Spoofing (zum ISP nur   BelWue Netze)
...

no access-list 121 ! IP Spoofing / Broadcast (vom ISP keine BelWue Netze / priv. Adressen)
access-list 121 deny ip any 0.0.0.0   255.255.255.0  ! kein directed broadcast (*.*.*.0)
access-list 121 deny ip any 0.0.0.255 255.255.255.0  ! kein directed broadcast (*.*.*.255)
access-list 121 deny ip host 255.255.255.255     any ! kein Broadcast als Source Adresse
access-list 121 deny ip 129.13.0.0 0.0.255.255   any ! Uni-Karlsruhe
...

no access-list 122 ! IP Spoofing / Broadcast (zum ISP nur BelWue Netze)
access-list 122 deny icmp any       0.0.0.0   255.255.255.0 ! kein directed broadcast (*.*.*.0)
access-list 122 deny icmp any       0.0.0.255 255.255.255.0 ! kein directed broadcast (*.*.*.255)
access-list 122 deny   ip 0.0.0.255 255.255.255.0       any ! Broadcast als Source Adresse
access-list 122 deny   ip 0.0.0.255 255.255.255.0       any ! kein Broadcast als Source Adresse
access-list 122 permit ip 129.13.0.0 0.0.255.255        any ! Uni-Karlsruhe
...
```

D.7 BGP ACL

```
! ------ Peering ISPs (Netze die nicht akzeptiert werden):
no access-list 133
access-list 133 deny   ip 0.0.0.0     0.255.255.255  255.0.0.0     0.255.255.255  ! Historischer Broadcast
access-list 133 deny   ip 10.0.0.0    0.255.255.255  255.0.0.0     0.255.255.255  ! Privater Adressbereich
access-list 133 deny   ip 127.0.0.0   0.255.255.255  255.0.0.0     0.255.255.255  ! LOOPBACK (IANA)
access-list 133 deny   ip 128.0.0.0   0.0.255.255    255.255.0.0   0.0.255.255    ! ?? (nicht vergeben)
access-list 133 deny   ip 169.254.0.0 0.0.255.255    255.255.0.0   0.0.255.255    ! IANA (link-local)
access-list 133 deny   ip 172.16.0.0  0.15.255.255   255.240.0.0   0.15.255.255   ! Privater Adressbereich
access-list 133 deny   ip 191.255.0.0 0.0.255.255    255.255.0.0   0.0.255.255    ! ?? (191/8 Not yet used)
access-list 133 deny   ip 192.0.0.0   0.0.0.255      255.255.255.0 0.0.0.255      ! IANA (NET-ROOT-NS-LAB)
access-list 133 deny   ip 192.0.2.0   0.0.0.255      255.255.255.0 0.0.0.255      ! IANA (example network)
access-list 133 deny   ip 192.168.0.0 0.0.255.255    255.255.0.0   0.0.255.255    ! Privater Adressbereich
access-list 133 deny   ip 224.0.0.0   15.255.255.255 240.0.0.0     15.255.255.255 ! Multicast Adressen
access-list 133 deny   ip 240.0.0.0   15.255.255.255 240.0.0.0     15.255.255.255 ! Reserved Class E
access-list 133 deny   ip 0.0.0.0     0.0.0.0        0.0.0.0       0.0.0.0        ! Default Route
```

```
access-list 133 permit ip any                       any
```

Siehe hierzu auch [45].

D.8 Nullrouten

```
ip route 0.0.0.0       255.0.0.0      null0 ! Historischer Broadcast
ip route 10.0.0.0      255.0.0.0      null0 ! Privater Adressbereich
ip route 127.0.0.0     255.0.0.0      null0 ! Loopbacknetz
ip route 128.0.0.0     255.255.0.0    null0 ! (nicht vergeben)
ip route 169.254.0.0   255.255.0.0    null0 ! DHCP auto-configuration address space
ip route 172.16.0.0    255.240.0.0    null0 ! Privater Adressbereich
ip route 191.255.0.0   255.255.0.0    null0 ! (nicht vergeben)
ip route 192.0.0.0     255.255.255.0  null0 ! IANA (NET-ROOT-NS-LAB)
ip route 192.0.2.0     255.255.255.0  null0 ! wg. Factory-Default 192.0.2.1
ip route 192.168.0.0   255.255.0.0    null0 ! Privater Adressbereich
ip route 223.255.255.0 255.255.255.0  null0 ! last broadcast
```

Siehe hierzu auch [45].

Anhang E

Sicherheitsrichtlinien einer Hochschule

Folgende Hinweise sollen der Erstellung einer individuellen Sicherheitsrichtlinie einer Hochschule dienen. Sie sind ein Auszug aus der "Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet" erstellt vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom September 1998 ([15]). Diese Hinweise treffen aber eher den Anschluss einer Verwaltung an das Internet; für den Anschluss einer gesamten Hochschule müssen sie entsprechend überarbeitet/reduziert werden.

E.1 Kommunikations- und Risikoanalyse

Ausgangspunkte einer derartigen Analyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle sowie die Risiken der unterschiedlichen Dienste.
In Anlehnung an die Empfehlungen des BSI-Grundschutzhandbuchs sind im Rahmen einer Risikoanalyse zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Welche Informationen sollen nicht nach außen gelangen?
- Wie können z.B. die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?

- Welche Zugänge werden benötigt (z.B. nur über einen Internet-Service-Provider)?
- Welche Datenmengen werden voraussichtlich übertragen?
- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?
- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?
- Welche Aktivitäten im Netz sollen protokolliert werden? (Dabei werden ggf. Fragen des Arbeitnehmerdatenschutzes tangiert)
- Welche Dienste sollen auf keinen Fall genutzt werden?
- Wird sichergestellt, dass nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind (was nicht erlaubt ist, ist verboten)?
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?
- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

E.2 Security Policy und Sicherheitskonzept

In Bezug auf die Firewall sollte die Security Policy folgende Festlegungen enthalten:

- Was soll geschützt werden?
- Welche Dienste sind erforderlich?
- Welche Benutzer werden zugelassen?
- Welche Ereignisse werden protokolliert und wer wertet diese Daten aus?
- Welcher Datendurchsatz ist zu erwarten?

Da die Sicherheit des Gesamtsystems nicht allein von der Firewall bestimmt wird, sind in die Security Policy auch flankierende Vorgaben aufzunehmern, wie das Verbot von zusätzlichen Netzzugängen z.B. per Modem oder ISDN, Virenschutz und Backup-Konzept.
Basierend auf der Security Policy ist ein Sicherheitskonzept zu erstellen, welches die Vorgaben in konkrete Maßnahmen (Konfigurationen, Filterregeln etc.) umsetzt.

E.3 Empfehlungen für den Betrieb einer Firewall

- Aufgrund der rechtlich unterschiedlichen Bewertung der Datenübertragung für eigene Zwecke einerseits und für Dritte andererseits sowie der damit verbundenen praktischen Konsequenzen sollte in einer Dienst- oder Betriebsvereinbarung klar geregelt werden, ob und wenn ja welche Dienste zur privaten Nutzung freigegeben sind.

- Im Hinblick darauf, dass bei behörden- und unternehmensinternen Systemen Mitbestimmungstatbestände erfüllt sind (Verhaltens- und Leistungskontrolle), müssen die Personalvertretungen und Betriebsräte schon bei der Planung und Einführung von Firewallsystemen und insbesondere der Protokollierung beteiligt werden. Gegebenenfalls müssen entsprechende Betriebs- oder Dienstvereinbarungen abgeschlossen werden, in denen das Verfahren der Protokollierung, der Kontrolle und der Auswertung der Protokolle verbindlich geregelt wird.

- Bei Datenübertragung für eigene Zwecke sind die Benutzer auf die Art und den Umfang technischer Kontrollen hinzuweisen, damit sie ihr Nutzerverhalten entsprechend steuern können; ferner müssen sie darüber informiert werden, welche Folgen es hat, wenn Nachrichten ausgefiltert werden.

- Zur Durchsetzung des Verbots einer privaten Nutzung oder des Zugriffs auf unerwünschte Adressen sollte grundsätzlich auf eine Protokollierung verzichtet werden. Die Durchsetzung des Verbots des Zugriffs auf unerwünschte Adressen sollte soweit möglich über die Sperrung solcher unerwünschter Adressen versucht und derartige Zugriffsversuche sollten protokolliert werden.

- Eine Protokollierung aller erfolgreichen, zulässigen Verbindungen ist für die Aufrechterhaltung eines ordnungsgemäßen Betriebs der Firewall nicht erforderlich; es dürfen unter den oben angeführten rechtlichen Rahmenbedingungen nur solche Verbindungen oder Verbindungsversuche aufgezeichnet werden, die einen Angriff darstellen und die zum Erkennen eines potentiellen Angriff erforderlich sind.

- Jede Protokollierung ist so auszugestalten, dass unter Wahrung des Zwecks ein datenschutzrechtlicher Mißbrauch vermieden wird, d.h.:

  - der Umfang der Protokolle sollte im Rahmen des Möglichen minimal sein,
  - Protokolle sind durch Zugriffsmaßnahmen gegen unbefugte Kenntnisnahme zu sichern,
  - es sind technisch-organisatorische Auswertungsverfahren festzulegen,
  - es sind möglichst kurze Löschfristen vorzusehen.

- Bei Inhaltskontrollen übertragener Daten (z.B. zum Zweck der Virenkontrolle) sind bereichsspezifische Regelungen und vertragliche Vereinbarungen zu beachten.
- Bei Datenübertragung für Dritte sind Inhaltskontrollen nur im Auftrag bzw. mit der Einwilligung des Betroffenen (Bei der zulässigen privaten Nutzung kommt u. U. auch eine generelle Einwilligung durch den Personal- oder Betriebsrat in Betracht. Die Betroffenen sind hierüber ausführlich zu informieren.) zulässig, wobei dem Auftraggeber (z.B. beim Outsourcing) Gestaltungsmöglichkeiten hinsichtlich folgender Aspekte einzuräumen sind:
  - Nutzung bzw. Umfang der Inhaltskontrolle,
  - technische und organisatorische Folgen bei ausgefilterten Nachrichten.
- Bei Inhaltskontrollen ist insgesamt der Eingriff in das Fernmeldegeheimnis und in das Recht auf informationelle Selbstbestimmung möglichst zu minimieren, d.h.:
  - weitgehend automatisierte Kontrolle, ohne regelmäßige Kenntnisnahme des Kontrollvorgangs oder ergebnisses durch Administratoren o.ä.,
  - Begrenzung des Inhalts-Scanning auf fest definierte Pattern (Virensignaturen) und Ausschluß des Scannings nach frei wählbaren Textstellen,
  - Aufklärung und Weiterverwendung bei gefundenen Schadnachrichten nur unter Beteiligung oder nach Rücksprache mit dem Betroffenen.

E.4 Checklisten

Im Anhang von zwei Dokumenten des Landesbeauftragten für den Datenschutz Niedersachsen (Datenschutz in Netzen [16] bzw. Grundschutz durch Firewall [17]) finden sich sehr detaillierte Checklisten hinsichtlich der technisch-organisatorischen Durchführung. Diese können durch einfaches Ankreuzen schnell zu einer Aufstellung von noch zu treffenden Maßnahmen führen.

Anhang F

Teilnehmer der Security-AG Treffen

Für das BelWü Sicherheitskonzept gab es Treffen am 1.12.00, 14.12.00, 25.1.01 und 31.5.01. An dem Papier mitgewirkt haben

Fachhochschule Albstadt-Sigmaringen	Volker Oertel
Fachhochschule Furtwangen	Claus-Peter Rohner
Fachhochschule Heilbronn	Stephan Bergfeld
Berufsakademie Karlsruhe	Johannes Freudenmann
Universität Heidelberg	Hartmuth Heldt
Universität Hohenheim	Roland Hofmann
Universität Karlsruhe	Bruno Lortz
Universität Karlsruhe	Reinhard Strebler
Universität Konstanz	Andreas Merkel
Universität Mannheim	Joachim Nerz
Universität Stuttgart	Tom Fischer
Universität Stuttgart	Igor Gilitschenski
Universität Stuttgart	Oliver Göbel
Universität Stuttgart	Lisa Golka
Universität Stuttgart	Florian Weimer
Universität Stuttgart	Boris Wesslowski
Universität Tübingen	Heinz Hipp
Universität Tübingen	Joerg Heitzenröther
Universität Ulm	Bernd Leibing
BelWü-Koordination	Dieter Copony
BelWü-Koordination	Jürgen Georgi
BelWü-Koordination	Wolfram Hellstern
BelWü-Koordination	Ulli Horlacher
BelWü-Koordination	Stefan Neuwirth
BelWü-Koordination	Peter Merdian

Literaturverzeichnis

[1] Newsgruppe Firewall (deutsch):
de.comp.security.firewall

[2] Newsgruppe Security (deutsch):
de.comp.security.misc

[3] Newsgruppe Security (englisch):
comp.security.announce

[4] Newsgruppe Security (englisch):
alt.security

[5] DFN-CERT Mailliste:
win-sec-ssc@cert.dfn.de

[6] Sicherheit im Internet:
http://www.sicherheit-im-internet.de/

[7] RUS CERT:
http://cert.uni-stuttgart.de/

[8] DFN CERT:
http://www.cert.dfn.de/

[9] The World Wide Web Security FAQ:
http://www.w3.org/Security/Faq/www-security-faq.html

[10] MITRE's Information Security Technical Center:
http://www.mitre.org/resources/centers/infosec/infosec.html

[11] How To Eliminate The Ten Most Critical Internet Security Threats - The Experts' Consensus:
http://www.sans.org/topten.htm

[12] Essential Security Actions: Step By Step. A Consensus Of the High Impact, Low Cost, Core Actions for a Program of System and Network Security:

http://www.sans.org/newlook/resources/esa.htm

Sicherheitsstudien/konzepte:

[13] RFC2196 (Site Security Handbook):
http://www.ietf.org/rfc/rfc2196.txt

[14] Zwicky/Cooper/Chapman: Building Internet Firewalls, O'Reilly, 2000

[15] Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet:
http://www.bfd.bund.de/technik/Ori_int/ohint_iv.html

[16] LFD Niedersachsen: Datenschutz in Netzen:
http://www.lfd.niedersachsen.de/dokumente/netze.pdf

[17] LFD Niedersachsen: Grundschutz durch Firewall:
http://www.lfd.niedersachsen.de/dokumente/firewall.pdf

[18] IDS-Studie von debis im Auftrag des BSI: Intrusion Detection Systeme (IDS) und Intrusion Response Systeme (IRS) (von Helden, Karsch, 1998):
http://www.bsi.de/literat/studien/ids/ids-stud.htm

[19] Sicherheit für Benutzer der Internet-Technologie (Arslan, Riekert, 1997) im Auftrag der Stabstelle für Verwaltungsreform im Innenministerium B-W:
http://www.david-datenschutz.de/secinternet.html

[20] Firewallstudie von Siemens im Auftrag des BSI: Gesicherte Verbindung von Computernetzen mit Hilfe einer Firewall (Bonnard/Wolff, 1997)
http://www.bsi.de/literat/studien/fw-stud.pdf

[21] Sicherheitskonzept Uni Karlsruhe:
http://www.rz.uni-karlsruhe.de/Uni/RZ/Netze/sicherheit.pdf

[22] BelWü-Sicherheitskonzepte (dieses Papier):
http://www.BelWue.DE/aktivitaeten/security/sicherheitskonzept

[23] BelWü/LVN-Sicherheitskonzepte (Einzelplatz-PC und LAN)

Anwendungen, Systeme:

[24] CERT UNIX Configuration Guidelines:
http://www.cert.org/tech_tips/unix_configuration_guidelines.html

[25] Incident Handling Step by Step: Unix Trojan Programs:
http://www.sans.org/y2k/DDoS.htm

[26] SSH:
http://www.employees.org/ satch/ssh/faq/ssh-faq.html

[27] SSH:
http://www.OpenSSH.com/

[28] SSH:
http://www.mindbright.se/mindterm/

[29] SSL Wrapper:
http://www.stunnel.org

[30] Relayfester Mailhost:
http://www.belwue.de/services/zentral/smtp-norelay.html

[31] Relayfestes Mail-CGI:
http://www.mailvalley.com/formmail

[32] Spamfilter:
http://www.belwue.de/wwwservices/hilfestellungen/spamblock.html

[33] RBL/DUL:
http://mail-abuse.org

[34] DNS:
http://cr.yp.to/djbdns/forgery.html

[35] Jugendfreier Web-Proxy:
http://www.belwue.de/services/zentral/wwwproxy.html

[36] Aktive Webinhalte und Schutzmöglichkeiten:
http://www.genua.de/forum/artikel/lanline/index_html

[37] Aktive Webinhalte: bunt, blinkend und gefährlich:
http://www.genua.de/forum/artikel/itbusiness/index_html

[38] Java:
http://cert.uni-stuttgart.de/ticker/article.php?mid=44

[39] Netmeeting:
http://www.shenton.org/ chris/nasa-hq/netmeeting/

[40] Portmapper:
http://www.sans.org/newlook/resources/IDFAQ/blocking.htm

[41] Ports von Trojaner:
http://www.robertgraham.com/pubs/firewall-seen.html
http://www.tu-berlin.de/www/software/avipports.shtml

[42] Passwort-Empfehlungen:
http://www.lfd.niedersachsen.de/dokumente/passwort.pdf

DDos Links:

[43] Denial of Service (DoS) Attack Resources:
http://www.denialinfo.com

[44] Distributed Attack Tools Section:
http://packetstorm.securify.com/distributed

Routing, Netzwerk:

[45] RFC2827 (Network Ingress Filtering):
http://www.ietf.org/rfc/rfc2827.txt

[46] ICMP:
http://www.sys-security.com/archive/papers/ICMP_Scanning_v2.5.pdf

[47] Funklan:
http://www.ccc.de/thema/wavelan

Cisco:

[48] TCP-Intercept:
http://www.ieng.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scdenial.htm

[49] Internet Security Advisories:
http://www.cisco.com/warp/public/707/advisory.html

[50] Top Ten Blocking Recommendations Using Cisco ACLs:
http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm

Für den Fall, dass die in diesem Literaturverzeichnis aufgeführten URLs nicht mehr erreichbar sind, finden sich für manche lokale Kopien unter http://www.BelWue.DE/aktivitaeten/security/lokale-literatur-kopien.html.

Anhang H

Verwendete Abkürzungen / Begriffe

ACL	access list
ADSM	Datenbackupsystem
Aftp	Anonymous FTP
ATM	Asynchronous Transfer Mode (Netzschicht)
BackOrifice	Fernwartungsprogramm für Windows-PCs (trojanisches Pferd von Hackern)
BelWü	Baden-Württembergs extended lan (Landeshochschulnetz)
BIND	Berkeley Internet Name Daemon
Blacklist	Verbotsliste
BSI	Bundesamt für Sicherheit in der Informationstechnik
DDoS	Distributed Denial of Service
DoS	Denial of Service
directed broadcast	Nutzung der Broadcastadresse von außerhalb
DMZ	DeMilitarized Zone
DNS	Domain Name System (System zur Zuordnung von Rechername / Rechernadre
DUL	Dial-up User List
fraggle	DoS Attacke
FTP	File Transfer Protocol (Internet Anwendungsprogramm)
FW	(die) Firewall
GRE	Tunnelprotokoll von Cisco
H.323	Multimedia Protokoll
HTTP	Hypertext Transport Protocol (Internet Protokoll)
HTTPS	Hypertext Transport Protocol mit SSL-Sicherheitstechnik (Internet Protokoll)
ICMP	Internet Control Message Protocol (Internet Protokoll)
ident	Programm zur Nutzeridentifikation
IDS	Intrusion Detection System
IIS	Microsoft Windows Internet Information Services (IIS Webserver)
IMAP	Interactive Mail Access Protocol

IOS	(Betriebssystem von Cisco-Routern)
IP	Internet Protocol (Internet Protokoll der Schicht 3)
IP Spoofing	Vortäuschung fremder IP-Adressen
IPSec	verschlüsseltes IP
IPv6	IP Version 6 (Nachfolger des derzeitigen IP)
IRC	Internet Relay Chat (Internet Anwendungsprogramm)
ISP	Internet Service Provider
LAN	Local Area Network
ldap	Lightweight Directory Access Protocol
lpr	Line PrinteR
LVN	Landesverwaltungsnetz in Baden-Württemberg
MBONE	Multicast Backbone
Multicast	Sonderform des Broadcast
MWK	Ministerium für Wissenschaft, Forschung und Kunst
NAT	Network Address Translation
NFS	Network File System
NNTP	Net(work) News Transfer Protocol
NQS	Network Queuing System
NTP	Network Time Protokoll
OLE	Object Linking and Embedding
PGP	Pretty Good Pricacy (Mail Verschlüsselungsverfahren)
POP	Post Office Protocol
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RBL	Realtime Blackhole List
rcmd	remote command
rcp	remote copy
RFC	Request for Comment (Internet Normierungspapier)
RIPE	Reseaux IP Europeenne
rlogin	remote login
rsh	remote shell
RUS	Rechenzentrum der Universität Stuttgart
RUS-CERT	RUS Computer Emergency Response Team/Stabsstelle IT-Sicherheit
RZ	Rechenzentrum
SAFT	Simple Asynchronous File Transfer
scp	secure copy
SDH	Synchronous Digital Hierarchy (Transport Netzwerk)
sendfile	Filetransfer Programm
SMTP	Simple Mail Transfer Protocol (Internet Anwendungsprogramm)
smurf	DoS Attacke
SNMP	Simple Network Management Protocol
Spam	Massenversand von (Werbe) Nachrichten per Mail oder News

SQL	Structured Query Language
SSH	secure shell
SSL	Secure Socket Layer (Internet-Sicherheitstechnik)
TCP	Transmission Control Protocol (Internet Protokoll)
TCP Syn	TCP Synchronisation
Telnet	virtuelles Terminalprogramm
TFTP	Trivial File Transfer Protocol
traffic shaping	Verkehrsbegrenzung
Upstream-ISP	ISP, der die Verbindung in das Internet (Transitverkehr) bereitstellt
UUCP	Unix To Unix Copy (Unix Übertraggungsprotokoll)
URL	Uniform Resource Locator
VLAN	Virtuelles LAN
Warez-sites	Umschlagplatz für Raubkopien
Whitelist	Erlaubnisliste
WU-FTP	FTP Programm
WWW	World Wide Web (Internet Anwendungsprogramm)
X11	graphisches Terminalsystem

Ein weiteres Glossar findet sich unter:
http://www.bfd.bund.de/technik/Ori_int/ohint_56.html#6.4

Index