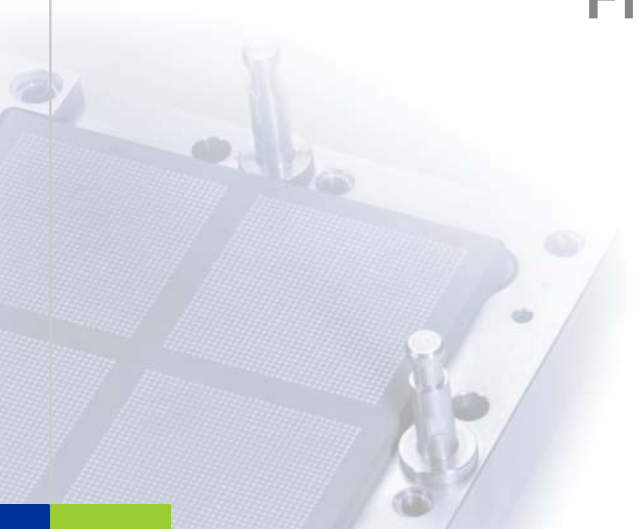
R|R|Z|N

Sicherheitstage WS 04/05

Firewallschutz für Institute

Christine Peter

22. November 2004



Zur Motivation:

R|R|Z|N

Studie von Symantec:

- Nahezu 60 Prozent aller bekannten Schwachstellen werden innerhalb eines Jahres ausgenutzt.
- Schwachstellen wandeln sich: Über 80 Prozent können von außen ausgenutzt werden.
- Schwachstellen werden immer schneller ausgenutzt: Die Zeitspanne zwischen der Bekanntmachung von Schwachstellen und ihrer Ausnutzung verkürzt sich zusehends.
- Die Schadensroutinen verändern sich. Der Trend geht weg vom bloßen Hinterlassen einer Botschaft hin zum Export von Daten.
- Zunahme von Trojanischen Pferden um 50 Prozent, die bösartigen Code oder Backdoors vornehmlich für den Export von Daten transportieren.

Zur Motivation:

R|R|Z|N

- Die Überwachung eines Testnetzes (ca. 200 Rechner) über den Zeitraum von einem Monat erbrachte folgendes Ergebnis:
  - ca. 80% der Rechner wurden attackiert.
  - Insgesamt wurden ca. 2000 Hackversuche registriert.

Typische Sicherheitsmängel in Instituten:

- Einsatz von Betriebssystemen ohne Benutzer-Administration.
- Rechner laufen ohne Betreuung.
- Rechner bieten nicht benötigte Dienste an.
- Rechner/Dienste, die nur intern verwendet werden, sind von außen zugänglich.

Dadurch besteht die Gefahr der Ausnutzung von Schwachstellen in

- Betriebssystemen,
- Anwendungssoftware oder
- Systemkonfigurationen

Das Bewusstsein für die vorhandene Gefahr wird leider oft erst durch den Eintritt eines Schadensfalles und dessen Auswirkungen geweckt:

- Rechner oder ganze Netzwerkbereiche sind u. U. für längere Zeit nicht verfügbar.
  - ➔ Dadurch können auf die Systeme angewiesene Benutzer ihre Arbeit nicht erledigen.
- Daten können entwendet oder gelöscht werden.
  - ➔ Dadurch kann die Arbeit von Monaten zerstört werden.
- Die Rechner oder die gewonnenen Daten können missbraucht werden.
  - ➔ Dies kann unter anderem zu einer Schädigung des Rufes der Universität führen.
- Es ist viel Arbeitszeit notwendig, um die entstandenen Probleme zu beheben.
- Die entstandenen Schäden und der Arbeitszeitverlust sind oft erheblich und schwer in Zahlen zu messen.

Zur Motivation:

R|R|Z|N

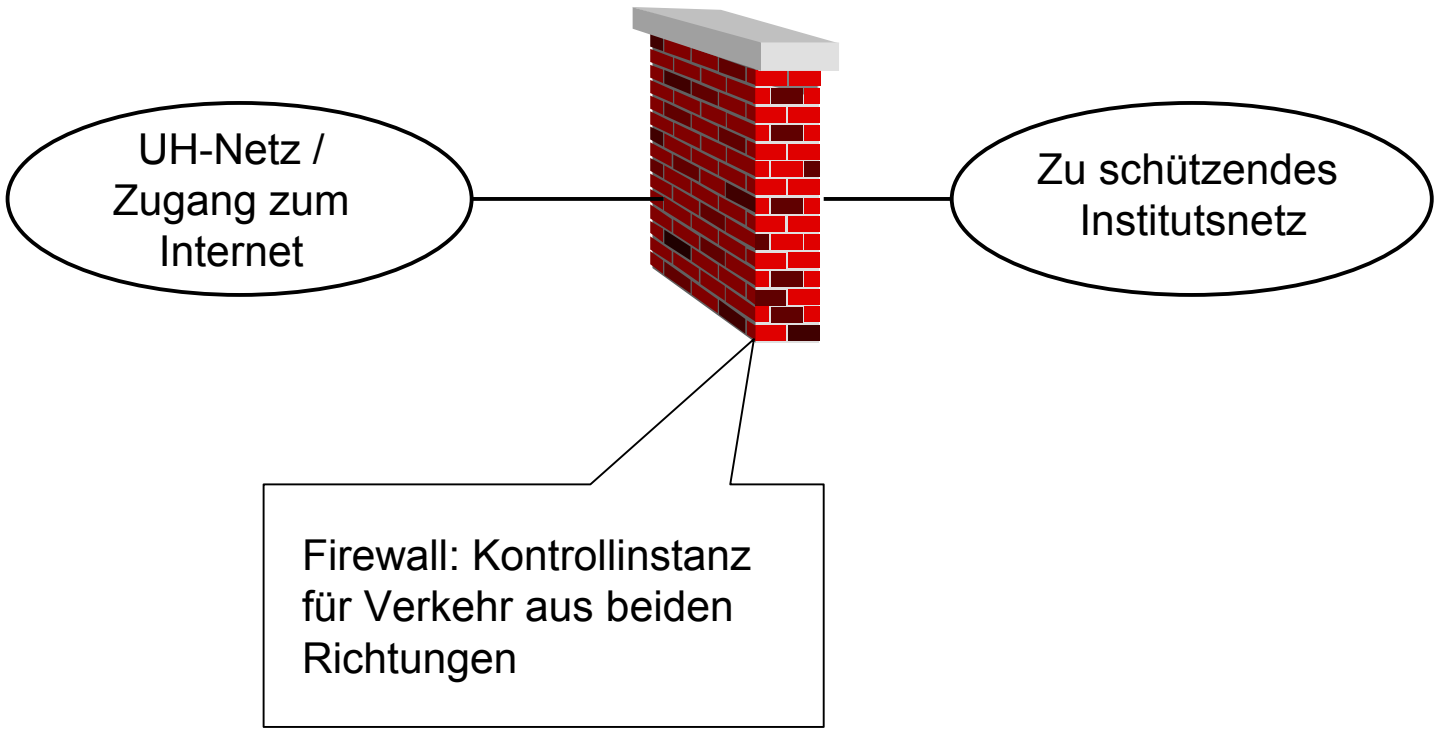
Abhilfe und Schutz ist unter Anderem möglich durch den

Einsatz von Firewall-Technik:

- Eine Firewall trennt das Netzwerk mit den zu schützenden Systemen von der Außenwelt.

- Eine Firewall kann Kommunikationsverbindungen erlauben und ablehnen.

Eigenschaften einer Firewall



Eigenschaften einer Firewall

R|R|Z|N

- **Jeglicher Datenverkehr:**
  - alle Zugriffe der geschützten Systeme nach außen
  - alle Zugriffe von außen auf eines der geschützten Systeme

  läuft durch die Firewall.

- **Dabei wird jedes einzelne Datenpaket untersucht und auf Zulässigkeit überprüft:**
  - IP-Adresse des Absenders (von wem kommt das Paket?)
  - IP-Adresse des Empfängers (wohin soll das Paket?)
  - Protokoll-Art IP, TCP, UDP, ICMP;
  - Ziel-Port-Nummer: welcher Netzwerk-Dienst soll angesprochen werden?
  - gehört das Paket zu einer bereits bestehenden Verbindung (stateful inspection) oder soll eine neue Verbindung eröffnen werden?

Eine Firewall

- **schützt eine Gruppe organisatorisch zusammengehörender Rechner vor**
  - Angreifern aus dem Internet
  - Angreifern aus dem restlichen Intranet.
- **Ebenso:**
  - Die Firewall begrenzt schädliche Zugriffe und die Verbreitung von Viren, Würmern usw. aus dem geschützten Abschnitt heraus.
  - Ein bestehendes Sicherheitsproblem bleibt somit „eingekesselt“und greift nicht auf andere Bereiche über.

Eine Firewall

- ist entweder eine spezielle Hardware
- oder ein dedizierter Rechner, der besonders für diese Aufgabe konfiguriert ist.

Eine Firewall übt neben ihrer Tätigkeit als Firewall keine weiteren „Nebentätigkeiten“ aus.

Eine Firewall sollte unbedingt so konfiguriert werden, dass sie nach der

„Default-Deny“- Maxime

arbeitet:

- Alle Pakete, die nicht durch eine spezielle Regel erlaubt sind, sind automatisch verboten:
  - Ob ankommende Verbindungen von der Firewall erlaubt oder verboten werden, ist durch einen Satz individuell bestimmter Regeln festgelegt.
  - Für jede ankommende Verbindung wird der Regelsatz sukzessive abgearbeitet, ob eine Regel passt.
  - Alle Verbindungen, für die im Regelsatz keine „passende“ Regel gefunden wird, gelten als prinzipiell unerwünscht und werden abgeblockt .
- Die Regeln sind verbindlich für das gesamte Institutsnetz und alle angeschlossenen Rechner.

Nachteile einer Firewall

R|R|Z|N

- **Die Einrichtung einer Firewall mit allen begleitenden Maßnahmen verursacht zunächst einmal Arbeit und kostet Zeit.**
  - Mittelfristig sollte für Sie und die Mitarbeiter am Institut dadurch aber die Arbeit weniger werden.
- **Der Datenverkehr wird kategorisiert, bewertet und reglementiert:**
  - D.h. eventuell auch als kritisch oder unnötig eingeschätzt und verboten.
  - Dadurch sind manche liebgewonnenen Zugriffe nicht mehr möglich.
- **Bei neuen Anforderungen an den Datenverkehr muss erst die Policy geändert werden. Das erfordert manchmal Zeit und gute Argumente.**
- **Eine Firewall kann ein trügerisches Gefühl von Sicherheit erzeugen. Dies kann zu weniger vorsichtigem oder gar leichtsinnigem Anwenderverhalten führen:**
  - Downloadverhalten
  - Umgang mit Mails
  - Aktualisierung der AV-Software
  - Patchen der Systeme

Nachteile einer Firewall

R|R|Z|N

- **Eine Firewall kann nicht alle Risiken ausschalten.**
- **Sie bietet keinerlei Schutz vor „importierten“ Angriffen!**
  - Gefahr durch E-Mail-Attachments.
  - Gefahr beim „Surfen“ durch „aktive“ Web-Inhalte und unkontrollierte Downloads.

  ➔ Die Firewall kann keine Aktivitäten verhindern, die **scheinbar legal** auf erlaubten Wegen ausgeführt werden!

  ➔ Die Disziplin der Anwender ist ein ganz wichtiger Sicherheits-Faktor.

  - Das Firewall-System kann Sie nur vor Rechnern vor der Firewall schützen, nicht aber vor den Geräten am eigenen Institut.

  ➔ Wird ein Rechner kompromittiert oder schleppt ein Benutzer einen Wurm in den Institutsbereich ein, sind trotz der Firewall alle Systeme gefährdet.

  ➔ Sie müssen also weiterhin für die Sicherheit der Einzelsysteme sorgen.

- **Für den Einsatz von Firewall-Systemen gibt es mehrere Realisierungsmöglichkeiten:**
  - **flächendeckender Einsatz von Personal Firewalls ???**
  - Firewall-System im Institut
  - zentraler Netzschutz: Firewall-System im RRZN

Personal Firewall als Alternative?

R|R|Z|N

- **Personal Firewalls als Schutz für ein Institutsnetz führen oft nicht zu einem Mehr an Sicherheit :**
  - Ohne eine sehr sorgfältige Konfiguration der Personal Firewall erhält der Anwender so viele Warnmeldungen, dass ernstzunehmende Alarme nicht mehr wahrgenommen werden.
  - Oft wird die Firewall-Funktion kurzerhand abgeschaltet, wenn sie gewünschte Verbindungen nicht zustande kommen lässt.
  - ➔ Sicherheit und Einhaltung der Sicherheits-Policy hängen u.U. am einzelnen Nutzer.
  - Ein trügerisches Sicherheitsgefühl beeinflusst eventuell das Anwenderverhalten.
  - Nötige Aktualisierungen unterbleiben oft, da der durch den Einsatz vieler Personal Firewalls erhöhte Betreuungsaufwand nicht geleistet werden kann.

Personal Firewall als Alternative?

R|R|Z|N

- **Prinzipielle „systembedingte“ Mängel der Personal-Firewall-Strategie :**
  - Personal Firewalls können durch manche Schadsoftware außer Betrieb gesetzt werden -und gaukeln oft noch angeblich einwandfreien Betrieb vor.
  - Ist das Betriebssystem erst korrumpiert, ist auch die beste Personal Firewall nur Makulatur.
  - ➔ Das kann bei einer dedizierten Firewall nicht passieren, da Firewallsoftware und Schadprogramm auf unterschiedlichen Geräten laufen.
  - Verkehr der eigentlich nur innerhalb des Subnetzes erlaubt sein soll, **ist dann auch generell erlaubt**. Mit einer dedizierten FW-Lösung kann dieser Verkehr nach außen abgeblockt werden.
  - **Personal Firewalls schützten nicht das Netz, sondern nur einzelne Rechner.**

Fazit:

- Zur Sicherung eines Institutsnetzes **nicht** geeignet.
- Eine dedizierte Firewall, die betreut und überwacht wird, bringt eine höhere Sicherheit.
- Höchstens als Sofortmaßnahme im akuten Notfall geeignet („besser als nichts“).
- Als zusätzliche, interne Sicherung zu bestehendem Firewall-System empfehlenswert.
- Gut geeignet für häusliche PCs.

Personal Firewall als Alternative?

R|R|Z|N

Eine Überlegung wert: **Erweiterung der Instituts-Security-Policy:**

- Personal Firewalls als zusätzlichen Schutz auf jedem Rechner.
- Personal Firewalls gibt es als
  - zusätzliche, kostenpflichtige oder auch frei erhältliche Software
  - im System bereits integrierte Software z.B.
    - Windows-XP-Firewall (eher nicht empfehlenswert…)
    - Iptables bei Linux
- Empfohlen: Professionelle Versionen mit zentraler Administration verwenden, damit die Regeln institutsweit unter Kontrolle sind.

Personal Firewall als Alternative?

R|R|Z|N

Auf alle Fälle dringend angeraten:

- **Personal Firewalls auf Laptops**
- **Über Laptops wird Schadsoftware oft auf dem „Schleichweg“ an der Firewall und den Firewallregeln vorbei ins Institutsnetz eingeschleust.**

- **Für den Einsatz von Firewall-Systemen gibt es mehrere Realisierungsmöglichkeiten:**
  - flächendeckender Einsatz von Personal Firewalls ???
  - **Firewall-System im Institut**
  - zentraler Netzschutz: Firewall-System im RRZN

Eigenes Firewall-System im Institut:

R|R|Z|N

- **Viele unterschiedliche Firewall-Systeme:**
  - Proprietäre Hardware/Software, beispielsweise
    - Router mit Firewall Feature Set (Cisco)
    - PIX-Firewall (Cisco)
  - Standard-Hardware mit Firewall-Software, beispielsweise
    - Linux-PC mit Linux-FW-Software (iptables)
    - Solaris-WS oder PC mit Firewall-Software von Checkpoint

    ...

Eigenes Firewall-System im Institut:

R|R|Z|N

- **Eine ganz eigene Lösung in alleiniger Instituts-Regie:**
  - Sie haben die freie Wahl bei allen Komponenten.
  - Das Institut ist nach Organisation des Anschlusses der Firewall an das UH-Netz unabhängig vom RRZN.

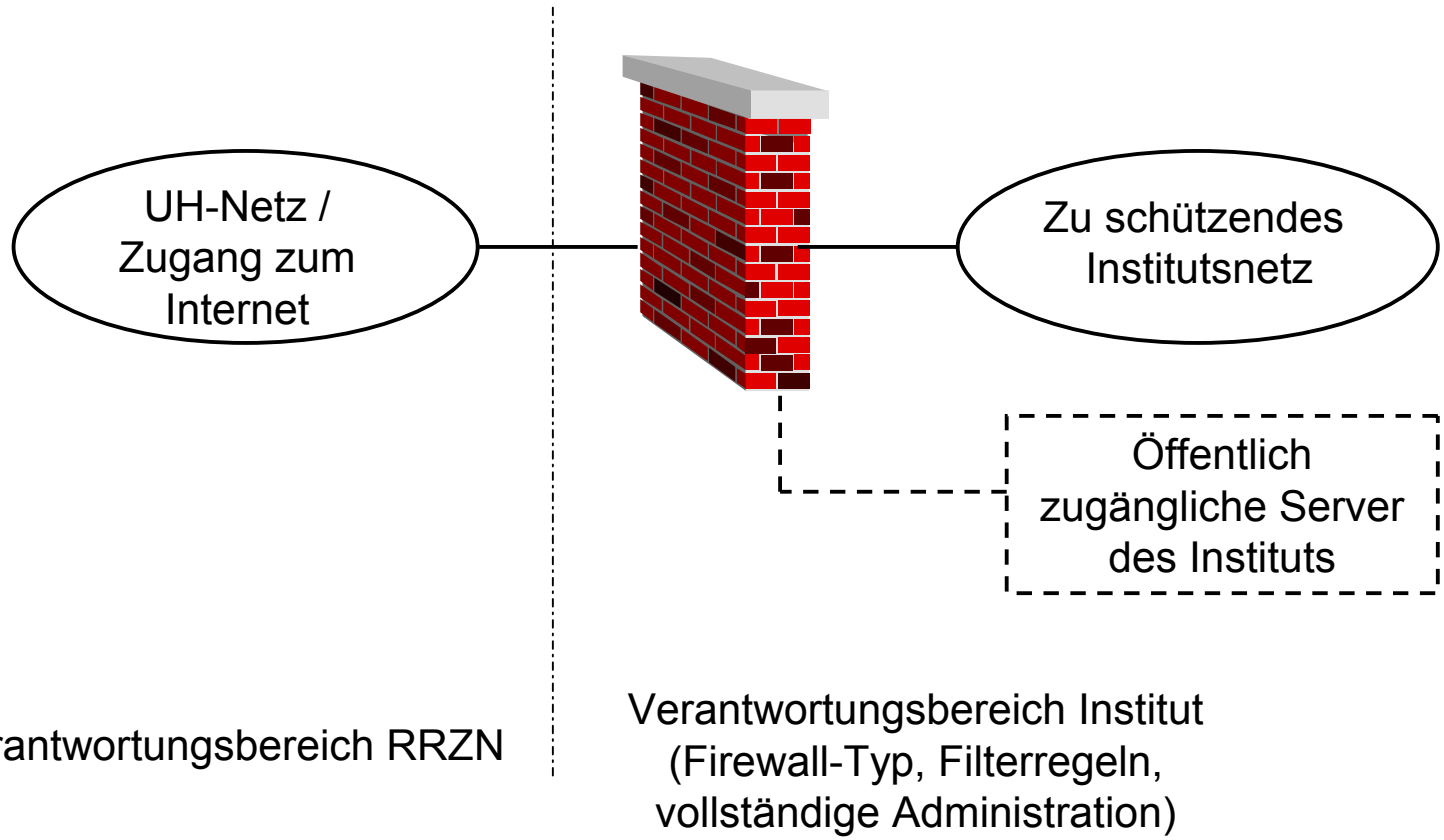
    Ansprechpartner für Anschluss am Switch: netz@rrzn.uni-hannover.de oder Herr Klinger, Tel 5130; klinger@rrzn.uni-hannover.de
- **Eine eigene Firewall, die vom Institut selbstständig konfiguriert und administriert wird,**
  - jedoch mit Soft / Hardwarekomponenten, zu denen im RRZN Know-How vorhanden ist (Suse-Linux, CISCO PIX).
  - Dadurch sind, wenn auch eingeschränkt, Unterstützungsmöglichkeiten durch das RRZN vorhanden.

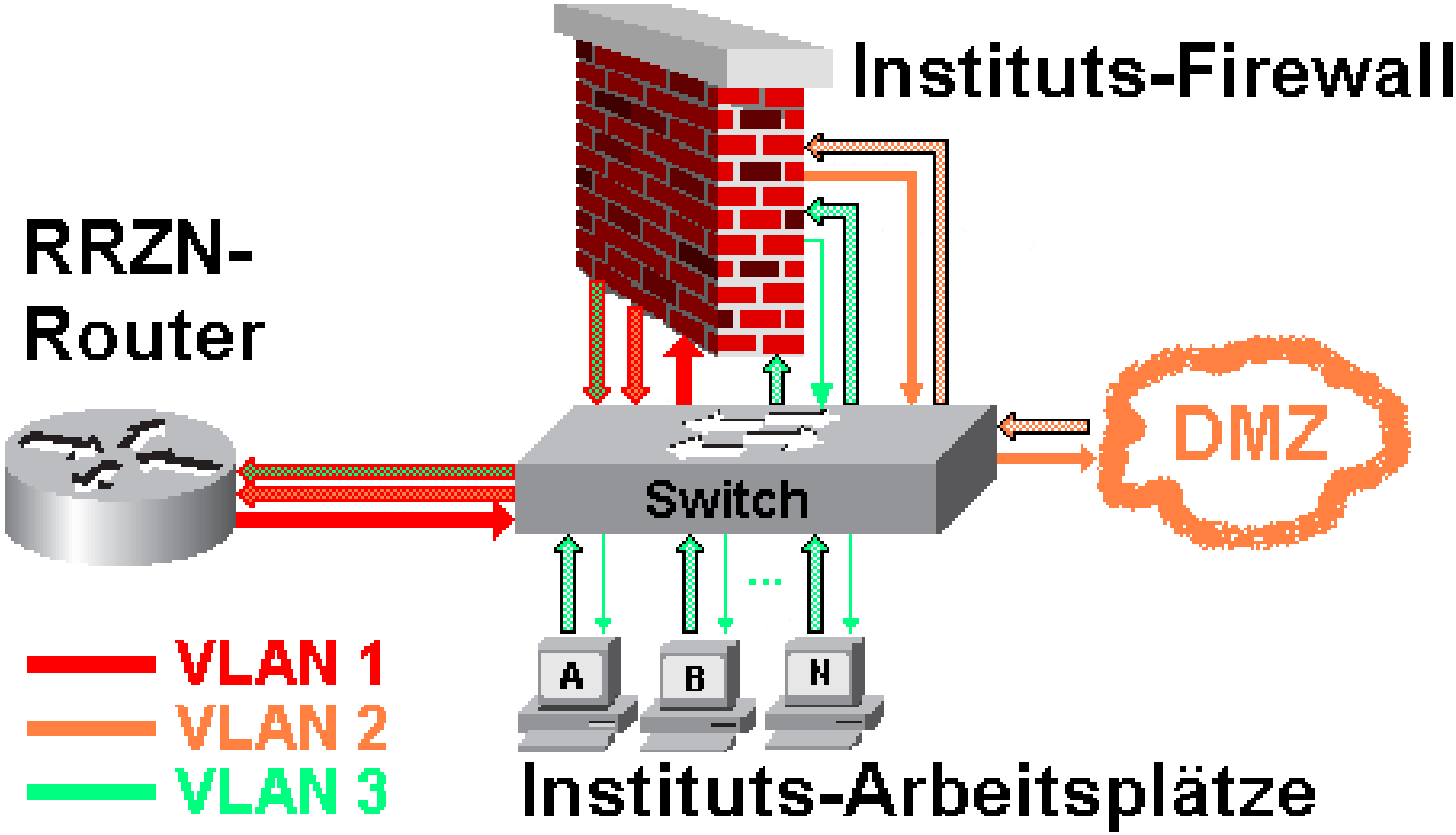
Eigenes Firewall-System im Institut:

R|R|Z|N

- **Lösung „Dr. Paul“**
  - Firewall auf der Basis von Debian-Linux und iptables
  - durch Herrn Dr. Paul sehr gut vorbereitete Lösung
  - Realisation dieser Lösung in alleiniger Instituts-Regie
  - Workshop „ Ein transparenter Firewall“ im RRZN / Ausbildungsraum am 16.12.2004 von 9.00 -16.00 Uhr.
  - Dozent: Herr Dr. Paul
  - Anmeldung:
    - per E-Mail an **peter@rrzn.uni-hannover.de**
  - Webseite mit weiteren Informationen und einer guten Beschreibung des Verfahrens: **https://cip13.amp.uni-hannover.de/FWKurs/**

Eigenes Firewall-System im Institut:




Instituts-Firewall
RRZN-
Router
DMZ
Switch
A
B
N
VLAN 1
VLAN 2
VLAN 3
Instituts-Arbeitsplätze

- **Für den Einsatz von Firewall-Systemen gibt es mehrere Realisierungsmöglichkeiten:**
  - flächendeckender Einsatz von Personal Firewalls ???
  - Firewall-System im Institut
  - **zentraler Netzschutz: Firewall-System im RRZN**

Zentraler Netzschutz durch RRZN

R|R|Z|N

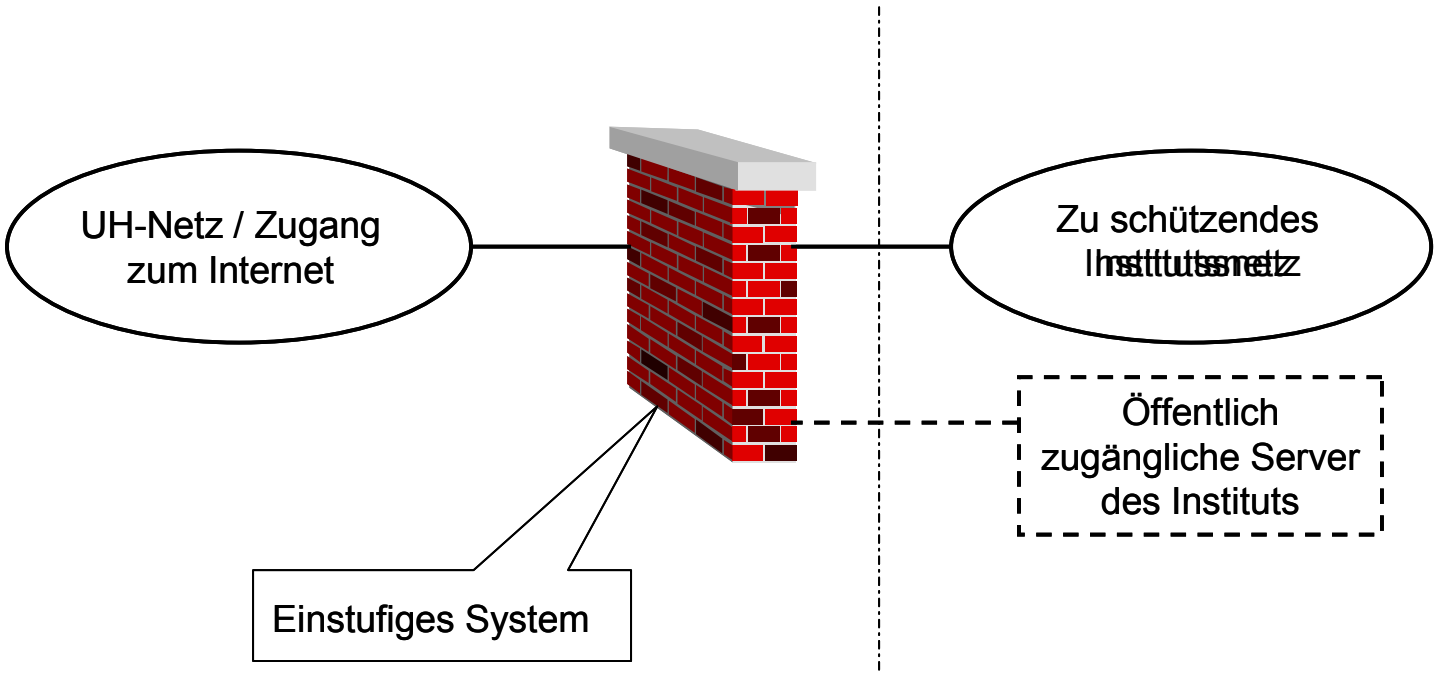
Das RRZN betreibt ein einstufiges Firewall-System.

Institute können sich hinter dieses Firewall-System schalten lassen.

- Das Institut definiert seine Anforderungen.
- Im gemeinsamen Gespräch zwischen Institut und RRZN wird eine Sicherheitspolicy für das Institut erarbeitet.
- Das RRZN überträgt die Ergebnisse in Firewall-Regeln.
- Das RRZN administriert die Geräte.
- Das RRZN trägt Änderungen ein.
- Das RRZN stellt die Logdaten zur Verfügung.
- Das Institut ist verantwortlich für die Abholung der Log-Daten und deren Kontrolle.

Dieser Service ist kostenlos für Institute der UH.

Zentraler Netzschutz durch RRZN



Betreibt man ein Firewall-System, ist kontinuierliche Pflege erforderlich:

- **Im Laufe der Zeit müssen die Firewall-Regeln verändert, weiterentwickelt und an geänderte Verhältnisse und Anforderungen angepasst werden:**
  - Regelsatz muss „widerspruchsfrei“ sein.
  - Auf die korrekte Reihenfolge muss geachtet werden.
- **Firewall-Software muss aktuell gehalten werden:**
  - regelmäßiges Einspielen von Patchen und neuen Versionen, damit das Firewall-System nicht anfällig für Sicherheitsprobleme wird.
- **Die Arbeit des Firewall-Systems muss kontinuierlich überwacht werden,**
  - um sein Funktionieren sicherzustellen und
  - um ungewöhnliche Ereignisse zu bemerken, die z.B. auf einen Einbruch in das Firewall-System selbst hindeuten können.
- **Eine regelmäßige (tägliche!) Log-Analyse ist erforderlich.**

Ohne kontinuierliche Pflege kann ein Firewall-System seine Schutzwirkung verlieren!!

- **noch einmal der Hinweis auf die Wichtigkeit der Beschäftigung mit den Log-Daten:**
  - Nur durch regelmäßige Sichtung der Logdaten können Unregelmäßigkeiten rechtzeitig erkannt werden.
  - Auch wenn sich „nichts“ tut: nur durch regelmäßige Beschäftigung mit den Logdaten bekommt man ein Gespür für den „normalen“ Verkehr.

Argumente für ein eigenes Firewall-System am Institut:

- Sie bestimmen selbst, mit welcher Hard- und Software Sie arbeiten.
- Sie sind unabhängig vom RRZN.

Argumente für die zentrale RRZN - Lösung:

- Das RRZN betreibt die Firewall für Sie, ohne dass für Sie finanzielle Kosten entstehen.
- Die professionelle, regelmäßige Betreuung der Firewall wird durch das RRZN sichergestellt.
- Es sind an Ihrer Organisationseinheit keine zusätzlichen personellen Ressourcen notwendig.
- Die nicht vorhandene Nachfolger-Problematik.

Vergleich der Alternativen

R|R|Z|N

	FWS im Institut	Zentraler Netzschutz
Schutzniveau	■ Grundschutz oder höher	■ Grundschutz
Firewallsystem	■ Auswahl d. Instituts	■ „RRZN-Standard“
Vorteile	■ Schutz individueller ■ flexibler bei Änderungen	■ Aufwand für Institut geringer ■ Kostenlos ■ keine Nachfolgerproblematik
Nachteile	■ Know-How erforderlich ■ bei Problemen ist man weitgehend auf sich gestellt ■ Administrationsaufwand ■ finanzieller Aufwand ■ „Nachfolgerproblem“	■ Änderungen: mit Zeitverzögerung ■ momentan keine DMZ möglich

Zentraler RRZN-Netzschutz:

R|R|Z|N

- **Verfahrensablauf in vier Phasen:**
  - Vorbereitungsphase
  - Testphase
  - Produktionsphase
  - Nachbearbeitung

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

Vorbereitende Tätigkeiten im Institut:

- **Für den Firewallbetrieb müssen Sie zuerst bei sich im Institut eine „Verkehrsanalyse“ betreiben:**
  - Identifizierung der Server-Systeme: auf welche Systeme muss überhaupt ein Zugriff von außerhalb des Institutes möglich sein.
  - Welche Applikationen laufen und welche Dienste werden angeboten.
  - Identifizierung der Ports, auf die ein Zugriff erlaubt werden muss.
- **Bei Instituten mit sehr unterschiedlichen internen Strukturen kann es unter Umständen auch möglich sein, dass nur bestimmte Gruppen die Firewall verwenden.**
- **Eine Umstrukturierung bei der Vergabe von IP-Adressen kann notwendig werden.**

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- **Für jedes Institut - beziehungsweise gegebenenfalls für den entsprechenden Teilbereich - müssen ein(e) „Netzschutz-Ansprechpartner(in) und eine Vertretung benannt werden.**
  - Nur diese erhalten Auskünfte über die Firewallkonfiguration und Dokumente / Dateien mit institutsinternen, eventuell vertraulichen Daten wie z.B.:
    - momentan aktive ACL
    - Logdaten.
  - Nur von diesen nimmt das RRZN Wünsche für Änderungen am Regelwerk entgegen (nur schriftlich!).
- **Benutzer müssen informiert und ev. befragt werden .**
- **Wünschenswert: Schulung der Benutzer.**

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- **Aufstellung der Anforderungen an das zukünftige Regelwerk :**
  - welche Dienste / Protokolle / Ports
  - zwischen welchen IPs / IP-Bereichen
  - in welcher Richtung

  sollen erlaubt/verboten sein.
- **Für den Log-Daten-Transfer :**
  - **Noch:** Bereitstellung eines Accounts auf einem Ihrer Rechner, damit Ihnen per ssh die Logdaten „zugestellt“ werden können.
  - **Alternativ:** Selbstabholung der Logdaten von einem Logserver im RRZN. Diese Alternative soll „RRZN-Standard“ werden.

Mustertabelle für Policy (1)

R|R|Z|N

Filter für Routereinstellungen für das Subnetz 130.75.xx (Domainkürzel)

Zugriffe von Innen:

	Dienst	Port	Quell-IP - „innen“	Ziel-IP - „außen“	Zweck
1	Mail:SMTP	25	IP des Mail-Servers	Mail-Server RRZN	Institutseigener Mailserver sendet Mail über RRZN
2	Mail: pop	110	Alle	Mailserver RRZN und 130.75.176.2	falls kein institutseigener Mailserver vorhanden ist 130.75.176.2 = studserv
3	Mail: imap	143	Alle	Mailserver RRZN und 130.75.176.2	
4	SSH	22	Alle	Alle	
5	HTTP	80	Alle	Alle	
6	HTTPS	443	Alle	Alle	
7	tcp/nntp	119	Alle	Newsserver RRZN	News
8	udp/ntp	123	Alle	Ntp-Server RRZN	Zeitsynchronisation
9	ICMP		Alle		echo, echo request
	FTP	21	Alle	Alle	
10	DNS	53	Alle	DNS-Server RRZN	
11	TCP	3299	IP des SAP-Gerätes	SAP-Server	SAP-Zugriff
12	TCP		alle? spezielle IPs	Lizenzserver RRZN	
13					

Mustertabelle für Policy (2)

R|R|Z|N

Zugriffe von Außen:

	Dienst	Port	Quell-IP - „außen“	Ziel-IP - „innen“	Zweck
1	Mail : Pop3/Imap	110/ 143	alle	IP des Mailservers	Mail abholen vom Instituts-Mailserver
2	Mail/ident	25/113	Mail-Server RRZN	IP des Mailservers	RRZN sendet Mail an Instituts-Mailserver
3	SSH	22	Alle	IP des SSH-Servers	Zugriff auf SSH-Server
4	FTP	21	Alle	IP des FTP-Servers	Zugriff auf FTP-Server
5	HTTP	80	Alle	IP des WWW-Servers	
6	HTTPS	443	Alle	IP des WWW-Servers	
7	eventuelle Dienste, die angeboten werden	???	Alle?	IP des Servers, der den Dienst anbietet	z.B. eigener News-Server, DNS-Server
8	tcp		Asterix	Instituts-IPs	Backup
9	tcp	6000 bis 6063	Anwendungsserver RRZN	keine ? alle ? spezielle Ips ?	für Zugriffe auf spezielle Software auf RRZN-Rechnern (Maple, Patran, Abaqus .....)
10					

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- **Vorbereitende Tätigkeiten im RRZN:**
  - Vorbereitende Umstellung der Netzwerkkonfiguration (ca. 1-4 Wochen).
  - Erstellung Access-Listen (2-3 Tage).
  - Bereitstellung eines Accounts auf dem Logdaten-Server des RRZN.

zum Aufbau der Access-Listen:

- Die ACL besteht aus einer Liste von Regeln.
- Diese Regeln erlauben / verbieten die vom Institut gewünschten und benötigten Zugriffe.
- Abschließend folgt die sogenannte

  Cleanup-Regel:

  - Alle anderen Zugriffsversuche werden verboten, d.h. jeglicher Datenverkehr, auf den nicht eine der vorherigen Regeln Anwendung fand, wird durch diese Regel blockiert.

Zentraler RRZN-Netzschutz: Testbetrieb

R|R|Z|N

Allgemeiner Hinweis:

- Während des Testbetriebs kann unter Umständen ein erhöhter zeitlicher Einsatz von Seiten des Institutes notwendig sein.
- Der Termin des Eintritts in die Testphase sollte deshalb sorgfältig gewählt werden, so dass beide Seiten die nötige Zeit aufbringen können.

Zentraler RRZN-Netzschutz: Testbetrieb

R|R|Z|N

- **Der Institutsverkehr wird umgeleitet und läuft nun über die Firewall:**
  - Dies erfolgt nach gegenseitiger terminlicher Absprache.
  - Die Benutzer im Institut müssen informiert werden, da es durch die Umleitung auf jeden Fall zum Abbruch aktiver Verbindungen kommt.
- **Die ACLs sind nun aktiv, aber noch nicht scharf, d.h.:**
  - Die einzelnen Firewall-Regeln der ACL greifen schon.
  - Einzig die Cleanup-Regel steht noch „auf Durchzug“, d.h. der „ungeregelte Rest-Verkehr“ der später verboten sein wird, wird momentan noch erlaubt, jedoch zur Analyse mitgeloggt.

Auszug aus Router-ACL outbound (1)

R|R|Z|N

```
permit tcp 130.75.XXX.0 0.0.0.255 any eq ftp
...   (telnet, ssh, http, https, ...)
remark kein institutseigner Mailserver
permit tcp 130.75.XXX.0  0.0.0.255 host IP RRZN Mailserver eq smtp
permit tcp 130.75.XXX.0  0.0.0.255 host IP RRZN Mailserver eq pop3
permit tcp 130.75.XXX.0  0.0.0.255 host IP RRZN Mailserver eq 143
remark institutseigner Mailserver
permit tcp host IP Mailserver Institut host IP RRZN Mailserver eq smtp
permit tcp 130.75.XXX.0  0.0.0.255 host IP Stud-Serv eq pop3
permit tcp 130.75.XXX.0  0.0.0.255 host IP Stud-Serv  eq 143
deny tcp any any eq smtp
… (pop3, imap)
permit tcp host 130.75.XXX.xxx   IPs SAP-Server eq SAP-Port
```

Auszug aus Router-ACL outbound (2)

R|R|Z|N

```
deny tcp 130.75.XXX.0  0.0.0.255  any eq 1214
deny tcp 130.75.XXX.0  0.0.0.255  any eq 445
deny udp 130.75.XXX.0  0.0.0.255  any eq netbios-ns
deny udp 130.75.XXX.0  0.0.0.255  any eq netbios-dgm

...
deny udp 130.75.XXX.0  0.0.0.255  any eq 1214

...
permit icmp 130.75.XXX.0  0.0.0.255  any echo
permit icmp 130.75.XXX.0  0.0.0.255  any traceroute

...
remark deny ip any  any log-input
permit ip any  any log-input
```

Auszug aus FW-ACL outbound (1)

R|R|Z|N

```
access-list inside_access_in   deny tcp any any object-group WinFS-TCP-SG
 …
access-list inside_access_in   permit tcp any host mgate6 object-group Mailuser-send-empf-SG
 access-list inside_access_in   permit tcp any host studserv object-group Mailuser-empf-SG
access-list inside_access_in   permit tcp any any object-group TCP-allgemein-SG
access-list inside_access_in   permit tcp object-group SAP-PCs-HG SAP-Sever-HG eq SAP-Port
access-list inside_access_in   permit tcp object-group Asterix-Sicherung-HG host asterix
…
access-list inside_access_in remark verbiete Kazaa-tcp
access-list inside_access_in   deny tcp any  any eq 1214
access-list inside_access_in   deny tcp any  any object-group Mailuser-send-empf-SG
```

Auszug aus FW-ACL outbound (2)

R|R|Z|N

```
access-list inside_access_in   permit tcp any gt 1024 any lt 1025 log
access-list inside_access_in   permit tcp any gt 1024 any log
…
access-list inside_access_in   deny tcp any  any log
access-list inside_access_in   permit udp any object-group DNS-HG eq domain
access-list inside_access_in   deny udp any  any object-group WinFS-UDP-SG
…
access-list inside_access_in remark verbiete Kazaa-udp
access-list inside_access_in   deny udp any  any eq 1214
access-list inside_access_in   deny udp any  any log
…
access-list inside_access_in   permit icmp any  any echo
access-list inside_access_in   permit icmp any  any traceroute
…
access-list inside_access_in   deny ip any  any log
```

Zentraler RRZN-Netzschutz: Testbetrieb

R|R|Z|N

Nun folgt der zweite für das Institut relative arbeitsintensive Abschnitt:

- **Die anfallenden Logdaten müssen sorgfältig durchsucht werden:**
  - Welche Verbindungen sind noch zu erlauben.
  - Welche Verbindungen sind noch explizit zu verbieten (zur Verminderung das Logdatenaufkommens).
- **Aus den Ergebnissen dieser Analysen ergeben sich neue Regeln für die ACLs.**
- **Diese neuen Regeln pflegt das RRZN auf Anforderung von Ihnen im Firewall-System ein.**

Zentraler RRZN-Netzschutz: Produktion

R|R|Z|N

- **Nach Abschluss dieser Phase wird „in Produktion“ gegangen:**
  - Die Cleanup-Regeln werden scharf geschaltet, d.h auf „deny“ gesetzt.
  - Auch die Scharfschaltung erfolgt nach gegenseitiger Absprache.
  - Bitte auch hiervon die Benutzer vorher informieren:
    - Falls Probleme auftauchen, sollten die Benutzer wissen, dass es an der Firewall liegen *kann*.

Zentraler RRZN-Netzschutz: Nachbearbeitung

R|R|Z|N

- **Eventuell nicht mehr funktionierende Anwendungen werden auf Zusammenhang mit der Scharfschaltung der Firewall untersucht.**
- **Um nicht funktionierende Zugriffe in den Logdaten finden zu können, benötigen wir in Ihrer Meldung folgende Daten:**
  - Zugriffszeitpunkt
  - IP des (ausführenden) Rechners
  - nicht funktionierende Anwendung/Dienst
  - wenn möglich die IP des Zielsystems

Sicherheit kann nicht ohne sicherheitsbewusstes Verhalten der Anwender erreicht werden!

Verhaltensempfehlungen für Anwender erforderlich, z. B.

- zum Passwortgebrauch
- zu Einsatz und Update von Anti-Viren-Software
- zum Internet-Gebrauch (u. a. Web, Mail)
- Wer ist bei auffälligen Vorkommnissen zu benachrichtigen?

Empfehlenswert: RRZN-Kurs „Sicherheit für Anwender“

Dienstag den 23.11.2004 um 9.15 Uhr

1 **PASS WÖRTER**	**Verwenden Sie sichere Passwörter und gehen Sie sorgsam mit Ihnen um.** **Ein sicheres Passwort ist mindestens 8 Zeichen lang und** ■ **enthält in gemischter Reihenfolge mindestens zwei Buchstaben (groß und klein), zwei Zahlen und zwei Sonderzeichen.** ■ **enthält keine unverfälschten Namen, andere Worte oder Wortteile aus dem Sprachschatz (sowohl in- als auch ausländisch).**

2 **VIREN SCANNER**	**Installieren Sie einen Virenscanner und halten Sie ihn aktuell:** ■ **durch Verwenden der aktuellsten Version.** ■ **durch zusätzliches Laden der neuesten Virenkennungen.** **Nutzen Sie den vom RRZN angebotenen Remote-Update-Service für Sophos:** **http://www.rrzn.uni-hannover.de/sophos_remote_update.html**

3 **BROWSER und BROWSEN**	**Als Browser möglichst nicht den InternetExplorer, besser Opera, Mozilla oder Netscape einsetzen.** **Wenn Sie auf den Internet-Explorer nicht verzichten möchten/können,** ■ **deaktivieren Sie alle Optionen zu ActiveX-Elementen oder** ■ **stellen Sie diese wenigstens auf „Eingabeaufforderung“.** **Deaktivieren Sie Java-Script und Java, lassen Sie es nur für vertrauenswürdige Sites zu.** **Bewegen Sie sich nicht auf dubiosen Seiten und laden Sie sich keine „interessanten Tools“ von unbekannten Webseiten auf Ihren Rechner.**

4 **E-Mail**	**Mail-Programme so einstellen,** **■ dass Anhänge nicht automatisch geöffnet werden.** **■ dass alle Dateinamen-Erweiterungen angezeigt werden.** **■ dass die automatische Vorschau nicht aktiv ist.** **Anhänge nicht unüberlegt öffnen, auch nicht bei bekannter Absenderadresse.** **Anhänge vor dem Öffnen speichern und auf Viren überprüfen.** **Keine HTML-formatierten E-Mails zulassen (sowohl beim Senden, als auch beim Empfang).**

5 **Betriebs-systeme**	■ **Nur Betriebssysteme mit Benutzerverwaltung verwenden.** ■ **Keine Standard-Installation vornehmen, sondern nur Komponenten installieren, die auch benötigt werden.** ■ **Nach der Installation die Systemeinstellungen so abändern, dass nur Dienste aktiviert sind, die auch benötigt werden.** ■ **Standardzugänge (guest bzw. Gast, ...) mit Standardpasswörtern entfernen.**

6 **SICHERHEITS PATCHE**	**Informieren Sie sich regelmäßig über aktuelle Sicherheitslöcher.** **Installieren Sie auf Ihren Systeme regelmäßig** ■ **aktuelle Service-Packs und** ■ **aktuelle Sicherheits-Patche und Hot-Fixes,** **um bekannte (und eventuell noch unbekannte) Sicherheitslücken schnellstmöglich zu schließen.** **Abonnieren Sie die neuesten Meldungen des DFN-CERT unter: http://www.rrzn.uni-hannover.de/abo_sec_mails.html**

7 **SSH**	**Sensible Daten wie Benutzername und Passwort sollten nicht im Klartext über das Netz gehen.** **Eine Alternative ist der Einsatz verschlüsselter Datenübertragung, wie sie von SSH ermöglicht wird.** **Näheres zu SSH können Sie unter folgenden Links lesen:** **http://www.rrzn.uni-hannover.de/ssh_windows.html** **http://www.rrzn.uni-hannover.de/ssh_unix.html**

Zwischen der Institutsleitung des teilnehmenden Institute wird eine Vereinbarung mit folgenden Inhalten geschlossen:

Das Subnetz des oben aufgeführten Instituts wird ab dem ***Datum*** hinter die vom RRZN betriebene Firewall geschaltet, um den Datenverkehr des Institutes durch eine für das Institut ***Institutsname*** angepasste Access-Liste zu filtern.

Festlegung der Ansprechpartner:

Als Ansprechpartner des Instituts fungieren:

1. Herr / Frau ***Name1 Tel. / E-Mail***
2. Herr / Frau ***Name2 Tel. / E-Mail***

Als Ansprechpartner für das RRZN fungieren:

1. **Fr. Christine Peter Tel. 762-8021 E-Mail: peter@rrzn.uni-hannover.de**
2. **Hr. Andreas Anft Tel. 762-19792 E-Mail: anft@rrzn.uni-hannover.de**

Regelungen zur Erstellung der Policy:

Die Erstellung der Sicherheitspolicy erfolgt gemeinsam durch Institut und RRZN.

Die einzelnen Regeln der Access-Liste (Verweis auf Anlage) wurden auf Basis von Institutsvorgaben in Absprache zwischen Institut und RRZN festgelegt.

Regelungen zur Verfahrensweise bei nötigen Änderungen:

Sollten Änderungen nötig sein, wird nach folgender Vorgehensweise verfahren:

- Änderungen an den Access-Listen werden vom RRZN vorgenommen.
- Das RRZN prüft die Änderungsanträge auf Konsistenz zur gemeinsam erstellten Sicherheitspolicy.
- Änderungsanträge können ausschließlich durch die oben genannten Ansprechpartner des Institutes gestellt werden.
- Anträge auf Änderung der Access-Liste werden zur gegenseitigen Absicherung nur in schriftlicher Form als E-Mail oder Brief entgegen-genommen.

Regelungen bzgl. der Logdaten.

Gültigkeitsdauer der Vereinbarung.

Sicherheitshinweise:

Des Weiteren bitten wir Sie, folgende Hinweise zu beherzigen:

- Auch optimal konfigurierte Firewall-Systeme bieten keine hundertprozentige Sicherheit, sie schützen nicht vor Fehlverhalten autorisierter Nutzer.
- Zu einem hohen Prozentsatz liegt die Verhinderung sicherheitsrelevanter Vorfälle nach wie vor in der Verantwortung der Anwender.
- Schärfen Sie das persönliche Risikobewusstsein Ihrer Mitarbeiter und verlassen Sie sich nicht auf vermeintliche technische Sicherheit.

Hinweis auf das RRZN-Merkblatt zum zentralen Netzschutz.