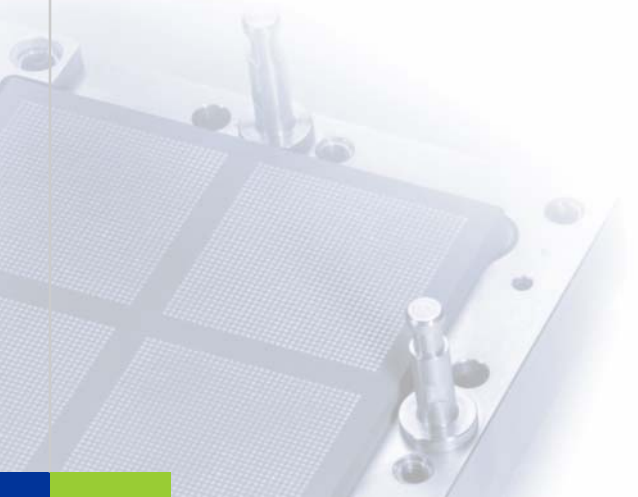
R|R|Z|N

Sicherheitstage WS 2006

Firewallschutz für Institute

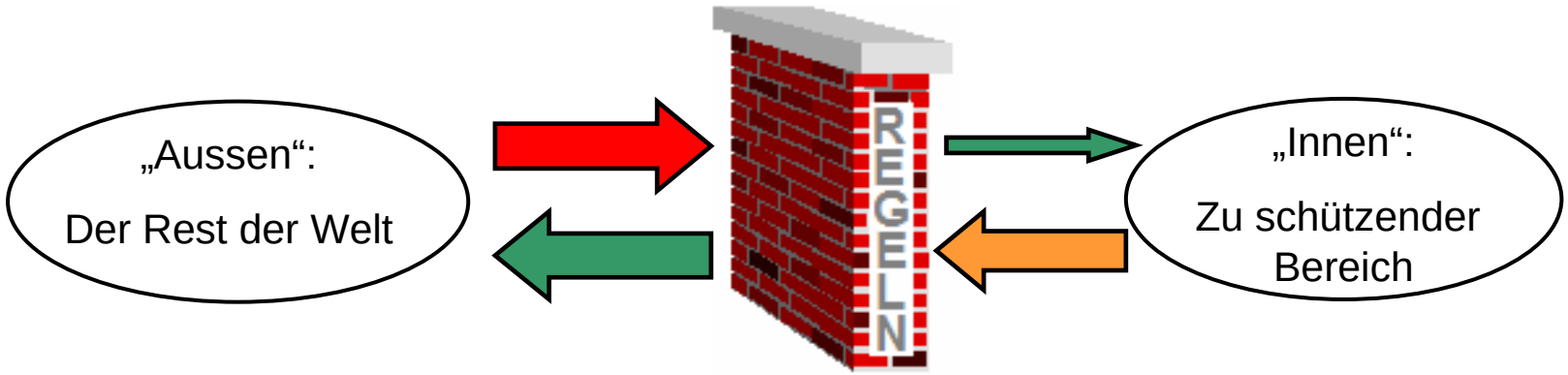
Christine Peter

20. November 2006



Einsatz von Firewall-Technik ist eine mögliche Sicherheitmaßnahme zum Schutz vor Angriffen.

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



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

  läuft durch die Firewall.

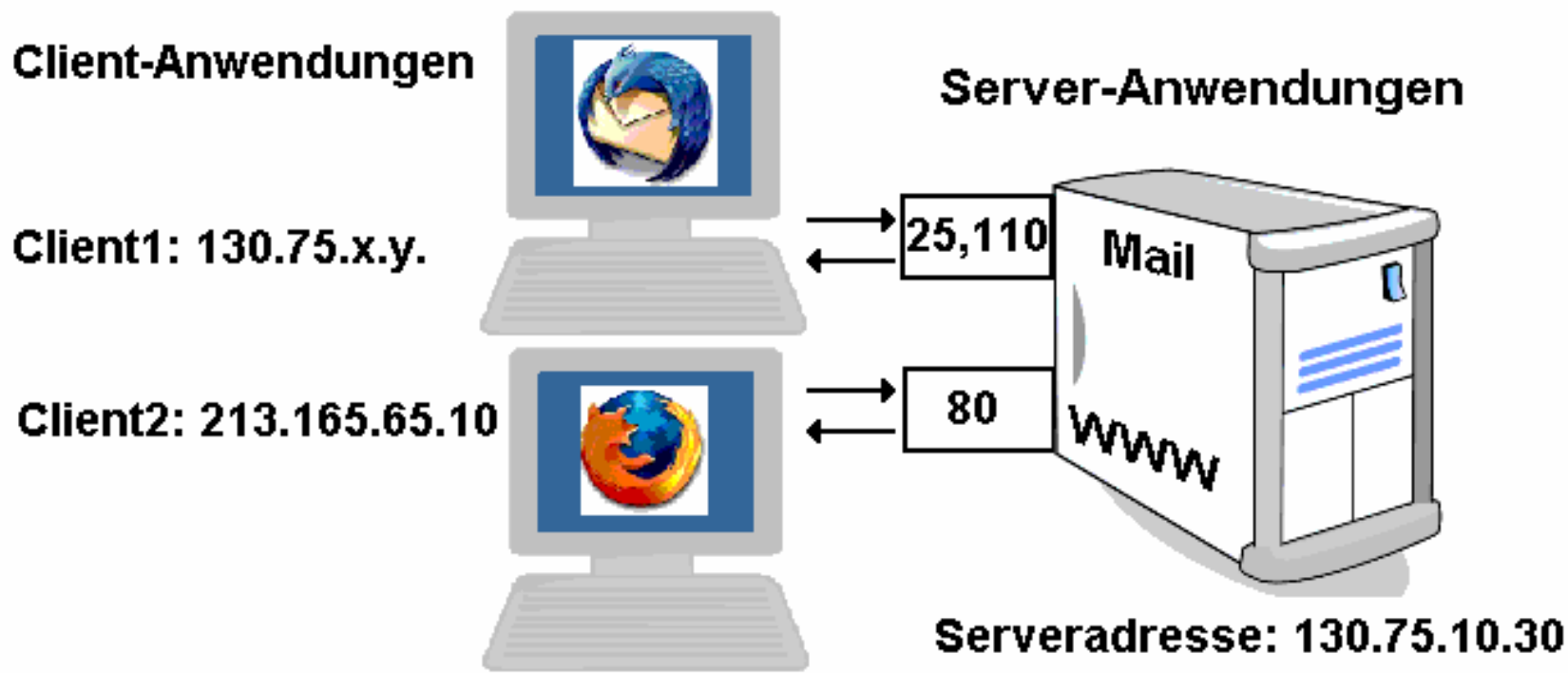
Grundlagen: Datenkommunikation im Internet

R|R|Z|N

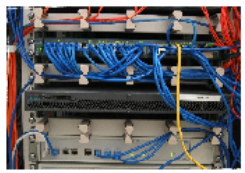
- Kommunikation im Internet = Austausch von Datenpaketen.
- Auch "Verbindungen" sind eigentlich nur Datenpakete, die zwischen zwei Rechnern ausgetauscht werden.
- Jedes Paket wird von einem Quell-Rechner an einen Ziel-Rechner geschickt.
- Eine Verbindung besteht aus mehreren Phasen:
  - Verbindungsaufbau
  - Austausch der eigentlichen Daten
  - Verbindungsabbau

- Der Aufbau dieser Datenpakete ist durch verschiedene Protokolle genau vorgeschrieben.
- Nur so können Quell- und Ziel-Rechner sich verstehen und eine sinnvolle Kommunikation realisieren.
- Beispiele für Protokolle sind: IP, TCP, UDP, ICMP, …
- Protokolle bilden die Basis des Datenaustausches im Internet.
  - Die Pakete kommen an das richtige Ziel.
  - Die Inhalte der Pakete werden richtig interpretiert.

- Auf der Grundlage der Protokolle, die eine Verbindung organisieren, können einzelne Rechner nun verschiedene Dienste anbieten.
- Hierbei tauschen Server- und Anwenderprogramme bestimmte Daten aus.



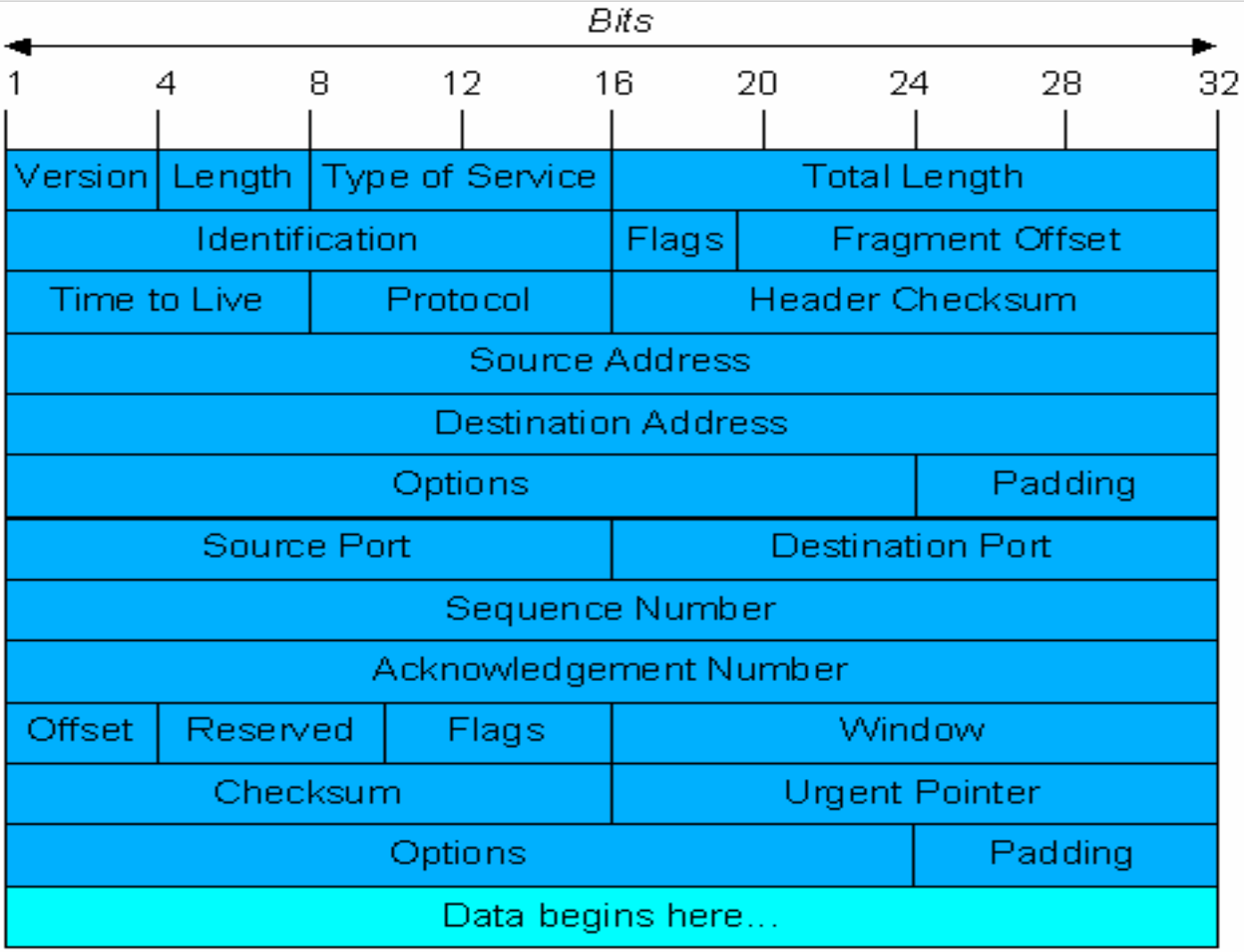
Beispiel Dienstleister RRZN



Telefon- oder Datennetz

Öffentlicher Zusteller

Hauspost


Bits
1
4
8
12
16
20
24
28
32
Version
Length
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Offset
Reserved
Flags
Window
Checksum
Urgent Pointer
Options
Padding
Data begins here...

Eine Regel in Firewall-verständlicher Syntax hat folgende Komponenten:

- **Aktion:** Deny oder Permit
- **Protokoll:** IP,TCP, ...
- **Quelladresse:** alle, einzelne IP oder Netzbereich
- **Quellport:** 1 – 65.535
- **Zieladresse:** alle, einzelne IP oder Netzbereich
- **Zielport:** 1 – 65.535 oder Name des Dienstes

Beispiele:

permit tcp host 130.75.1.1 host *130.75.x.y* eq pop3

permit tcp host 130.75. 2.1 gt 1024 host 130.75.x.z gt 1024

deny tcp any any eq 445

Alle Regeln zusammen bilden die sogenannte Access-Control-List (ACL)

Strukturierungs-Möglichkeit für Firewall-ACLs:

- **Bildung von Network-Groups:** verschiedene IPs können zu einer Gruppe zusammengefasst werden

```
network-object host 130.75.XXX.1
network-object host 130.75.XXX.2
network-object host 130.75.XXX.7
network-object host 130.75.XXX.9
```

→ object-group network **Mailserver-HG**

- **Bildung von Service-Groups:** verschiedene Ports/Dienste können zu einer Gruppe zusammengefasst werden

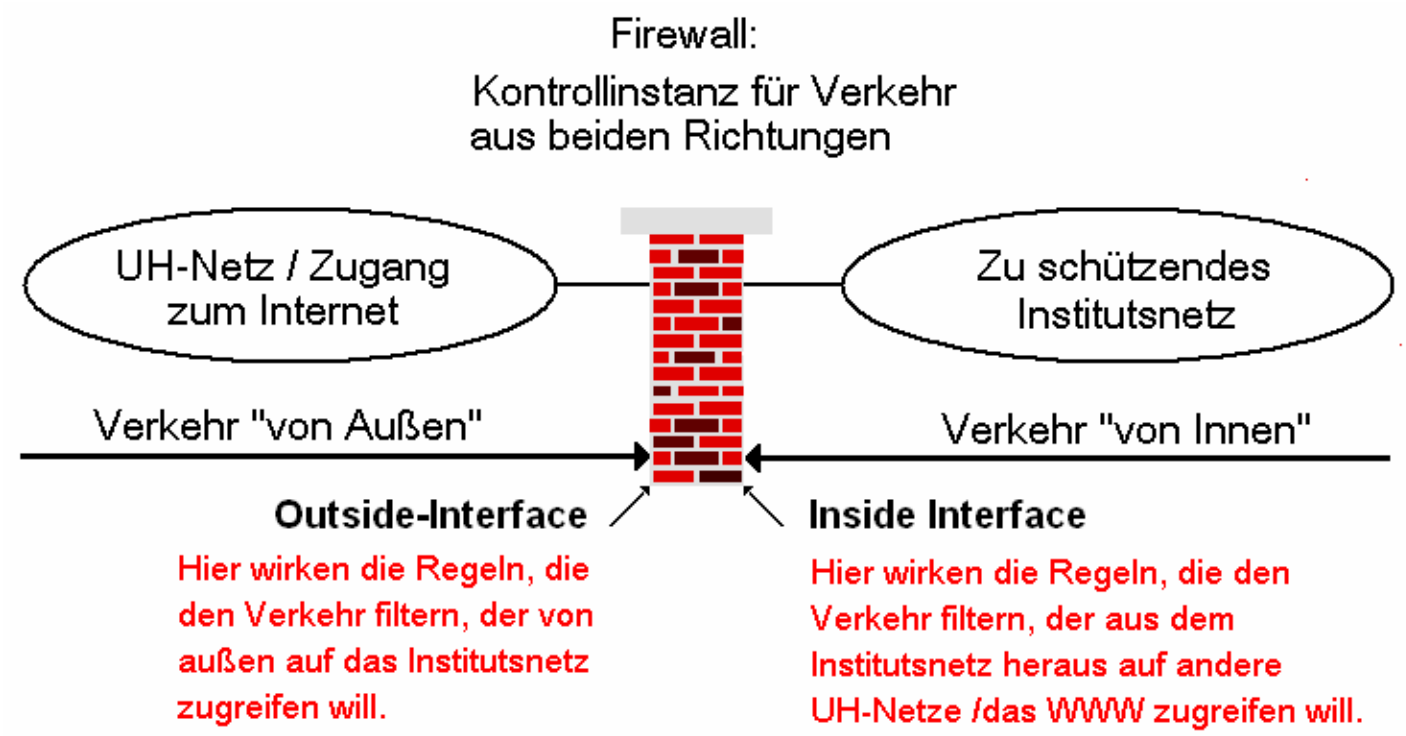
```
port-object eq pop3
port-object eq imap4
port-object eq smtp
```

→ object-group service **Mailen-SG**

- **Konfiguration vereinfacht sich, die ACL wird übersichtlicher:**
  - permit any object-group Mailserver-HG Mailen-SG

Eine Access-Control-List besteht aus zwei Abschnitten:

- **Outbound: Zur Regelung des Verkehrs von „innen“ nach „außen“.**
- **Inbound: Zur Regelung des Verkehrs von „außen“ nach „innen“.**



Die Reihenfolge der Regeln ist wichtig:

- **Die Regeln werden sukzessive nach abgearbeitet.**
- **Sobald eine passende Regel erreicht wird, werden die restlichen Regeln nicht mehr durchlaufen.**

Beispiel:

...

permit tcp any host *130.75.150.20* eq ssh

...

deny tcp host 130.75. 2.x host *130.75.150.20* eq ssh

Paket:
Quell-IP: 130.75.2.25
Ziel-IP: 130.75.150.20
Zielport: 22 (ssh)

Passende Regel gefunden,
Paket ist erlaubt
und wird durchgelassen

Eine optimal konfigurierte Firewall arbeitet nach der Maxime:

„Default-Deny“

- Alle Pakete, die nicht durch eine spezielle Regel erlaubt werden, sollen automatisch verboten sein:
  - 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:
    - als letzte Regel jeder ACL findet sich die Cleanup–Regel

      deny ip any any log

Wie arbeitet eine Firewall

R|R|Z|N

- **Eine Firewall kann nicht alle Risiken ausschalten.**
- **Insbesondere keinerlei Schutz vor Angriffen auf erlaubten Wegen!**
  - Gefahr durch E-Mail-Anhänge.
  - Gefahr beim „Surfen“ durch „aktive“ Web-Inhalte und unbedachte Downloads.

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

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

  - Das Firewall-System kann nur vor Rechnern „vor“ der Firewall schützen.

  ➔ Kompromittierte oder verwurmte Rechner gefährden trotz der Firewall alle Systeme im geschützten Bereich.

  ➔ Es muss also weiterhin für die Sicherheit der Einzelsysteme gesorgt werden.

Zentraler RRZN-Netzschutz:

R|R|Z|N

Das RRZN betreibt ein einstufiges Firewall-System.

Institute können sich hinter dieses Firewall-System schalten lassen.

- Das Institut definiert seine Kommunikations-Anforderungen.
- Im gemeinsamen Gespräch zwischen Institut und RRZN wird eine Sicherheitspolicy für das Institut erarbeitet.

Vom RRZN übernommene Aufgaben:

- Umsetzung der Policy in Firewall-Regeln.
- Administration der Geräte.
- Eintragungen von Änderungen.
- Bereitstellung der Logdaten auf einem zentralen Server.

Das Institut ist verantwortlich für den Umgang mit den Log-Daten.

Zentraler RRZN-Netzschutz:

R|R|Z|N

Vorteile der Firewall im RRZN

- zeitlicher Aufwand für Institut ist sehr gering
- kein zusätzlicher personeller Aufwand
- kostenlos
- regelmäßige Wartung der Firewall ist sichergestellt
- keine Nachfolgerproblematik
- redundante Systeme
- Hilfsmittel zur Analyse von Logdaten werden zur Verfügung gestellt
- Bei Problemen: Unterstützung durch das RRZN

Nachteile der Firewall im RRZN

- Änderungen: mit Zeitverzögerung
- keine DMZ möglich

Zentraler RRZN-Netzschutz:

R|R|Z|N

- **Verfahrensablauf in mehreren Phasen / Stufen:**
  - Vorbereitungsphase
  - Stufe 1: Umstellung mit vereinfachter Policy
  - Stufe 2: Verfeinerung der Regeln aus Stufe 1
- **Ab Umstellungstermin: Nachbesserungen**

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

Vorbereitende Tätigkeiten im Institut:

- 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 vertrauliche Daten wie z.B.:
    - die momentan aktiven Firewallregeln
    - Logdaten.
  - Nur von diesen nimmt das RRZN (schriftlich) Wünsche für Änderungen am Regelwerk entgegen.
- Bereitstellung von 2 IP-Adressen aus dem IP Bereich des Institutes
  - Management-IP
  - Failover-IP

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- Bei Instituten mit sehr unterschiedlichen internen Strukturen kann es unter Umständen auch möglich sein, dass nur für bestimmte Bereiche ein Firewall-Schutz realisiert werden kann.
- Eine Umstrukturierung bei der Vergabe von IP-Adressen kann notwendig werden.
- Bei sehr kleinen Instituten kann es sein, dass sie mit anderen kleinen Instituten zusammen hinter einer Firewall angesiedelt werden.
- Benutzer müssen informiert und befragt werden .
- Verbreitung von Informationen über sicherheitskonformes Anwenderverhalten.

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- **Für den Firewallbetrieb muss im Institut zunächst eine „Verkehrsanalyse“ betrieben werden :**
  - 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.
- **Daraus ergibt sich eine Aufstellung der Anforderungen an das zukünftige Regelwerk.**

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

Zur Erleichterung dieser Aufgabe bietet das RRZN eine Muster-Policy:

- Diese enthält ein Standard-Profil, welches die meisten Anforderungen eines Institutes abdeckt.
- Sie kann ausgefüllt und um spezifische Institutsbedürfnisse ergänzt werden.

Philosophie der Musterpolicy:

- **Verkehr von innen nach außen wird wenig reglementiert**
  - Nur sicherheitsrelevante Ports werden verboten.
  - Ungehindertes Arbeiten soll möglich sein.

- **Verkehr von außen nach innen wird viel stringenter behandelt:**
  - Nur was unbedingt nötig ist, wird erlaubt.
  - Alles Andere wird verboten.

Zentraler RRZN-Netzschutz: Vorbereitung

R|R|Z|N

- **Vorbereitende Tätigkeiten im RRZN:**
  - Vorbereitende Umstellung der Netzwerkkonfiguration.
  - Erstellung der Access-Listen.
  - Vorbereitungen für den Logdaten-Transfer:
    - RRZN: Bereitstellung eines Accounts auf dem Logdaten-Server des RRZN.
    - Institut: „Initialisierung“ des User durch Vergabe eines geeigneten Passwortes.
  - Vereinbarung eines Umstellungstermines.

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Umstellung des Institutes mit einfachster Policy:

- Institut nennt die IPs der Rechner, die von außen erreichbar sein müssen.
- Verkehr von Innen nach Außen:
  - WinFS- und P2P-Ports werden gesperrt.
  - Alles andere ist erlaubt.
- Verkehr von Außen nach Innen:
  - Die IPs der Liste werden freigeschaltet.
  - Zugriffe auf alle anderen IPs des Institutsnetzes werden verboten.

Formular für die Stufe 1-Policy:

Firewalleinstellungen für das Subnetz 130.75.SUBx.von-bis

Zugriffe von Außen (aus dem UH-Netz und dem WWW ins Institutsnetz):

folgende Ips sollen für die Dauer der Stufe 1 komplett für den Zugriff von Außen freigeschalte werden (alle anderen Rechner des Vlans sind von außen nicht erreichbar).

Dienst/Prot.	Port	Quell-IP - „außen“	Ziel-IP - „innen“
ip	any	any	130.75.x.a 130.75.x.b 130.75.x.c

Haben Sie einen institutseigenen Mailserver? Ja ☐ Nein ☐

Bitte tragen Sie hier die Management-IP und die Failover-IP ein:

M-IP:

Fo-IP:

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Komplette Freischaltung:

Protokoll	Port	Quell-IP - „außen“	Ziel-IP - „innen“
ip	any	any	130.75.x.a 130.75.x.b 130.75.x.c

Alternativ: Einschränkungen für einzelne, freizuschaltende Rechner:

Protokoll	Port	Quell-IP - „außen“	Ziel-IP - „innen“
tcp	http https	any / 130.75.x.x / andere IPs	130.75.x.a 130.75.x.b
tcp	ssh	Any / 130.75.x.x / andere IPs	130.75.x.c

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Auszug aus FW-ACL am Outside-Interface :

```
object-group network IPs-Stufe1-INST-HG
  network-object host 130.75.x.r1
  network-object host 130.75.x.r2
object-group network www-INST-HG
  network-object host 130.75.x.r3
  network-object host 130.75.x.r3
…
object-group service www-TCP-SG
  port-object eq www
  port-object eq https
…
permit tcp any object-group www-INST-HG eq object-group www-TCP-SG log

permit ip 130.75.x.x object-group IPs-Stufe1-INST-HG log
…
deny ip any any log
```

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Vorteile:

- Lässt sich für Institut und RRZN schnell realisieren:
  - Sobald das Institut die freizuschaltenden IPs benannt hat, kann die Realisierung meistens im Laufe von 1 Woche erfolgen.
- Schon diese rudimentäre Policy bringt eine sehr akzeptable Schutzfunktion.
- Obwohl die manchmal zeitaufwendige Verkehrsanalyse im Institut noch nicht komplett abgeschlossen ist, kann das Institutsnetz schon geschützt werden.
- Das Institut bezieht schon Logdaten, diese können bei der Analyse hilfreich sein.

Zentraler RRZN-Netzschutz: Stufe 1

R|R|Z|N

Ab dem Umstellungstermin ist institutsseitig Folgendes zu erledigen:

- Anhand der Logdaten kann der Verkehr analysiert werden:
  - Für jeden frei geschalteten Rechner wird untersucht, welche Ports genau für den Zugriff freigegeben werden müssen.
  - Welche Verbindungen sind noch explizit zu verbieten (zur Verminderung des Logdatenaufkommens).
- Aus den Ergebnissen dieser Analysen ergeben sich die verfeinerten Regeln für Stufe 2.
- Diese neuen oder angepassten Regeln pflegt das RRZN bei Übergang zu Stufe 2 im Firewall-System ein.

Der Übergang zu Stufe 2:

- Verkehrsanalyse ist abgeschlossen, das Institut wünscht den Übergang zu Stufe 2:
  - Reaktionszeit des RRZN: möglichst kurz.
  - Abhängig vom Zustand der Warteliste.
- Das Institut wünscht den Übergang zu Stufe 2 nicht:
  - Oft bedingt durch personelle Situation im Institut
  - unproblematisch bei Verkehr von Innen nach Außen.
  - **Nicht auf Dauer akzeptabel** bei Verkehr von Außen nach Innen: Regeln für die Zugriffe auf die Server **sollten unbedingt** angepasst werden!

Zentraler RRZN-Netzschutz: Nachbessserung

R|R|Z|N

- Eventuell nicht mehr funktionierende Anwendungen müssen auf Zusammenhang mit der Firewall untersucht werden.
- Um nicht funktionierende Zugriffe in den Logdaten finden zu können, sind folgende Daten hilfreich :
  - Zugriffszeitpunkt
  - IP des ausführenden Rechners
  - nicht funktionierende Anwendung/Dienst
  - wenn möglich die IP des Zielsystems
- Neue Kommunikationsanforderungen ans RRZN melden.
- Bei Schwierigkeiten: Telefonischer Support und „Live-Zugriff“.

Die Analyse der Logdaten liegt im Aufgabenbereich des Institutes.

Dazu einige prinzipielle Anmerkungen:

- Logdaten sind sensible Daten!
- Es lassen sich unter Umständen Rückschlüsse auf einzelne Personen ziehen.
  - Damit unterliegen Logdaten dem Datenschutz und es existieren gewisse Auflagen, wie mit ihnen umgegangen werden muss.
- Das Erkennen von Sicherheitsproblematiken ist der einzige Grund für das Sichten von Logdaten.
- Die Kontrolle über die Logdaten sollte auf jeden Fall ein Mitarbeiter des Institutes innehaben, der auf das Datengeheimnis verpflichtet wurde.
- Dieser Mitarbeiter sollte sich seiner Verantwortung bewusst sein.

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

- Vom Sicherheitsaspekt her ist die Analyse der Logdaten von nicht zu unterschätzender Wichtigkeit:
  - 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.
- Service des RRZN: grafische und tabellarische Aufbereitung der Logdaten:
  - allgemeine Tagesübersicht: Wie war das Verkehrsaufkommen über den Tag verteilt.
  - verschiedene tabellarische Auswertungen
  - Die Logdaten-Auswertungen sind auf einer Webseite einsehbar (Username / Passwort erforderlich).

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

Beispiel für eine Tagesübersicht (Werktag):

5er-Netz RRZN am Di. 01. Nov 2005

logx 2005/09/14 H.Kessener RRZN

Tagesverlauf

Stunde	Verbindungen		Volumen [Bytes]	
	eingehend	ausgehend	eingehend	ausgehend
0	40	542	182.361.831	23.803.812
1	33	618	25.409	9.769.542
2	36	622	395.201.239	13.488.367
3	36	611	49.785	8.963.173
4	103	618	203.500	45.208.641
5	51	701	5.077.062	9.584.944
6	35	1.458	25.887	33.923.941
7	42	4.202	26.860	198.526.179
8	73	9.150	5.334.456	405.300.983
9	115	8.962	3.423.544.010	505.252.578
10	133	10.589	72.654.368	948.005.574
11	281	11.910	8.194.304.173	1.106.807.684
12	145	11.257	2.927.257.665	593.539.022
13	100	9.471	6.368.516	377.554.208
14	132	12.385	11.822.779	1.119.766.185
15	192	11.369	2.580.257.787	1.746.595.563
16	166	10.016	4.363.694	703.816.504
17	76	3.656	1.730.399.825	683.666.045
18	32	2.873	105.377	59.834.281
19	30	1.896	25.227	21.594.949
20	32	2.114	8.052.025	25.301.368
21	24	1.618	23.858	171.617.074
22	28	783	776.967.596	13.276.013
23	37	771	844.829.041	28.722.590
Summe	1.972	118.192	21.169.281.970	8.853.919.220

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

Detaillierte Auswertungen (Top-50)								
Hosts	**extern**				**intern**			
	nach Verbindungen		nach Volumen		nach Verbindungen		nach Volumen	
	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend
Verbindungen	**eingehend**				**ausgehend**			
	nach Volumen		nach Dauer		nach Volumen		nach Dauer	

Top-50 Hosts extern nach Volumen ausgehend

Nr.	Host	Verbindungen	Bytes
1	[illegible]	47	2.924.778.156
2	[illegible]	4.563	1.538.269.663
3	[illegible]	8	1.144.293.905
4	[illegible]	13	1.118.209.747
5	[illegible]	12.377	658.501.421
6	[illegible]	753	548.450.748
7	[illegible]	182	271.083.246
8	[illegible]	4	244.242.835
9	[illegible]	16	231.348.554
10	[illegible]	2	162.965.852
11	[illegible]	2	148.236.190
12	[illegible]	3	144.944.657
13	[illegible]	347	134.619.350
14	[illegible]	1.470	133.006.482
15	[illegible]	10	120.668.675
16	[illegible]	1.988	112.604.705
17	[illegible]	430	111.701.286

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

Detaillierte Auswertungen (Top-50)								
Hosts	**extern**				**intern**			
	nach Verbindungen		nach Volumen		nach Verbindungen		nach Volumen	
	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend	eingehend	ausgehend
Verbindungen	**eingehend**				**ausgehend**			
	nach Volumen		nach Dauer		nach Volumen		nach Dauer	

Top-50 Hosts extern nach Verbindungen eingehend

Nr.	Host	Verbindungen	Bytes
1	[illegible]	574	570.672
2	[illegible]	486	5.702.167
3	[illegible]	341	33.956.440
4	[illegible]	283	33.820
5	[illegible]	96	8.521.468.252
6	[illegible]	51	586.242
7	[illegible]	36	2.736
8	[illegible]	36	184.174
9	[illegible]	30	2.352
10	[illegible]	27	2.610.473
11	[illegible]	27	1.068.226
12	[illegible]	24	19.614.559
13	[illegible]	16	119.804
14	[illegible]	12	216
15	[illegible]	9	392.304
16	[illegible]	8	408.392
17	[illegible]	8	4.192
18	[illegible]	7	939.636.510

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

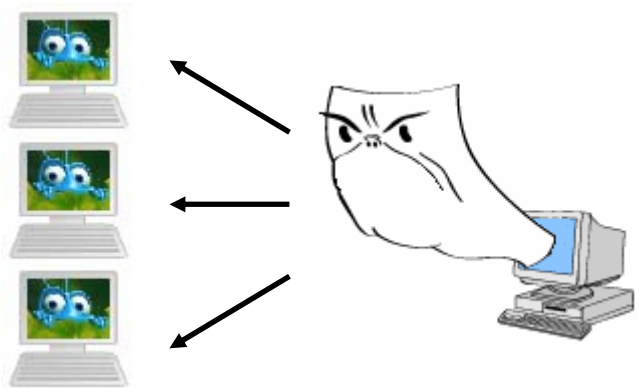
- Durch die tabellarische Aufbereitung kristallisiert sich über Tage und Wochen eine Rangfolge heraus:
  - Mit der Zeit bekommen Sie ein Gespür dafür, welche Rechner „zu Recht“ auf den Top-Plätzen stehen.
  - Es fällt auf, wenn dort plötzlich ein Rechner auftaucht, der an dieser Stelle eigentlich nichts zu suchen hat.

- Rechner oder Tageszeiten, die in der Logdaten-Auswertung auffallen, können nun gezielt in den Logdaten genauer untersucht werden.

Zentraler RRZN-Netzschutz: Logdaten

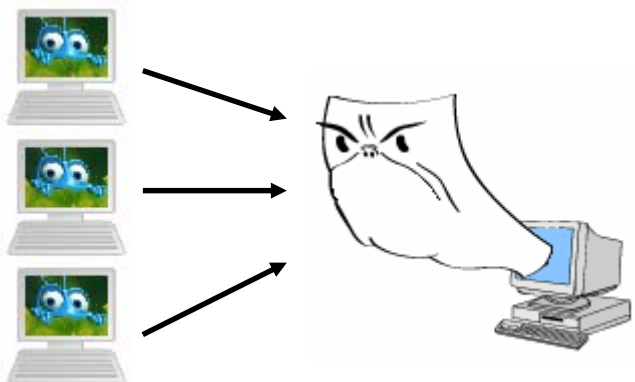
R|R|Z|N

- **Top50-Liste der externen Hosts mit den meisten Verbindungen**
  - eingehend



Scan?

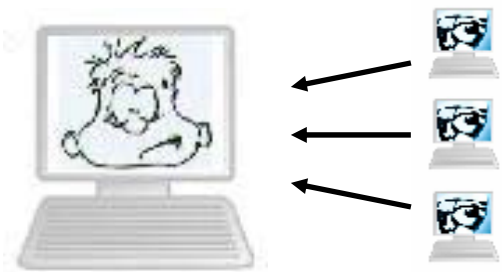
  - ausgehend



Datenspionage?
Adware?

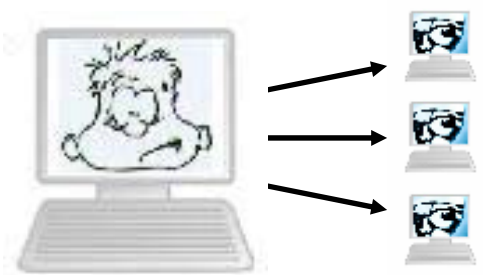
Zentraler RRZN-Netzschutz: Logdaten

- **Top50-Liste der internen Hosts mit den meisten Verbindungen**
  - eingehend



DOS?
Backdoor?

  - ausgehend

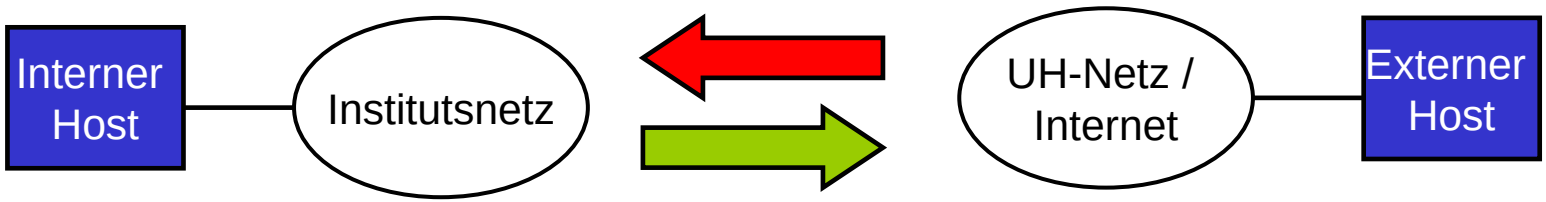


Wurm
Virus?

Zentraler RRZN-Netzschutz: Logdaten

R|R|Z|N

- Top50-Liste der internen / externen Hosts mit dem größten Transfervolumen
  - eingehend
  - ausgehend



RRZN-Empfehlung: Erweiterung der Instituts-Security-Policy:

Ein Soll:

- Personal Firewalls als zusätzlichen Schutz auf jedem Rechner.

Ein Muss:

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

Informationen auf den Security-Webseiten des RRZN:

http://www.rrzn.uni-hannover.de/firewall.html

Sicherheit kann nicht ohne sicherheitsbewusstes Verhalten der Anwender erreicht werden!

Verteilen Sie Informationen zur Anwendersicherheit in Ihrem Institut:

- Folien des RRZN-Kurses „Sicherheit für Anwender“

  http://www.rrzn.uni-hannover.de/sicherheitstage.html

- Flyer zur IT-Sicherheit mit Tipps und Angeboten des RRZN zum sicheren Betrieb von Rechnern; Download einer Kopiervorlage unter:

  http://www.rrzn.uni-hannover.de/it_sicherheit.html

- Merkblatt zum RRZN-Netzschutz mit den wichtigsten Regeln für ein sicherheitskonformes Anwenderverhalten. Das Merkblatt ist verfügbar unter auf der Webseite zum RRZN-Netzschutz unter „Dokumente zum Download“

  http://www.rrzn.uni-hannover.de/netzschutz.html

Wir hoffen auf neue Interessenten!

Melden Sie sich bei Christine Peter;
per E-Mail: peter@rrzn.uni-hannover.de
oder telefonisch: 8021

http://www.rrzn.uni-hannover.de/netzschutz.html