Basiswissen für Netzverantwortliche

Fehlerbehebung, Missbrauch und Sicherheit im MWN

Dr. Helmut Reiser, Claus Wimmer

12. März 2009

Folien unter: www.lrz.de/services/schulung/unterlagen/nv-sicherheit

Netzverantwortlicher

- Unser Kontakt und Ansprechpartner
- Aufgaben:
  - zuständig für einen (Netz-) Bereich
  - (alleinige) Schnittstelle zum LRZ (Arealbetreuer) in Netzfragen
  - Schnittstelle für Benutzer in seinem Bereich für Netzfragen
  - **Dokumentation**
  - **Fehlerverfolgung**
  - **Mithilfe bei Netzmissbrauch und kompromittierten Systemen**
  - Planung und Inbetriebnahme von Erweiterungen der Gebäudenetze
- Wer ist mein Netzverantwortlicher ?
  www.lrz.de/services/netz/db_netzverantwortliche/

Inhalt

- Sicherheitsleitlinie des LRZ
- Basiswissen
- Aufgaben des Netzverantwortlichen
- Sicherheitsdienste des LRZ und Abuse Bearbeitung
  - ...
- Konkrete Beispiele
- Informationsquellen

Sicherheitsleitlinie des LRZ

- Nutzungsrichtlinien:
  www.lrz.de/wir/regelwerk/benutzungsrichtlinien/
- Das LRZ versteht sich nicht als Netz-Polizist !
- So viel Freiheit wie möglich;
  so viel Security wie angemessen (nötig) und realisierbar !

⇨ Freiheit in Forschung & Lehre

⇨ Security kostet
  - Person-Power
  - Geld
  - Bequemlichkeit

Basiswissen: Ethernet und MAC Adressen

- Netztechnologie für Local Area Networks (LAN)
- Ursprünglich entwickelt um Systeme in kleinen Bereichen zu verbinden (Gebäude oder Gebäudeteil)
- LAN-Segment definiert durch Netzkomponente (Hub, Switch)
- Adressierung über MAC Adressen:
  - 48 Bit (6 Byte) lang
  - Jede Netzwerkkarte hat MAC Adresse; damit Identifikation des Endsystems möglich
  - Sollte (weltweit) eindeutig sein (aber per Software änderbar)
  - Hexadezimal-Notation:
    `08:00:20:ae:fd:7e` oder `08-00-20-ae-fd-7e`
  - Auslesen der MAC Adressen, abhängig vom Betriebssystem siehe: http://de.wikipedia.org/wiki/MAC-Adresse

Basiswissen: TCP/IP

- Datenaustausch über Grenzen von LANs hinweg; *Internetworking*
- Internet Protocol (IP):
  - Weitervermittlung von (IP-) Paketen und Wegewahl
  - IP-Adressen:
    - IP Version4: 32 Bit lang, Dezimalnotation in vier Blöcken: 129.187.10.15
    - IP Version6: 128 Bit lang, Hexadezimalnotation mit Doppelpunkt 2001:0db8:85a3:08d3:1319:8a2e:0370:7344
- Transmission Control Protocol (TCP):
  - Zuverlässige Ende-zu-Ende Verbindung
  - Ports:
    - 16 Bit lang, Dezimalnotation; z.B. 80
    - Adressiert Anwendungsdienst, z.B. 80 = HTTP (Webserver), 22 = ssh

Mithilfe des Netzverantwortlichen

- Fehlerverfolgung:
  - Überprüfung von Anschlüssen/Patchungen am Switch
    - Erkennung von Schleifen
    - Identifikation von angeschlossenen Systemen
  - Mithilfe bei der Überprüfung von Konfigurationen
- Netzmissbrauch und kompromittierte Systeme (Abuse Bearbeitung)
  - Identifikation
  - Information der Nutzer
  - „Säubern“ infizierter Maschinen

Inhalt

- Sicherheitsleitlinie des LRZ
- Basiswissen
- Aufgaben des Netzverantwortlichen
- Sicherheitsdienste des LRZ und Abuse Bearbeitung
  - ...
- Konkrete Beispiele
- Informationsquellen

Sicherheitsdienste des LRZ: Überblick

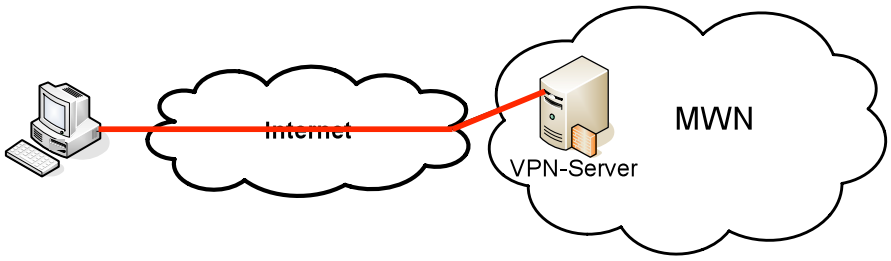
- Private IP-Adressen
- Virtuelles privates Netz (VPN)
- Bearbeitung von Missbrauchsfällen (ABUSE)
- Sicherheitsmeldungen von ABUSE
- NAT-o-MAT
- NYX
- MAC Flooding, schwarze Access Points
- Virtuelle Firewall
- Sperren im MWN
- E-Mail
- Viren: Sophos
- Windows Server Update Service (WSUS)

Sicherheitsdienste: Private IP-Adressen

- Vordefinierte Netzbereiche:
  - 10.0.0.0 bis 10.255.255.255
  - 172.16.0.0–172.31.255.255
  - 192.168.0.0–192.168.255.255
  - Werden an Systeme im MWN vergeben und gerouted: 10.148. – 10.159.
- Im Internet nicht weitervermittelt (kein Routing), **ABER** Routing im MWN
- Systeme vom Internet aus NICHT erreichbar, d.h.
  - Schutz vor Angriffen aus dem Internet
  - Kein Schutz vor Angriffen aus dem MWN
  - Systeme nicht als Plattform für Angriffe auf Rechner außerhalb des MWN nutzbar

Sicherheitsdienst: Virtual Private Network (VPN)

- Aufbau eines sicheren Teilnetzes über unsichere Netze (Internet, Funknetze,…)
- Tunnel; realisiert durch Verschlüsselung der Kommunikation (IPsec)



VPN im MWN

- VPN erforderlich für
  - WLAN-Anschlüsse im MWN
  - Öffentliche Anschlussdosen für mobile Rechner im MWN
  - Nutzung von zugangsbeschränkten, internen MWN-Diensten (Online-Zeitschrifte, Sophos, …) über fremde Internet-Anbieter oder Bewohner von Studentenwohnheimen
- Voraussetzungen:
  - Cisco VPN Client
  - Kennung: AFS, CampusLMU, MyTUM.de oder Radius
- Informationen:
  - www.lrz.de/services/netz/mobil/vpn/

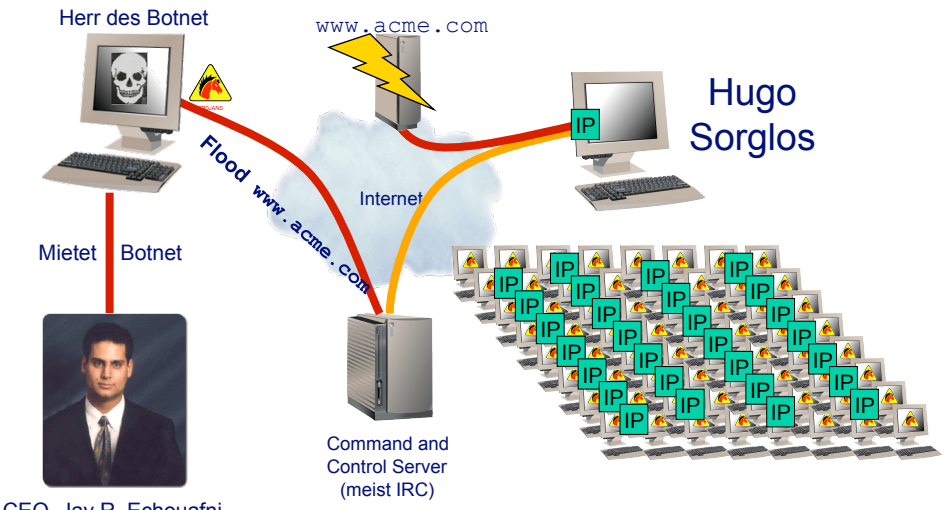
Sicherheitsdienste des LRZ: Überblick

- Private IP-Adressen
- Virtuelles privates Netz (VPN)
- Bearbeitung von Missbrauchsfällen (ABUSE)
- Sicherheitsmeldungen von ABUSE
- NAT-o-MAT
- NYX
- MAC Flooding, schwarze Access Points
- Virtuelle Firewall
- Sperren im MWN
- E-Mail
- Viren: Sophos
- Windows Server Update Service (WSUS)

Klassifikation von Abuse-Fällen

- Gehackte oder mit Würmern / Trojanern / … infizierte Rechner; sehr oft Bot-Netz-Slaves
- (Un)berechtigte (Spam-)Beschwerden
- Copyright-Verletzungen (externe Hinweise)
- Hinweise und Anfragen von MWN-Benutzern
- Fehlverhalten von MWN-Benutzern (absichtlich oder unabsichtlich)
- Externe Hinweise: DFN-CERT; z.B. Bot-Netze
- Google: Hinweis auf “böswillige” Inhalte in Web-Seiten
- Sonstige strafrechtlich relevante Fälle
- Siehe auch: www.lrz.de/services/security/abuse/

Einschub: Botnets



Mit freundlicher Genehmigung von Udo Schneider, Trend Micro ©

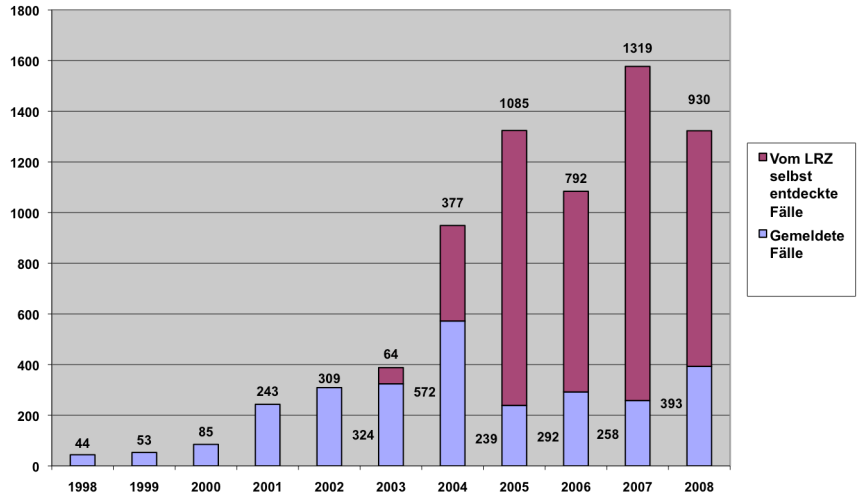
Abuse Bearbeitung

- Ermittlung des Verursachers (Rechner bzw. Kennung)
- Benachrichtigung weiterleiten an
  - Benutzer → Kennung, priv. Rechner
  - Ansprechpartner für Kennung
  - Netzverantwortlicher → MWN-Rechner
- Antwort an den Beschwerdeführer
- Bei Bedarf Eskalation

Abuse Bearbeitung: Eskalation

- Bei Kennungen und privaten Rechnern:
  - Benachrichtigung des Benutzers (möglichst direkt)
  - Sperre der Kennung (temporär oder dauerhaft)
  - Disziplinarisches Verfahren
- Bei MWN-Rechnern:
  - Benachrichtigung des Netzverantwortlichen
  - Sperre am Internet-Übergang bzw. im NAT-o-MAT
  - Sperre eines kompletten Subnetzes am Backbone-Router

Abuse Fälle



Bsp. einer automatischen Benachrichtigung

Sehr geehrte Netzverantwortliche,

der folgende Rechner aus Ihrem Bereich zeigt ein auffälliges Kommunikationsverhalten und wurde automatisch an der Nutzung des Internets gehindert.

Sehr wahrscheinlich ist der betreffende Rechner von einem Wurm oder Virus befallen. Auch P2P-Software (zum Filesharing, wie z.B. Gnutella, Kazaa, BitTorrent) kann in ungünstigen Fällen zu dieser Meldung führen.

Um wieder Zugriff auf die Internetdienste zu erhalten, beenden Sie eventuell laufende P2P-Software und versichern Sie sich bitte, dass ein aktueller Virenscanner auf dem System installiert und aktiviert wurde.

Ist die Ursache für die Sperrung beseitigt, wird nach spätestens 15 Minuten der Zugriff auf die Internetdienste automatisch wieder ermöglicht.

Automatische Benachrichtigung (Forts.)

Status Report for [redacted]

Gesperrt seit / Blocked since 29.10.07 16:48

Überschreitungen Number of hits	Protokoll Protocol	Zielport und Grund der Sperrung Destination port and suspension reason
8376	TCP	49000

Information found via SNMP from Switches and Routers

IP	MAC	Device	Interface	created	last update
[redacted]7.1	00:02:B3:C8:62:7D	swh3-kzm.net.lrz-muenchen.de	E6	Jan 17, 2007 1:30:17 PM	Oct 19, 2007 5:09:28 AM

Mit freundlichen Grüßen

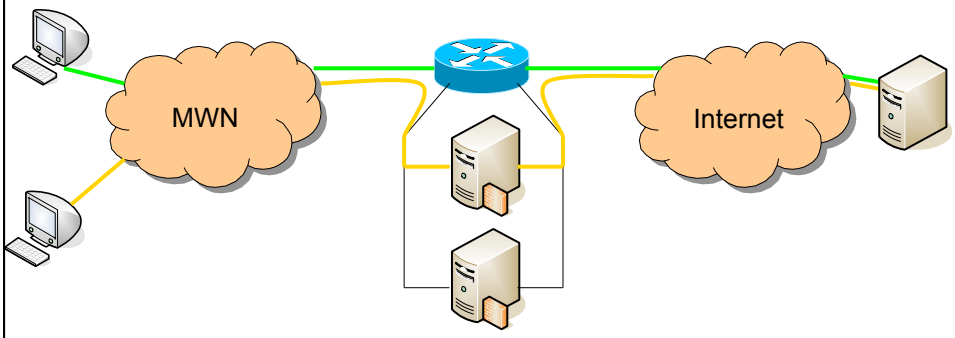
Nat-O-Mat

- Generisches Intrusion Detection / Intrusion Prevention System
- Dynamische Bandbreitenbeschränkung

Grundidee des NAT-o-MAT

- Transparentes NAT-Gateway
  - NAT = Network Adress Translation; Umsetzung privater Adressen
  - Keine Konfiguration erforderlich (transparente Nutzung)
  - Private Netze werden über NAT-o-MAT geleitet: Studentenwerke, VPN, Einwahlnetze
- Erkennung von Auffälligkeiten durch
  - Analyse des Kommunikationsverhaltens (z.B. Paketraten)
  - Zahl der Kommunikationspartner
- Begrenzung der “False Positive”-Rate
  - durch sanfte Sperrungen (sog. Softlimits),
  - Begrenzung der erlaubten Paketrate / Bandbreite
  - Vollständige Sperrung nur im Fall einer Eskalation

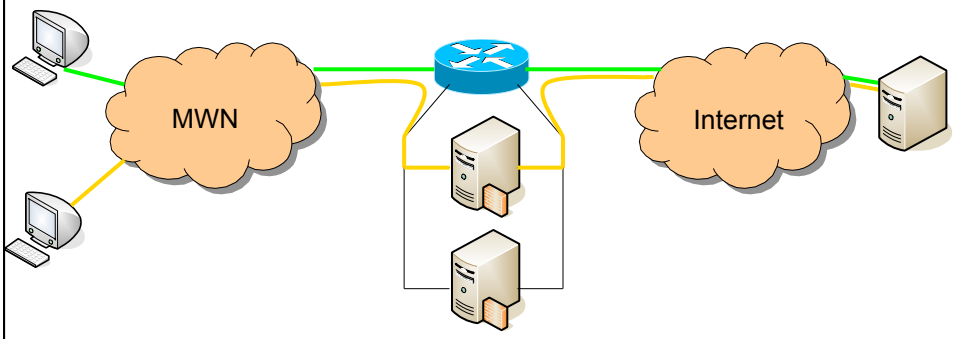
Einbindung ins Netz



NAT-o-MAT

- NAT-o-MAT ist selbständiger Router
- Umleitung ausgewählter Pakete per Policy based Routing zum NAT-o-MAT

Einbindung ins Netz



NAT-o-MAT

- Verkehr wird analysiert, parametrisiert und ggf. gefiltert.
- Erlaubter Verkehr wird über den WAN-Router weitergeleitet

Durchsetzung der Regeln

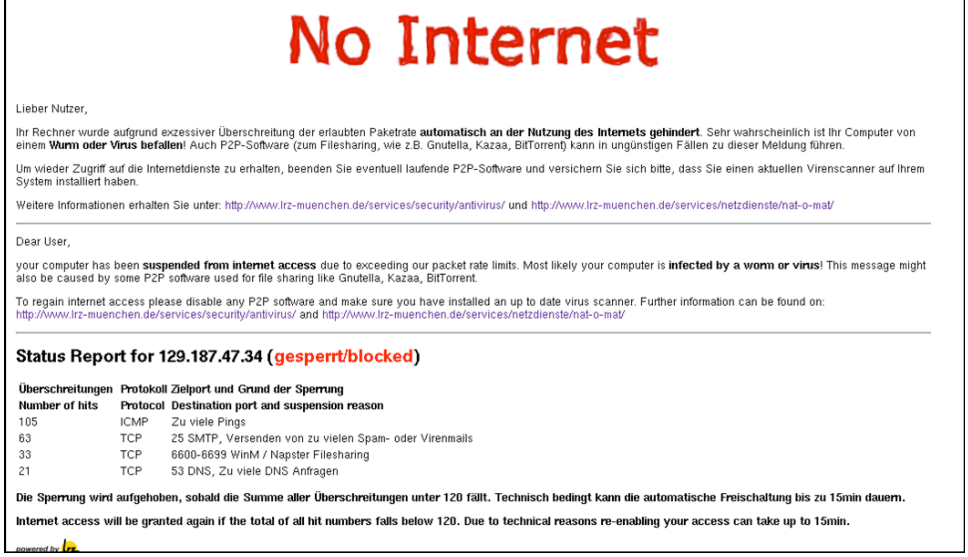
- Strafpunkte pro IP-Adresse
  - bezieht sich auf die Verstöße eines gleitenden Zeitfensters (z.B. die letzten 15 Minuten)
  - Limits für Sperrung, Freischaltung, Benachrichtigung
- Automatische Sperrung und Freischaltung
  - basierend auf Strafpunktekonto mit gleitendem Zeitfenster
  - transparentes Verfahren für den Benutzer
  - Keine manuelle Intervention notwendig

Durchsetzung der Regeln: 4-stufiges Eskalationsprinzip

1. Bei kurzzeitigen Überschreitungen: 30 Versuche/s
   - Keine Einschränkung unterhalb der “Burst-Bedingung”
2. Bei Überschreitung der “Burst-Bedingung”: 31. Versuch
   - **Soft-Limit:** Blockierung der verursachenden IP-Pakete
   - Inkrement der Strafpunkte 1 Punkt je 10 Versuche/s
3. Bei Erreichen des Strafpunkt-Limits: 120 Punkte
   - **Hard-Limit:** Sperrung der verursachenden IP-Adresse
   - Erzeugung einer benutzerbezogenen Hinweisseite
4. Bei anhaltendem Verstoß und hoher Strafpunktzahl: > 1000 Punkte
   - Email-Benachrichtigung an eine verantwortliche Person mit vollständigem IDS-Report (an interne Verursacher)

- Beispiel
  Port-Scan: eine Absender IP auf einen Ziel-Port (auf mehreren Ziel-Systemen)

Automatisierter Warnhinweis



No Internet

Lieber Nutzer,

Ihr Rechner wurde aufgrund exzessiver Überschreitung der erlaubten Paketrate **automatisch an der Nutzung des Internets gehindert**. Sehr wahrscheinlich ist Ihr Computer von einem **Wurm oder Virus befallen**! Auch P2P-Software (zum Filesharing, wie z.B. Gnutella, Kazaa, BitTorrent) kann in ungünstigen Fällen zu dieser Meldung führen.

Um wieder Zugriff auf die Internetdienste zu erhalten, beenden Sie eventuell laufende P2P-Software und versichern Sie sich bitte, dass Sie einen aktuellen Virenscanner auf Ihrem System installiert haben.

Weitere Informationen erhalten Sie unter: http://www.lrz-muenchen.de/services/security/antivirus/ und http://www.lrz-muenchen.de/services/netzdienste/nat-o-mat/

Dear User,

your computer has been **suspended from internet access** due to exceeding our packet rate limits. Most likely your computer is **infected by a worm or virus**! This message might also be caused by some P2P software used for file sharing like Gnutella, Kazaa, BitTorrent.

To regain internet access please disable any P2P software and make sure you have installed an up to date virus scanner. Further information can be found on: http://www.lrz-muenchen.de/services/security/antivirus/ and http://www.lrz-muenchen.de/services/netzdienste/nat-o-mat/

Status Report for 129.187.47.34 (gesperrt/blocked)

Überschreitungen Number of hits	Protokoll Protocol	Zielport und Grund der Sperrung Destination port and suspension reason
105	ICMP	Zu viele Pings
63	TCP	25 SMTP, Versenden von zu vielen Spam- oder Virenmails
33	TCP	6600-6699 WinM / Napster Filesharing
21	TCP	53 DNS, Zu viele DNS Anfragen

Die Sperrung wird aufgehoben, sobald die Summe aller Überschreitungen unter 120 fällt. Technisch bedingt kann die automatische Freischaltung bis zu 15min dauern.

Internet access will be granted again if the total of all hit numbers falls below 120. Due to technical reasons re-enabling your access can take up to 15min.

powered by lrz

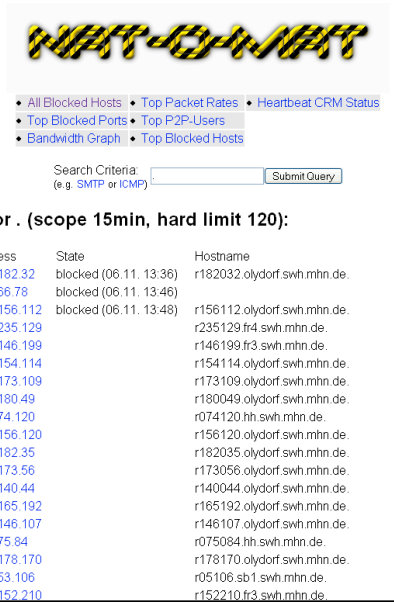
Traffic Shaping

- Bandbreiten- und Paketratenbegrenzung für P2P-Protokolle (z.B. Filesharing via Kazaa oder Bittorrent).
- Z.Zt. realisiert: Gemeinsame Bandbreitenklassen für alle Nutzer:
  - 2Mbit/s für BitTorrent
  - 1Mbit/s für alle anderen P2P-Protokolle

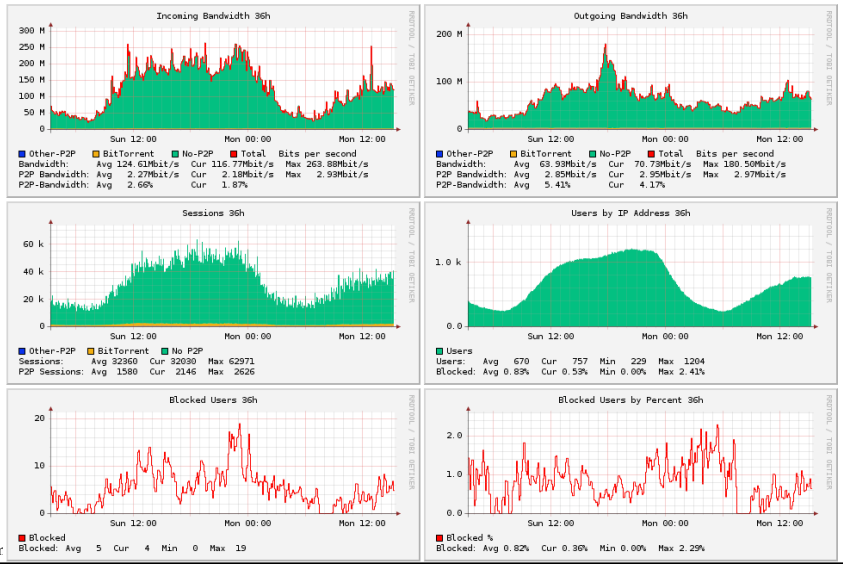
NAT-o-MAT

Demo

Management Interface: All Blocked Hosts



Bandbreiten



Dr. Helm

1

Praxiseinsatz

- Kennzahlen (Stand Feb. 2009)
  - Anzahl der Hosts: ~ 2.500
  - Anzahl Sessions: ~ 90.000
  - Durchsatz: ~ 330 Mbit/s (in), ~ 140 Mbit/s (out)
  - P2P-Anteil: 1% bis 4% (in), 2% bis 7% (out)
  - Durch Hard Limits gesperrte Hosts: 0,1 bis 2 %

32

Dr. Helmut Reiser

Automatische Benachrichtigung (Forts.)

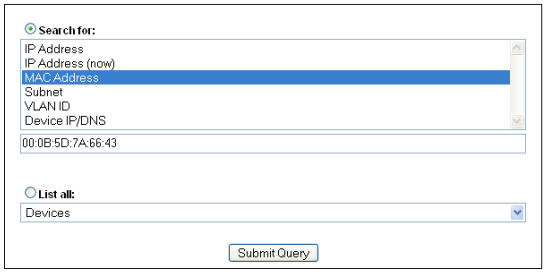
```
Status Report for [redacted]

Gesperrt seit / Blocked since 29.10.07 16:48

Überschreitungen   Protokoll Zielport und Grund der Sperrung
Number of hits     Protocol  Destination port and suspension
reason
8376               TCP       49000

Information found via SNMP from Switches and Routers

IP MAC Device Interface created last update
[redacted].1 00:02:B3:C8:62:7D swh3-kzm.net.lrz-muenchen.de E6
Jan 17, 2007 1:30:17 PM Oct 19, 2007 5:09:28 AM

Mit freundlichen Grüßen

Nat-O-Mat
```

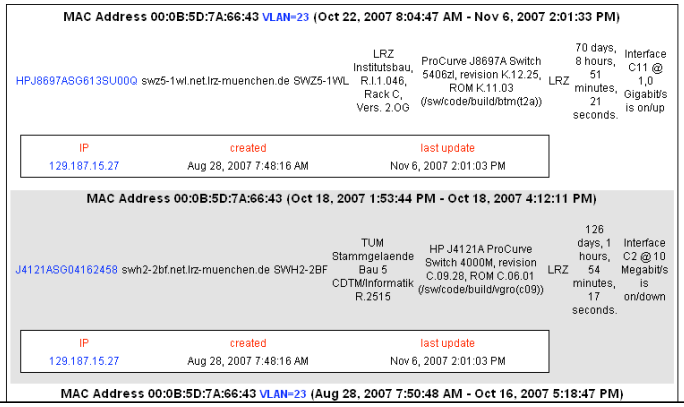

Sicherheitsdienste des LRZ: Überblick

- Private IP-Adressen
- Virtuelles privates Netz (VPN)
- Bearbeitung von Missbrauchsfällen (ABUSE)
- Sicherheitsmeldungen von ABUSE
- NAT-o-MAT
- NYX
- MAC Flooding, schwarze Access Points
- Virtuelle Firewall
- Sperren im MWN
- E-Mail
- Viren: Sophos
- Windows Server Update Service (WSUS)

Nyx: Identifikation und Lokalisierung von Systemen

- Auffällige Systeme; bekannte Info: MAC oder IP Adresse
- Problem: Rechner müssen lokalisiert und gesäubert werden
- Lokalisierung:
  - MAC Adresse
  - IP-Adresse
  - Switch
  - Anschluss-Port
- Eigenentwicklung zur Lokalisierung: Nyx
  - Aufbau einer internen Datenbank
  - Maschinelles Lernen zur Erkennung der Up/Downlink Ports
  - Schnittstelle zur automatischen Suche
  - Nutzerinterface: DEMO





Nyx: MAC Spoofing/Flooding

- Nyx findet Switch-Ports mit mehreren (extrem vielen) MAC-Adressen:
  - Mini-Switch (problemlos)
  - System verändert (fälscht) MAC Adressen (Spoofing)
  - „schwarzer“ WLAN Access Point
  - …..
- Ggf. Benachrichtigung an Netzverantwortliche
- Mithilfe bei der Problemlösung

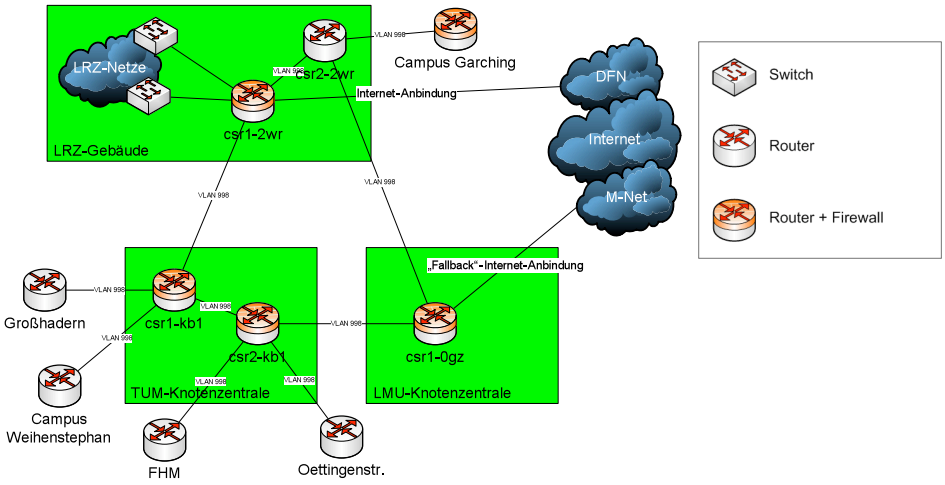
Sicherheitsdienste des LRZ: Überblick

- Private IP-Adressen
- Virtuelles privates Netz (VPN)
- Bearbeitung von Missbrauchsfällen (ABUSE)
- Sicherheitsmeldungen von ABUSE
- NAT-o-MAT
- NYX
- MAC Flooding, schwarze Access Points
- Virtuelle Firewall
- Sperren im MWN
- E-Mail
- Viren: Sophos
- Windows Server Update Service (WSUS)

Virtuelle Firewalls im MWN

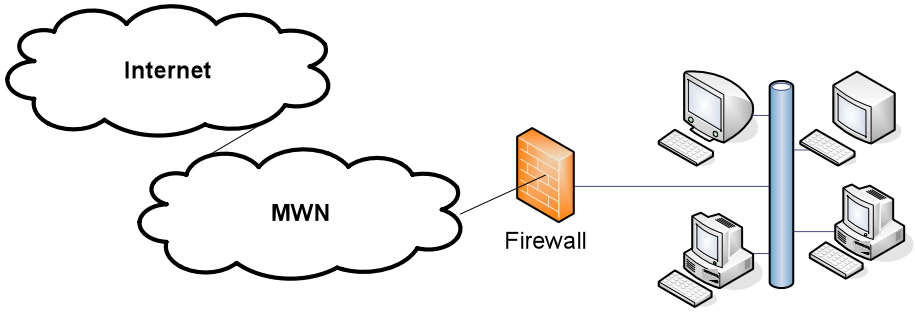
- Firewall-Blade: Einschübe in Kern-Router
  - Technisch äquivalent zu Cisco PIX
  - Mandantenfähig, d.h. logisch **„eigene“ Firewall** pro Kunde
- Filter
  - Paketfilter: Stateful
  - Applikation: HTTP, SIP, …
- LRZ stellt Grundkonfiguration bereit
- Anpassung durch den Kunden erforderlich!
- Benutzer-Interface zur Administration
  - Graphisches Web-Interface (signiertes Java-Applet)
- Logging/Monitoring: eigenes Log-File und Web-Interface

Integration der virtuellen FW im MWN



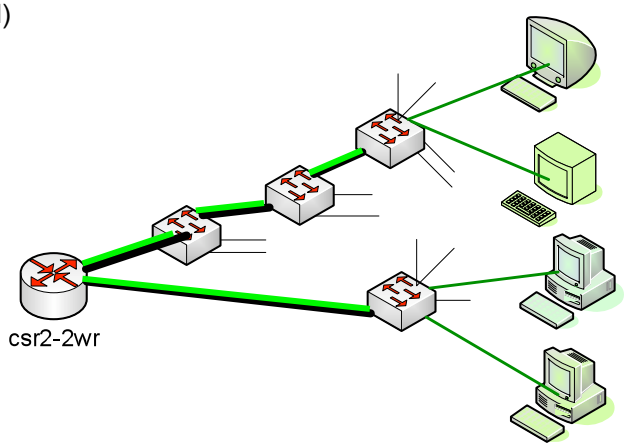
Integration der virt. FW beim Kunden: Logische Sicht

- Platzierung der Firewall unmittelbar „vor“ dem Kundennetz



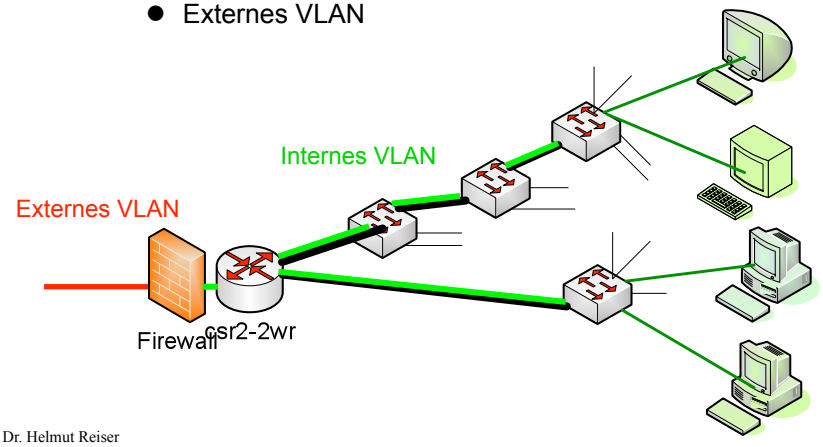
Einschub: Virtuelles LAN (VLAN)

- Zweck: Betrieb eines LAN über mehrere Switches hinweg
- Trennung des Verkehrs im VLAN vom restlichen Verkehr (im Kabel)



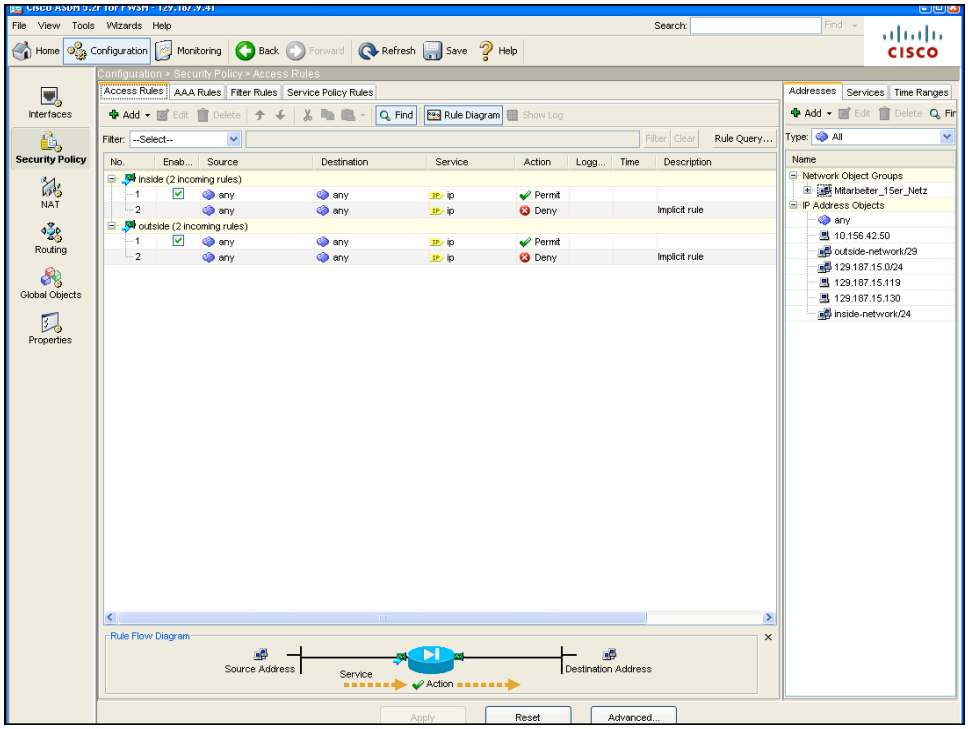
Integration der virt. FW beim Kunden: Technische Sicht

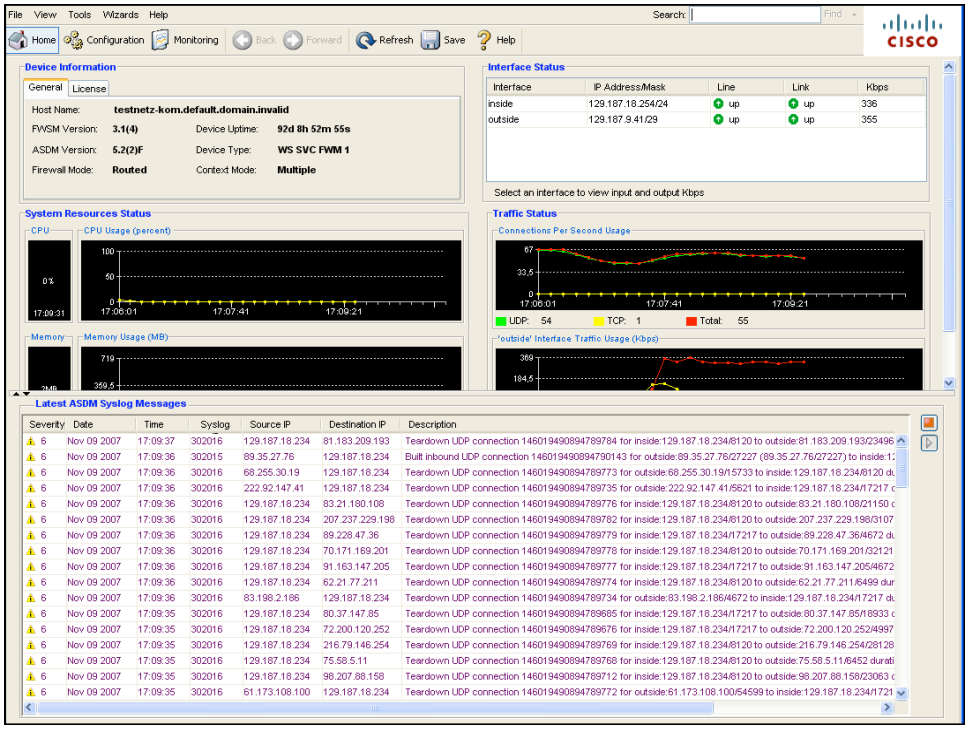
- „Platzierung“ der virtuellen Firewall vor Institutsnetz durch
  - Internes und
  - Externes VLAN



Dr. Helmut Reiser

43





Aufgaben Netzverantwortlicher / FW-Admin

- Netzverantwortlicher:
  - Multiplikator-Funktion
  - Bündelung der Interessen aus seinem Netzberich
  - Abstimmung bzgl. Betrieb einer Firewall (z.B. Betrieb pro Institut und nicht pro Lehrstuhl)
- Firewall-Admin
  - Konfiguration der Firewall
  - Betrieb, Aktualisierung und Wartung
  - Überwachung der Log-Dateien
  - Dazu: grundlegende Kenntnisse erforderlich
- Kurs: virtuelle Firewall im MWN
- Kontakt: firewall@lrz.de
- Info: www.lrz.de/services/security/virtuelle-fw/

Sicherheitsdienste des LRZ: Überblick

- Private IP-Adressen
- Virtuelles privates Netz (VPN)
- Bearbeitung von Missbrauchsfällen (ABUSE)
- Sicherheitsmeldungen von ABUSE
- NAT-o-MAT
- NYX
- MAC Flooding, schwarze Access Points
- Virtuelle Firewall
- Sperren im MWN
- E-Mail
- Viren: Sophos
- Windows Server Update Service (WSUS)

Beschränkungen und Sperren im MWN

- Port-Sperren am X-WIN Übergang
- Für ein- und ausgehenden Verkehr:

Protokol	Port	Dienst
TCP + UDP	42	WINS
TCP + UDP	135,137-139,445 ,539	MS-Netbios
TCP + UDP	1433, 1434	SQL-Server
UDP	213	IPX over IP

- Für eingehenden Verkehr

TCP	25	MAIL

Sperren und Monitoring im MWN

- Sonstige Filter:
  - IP-Spoofing Filter; nur MWN-Adressen von innen nach außen und nur nicht MWN-Adressen von außen nach innen
  - Broadcast Ping nach außen
- Beobachtung und ggf. Sperrung der Rechner bei:
  - Betrieb FTP Server aus Nicht-Standard Port (20 und 21)
  - Sehr viele Mail-Verbindungen in kurzer Zeit
  - Massive Portscans
  - Ungewöhnlich hoher Datenverkehr (2 GB pro Stunde bzw. 3 GB pro Halbtag)

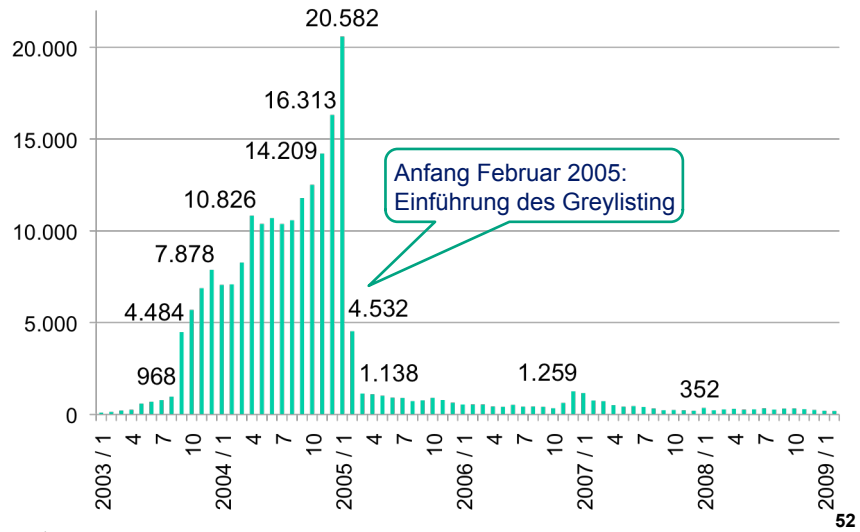
Sicherheitsdienste des LRZ: Überblick

- Private IP-Adressen
- Virtuelles privates Netz (VPN)
- Bearbeitung von Missbrauchsfällen (ABUSE)
- Sicherheitsmeldungen von ABUSE
- NAT-o-MAT
- NYX
- MAC Flooding, schwarze Access Points
- Virtuelle Firewall
- Sperren im MWN
- E-Mail
- Viren: Sophos
- Windows Server Update Service (WSUS)

E-Mail

- Nur bestimmte Mail-Server vom Internet aus erreichbar
- Jeder MWN-Rechner (Prüfung der IP-Adresse) darf E-Mails verschicken
- Zentrale Mail-Relays des LRZ:
  - Relay-Blocking
  - Ausgefeilte Spam-Abwehr (extrem erfolgreich ☺)
  - Spam-Tagging (SpamAssassin)
  - Blocken diverser Attachment-Typen
  - Viren-Filterung der Attachments (keine Benachrichtigung !)

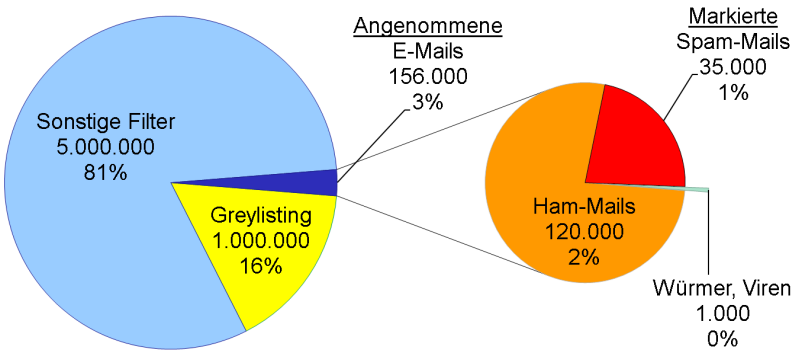
Persönliche Spam-Statistik seit 2003 von Dr. E. Bötsch



Spam-Abwehr am LRZ

Von den Mail-Relays pro Tag bearbeitete E-Mails

(Peak: 20.000.000 (!) E-Mails)



Insgesamt abgelehnte E-Mails
6.000.000, 97%

Beschränkungen bei Mail

- Syntaktisch korrekte Adresse
- Gültige Absender-Domain
- Empfängeradresse im MWN (für Mails aus dem Internet)
- Maximale Größe einer Mail
  - 30 MByte
- Anzahl der Mail
  - Soft-Event: 20 Mails in 5 Min oder 80 Mails in der Stunde
  - Hard-Event: 300 Mails/Minute oder 1000 Mails/h
- Bsp. PC der „Aldi-Klasse“ mit Fast-Ethernet Verbindung schafft:
  - 5.000 Mails/Min
  - 60.000 Mails/h

Viren und Virenscanner

- Virus: Programm oder Programmerweiterung, die
  - **Schaden** anrichten kann (Daten löschen, Spam versenden, Rechner zum Bot-Netz Client machen, usw.)
  - Sich selbst replizieren kann (**Infektion anderer Systeme**)
- Schutz vor Viren durch ständig aktualisierten Virenscanner

- LRZ: Sophos Anti-Virus Landeslizenz

Sophos Anti-Virus

- LRZ bietet (kostenlos) Virenscanner
- Nutzungsberechtigt:
  - Universitäten
  - Fachhochschulen
  - Akademische Einrichtungen
  - Komplette Liste: www.lrz.de/services/security/antivirus/institute/
  - Auch **private Nutzung** durch Bedienstete u. Studenten explizit erlaubt und erwünscht
- Flächendeckender Einsatz erwünscht!
- Automatische Aktualisierung der Virensignatur und Software
- Informationen: www.lrz.de/services/security/antivirus/

Sophos Nutzung

- Download und Installation des Clients
- Aktualisierung konfigurieren:
  - Automatische Aktualisierung (bei permanenter Verbindung ins MWN)
  - Manuelle Aktualisierung (VPN oder Wählverbindung)

- *Sophos Enterprise Manager* (SEM)
  - Eigener Update Server für größere Institute
  - Aktualisierung des SEM über LRZ Sophos Server

Windows Server Update Service (WSUS)

- Automatische Aktualisierung von Windows Rechnern im MWN
  - Auch für Systeme ohne Internet-Zugang
  - Keine Erfassung (oder Weiterleitung) von Nutzerdaten
- Updates für:
  - Windows Betriebssysteme
  - MS Produkte: z.B. Internet Explorer, MediaPlayer, usw.
  - MS Office
  - MS Exchange
  - SQL Server
  - Treiber

WSUS Gruppen und Konfiguration

- Zielgruppen:
  - WSUS (vom LRZ empfohlene Gruppe): Updates, Sicherheitsupdates, Patches f. Windows, Office und MSDE
  - AllUpdates: Alle von MS freigegebene Updates
  - Server: WSUS + Sharepoint, SQL Server, Exchange
- Service Packs werden NICHT über WSUS verteilt; Download über www.lrz.de/services/security/mwnsus/
- Konfiguration:
  - Schritt für Schritt Anleitung unter www.lrz.de/services/security/mwnsus/#Konfiguration

Inhalt

- Sicherheitsleitlinie des LRZ
- Basiswissen
- Aufgaben des Netzverantwortlichen
- Sicherheitsdienste des LRZ und Abuse Bearbeitung
  - ...
- Konkrete Beispiele
- Informationsquellen

Aufgaben des NV an praktischen Beispielen

- Erhöhter Mail Versand
- Copyright Verletzungen
- Port Scan und Denial of Service (DoS) Angriff
- Erhöhter Datenverkehr

- Aktionen des Netzverantwortlichen

Erhöhter Mail Versand

- Zwei Rechnerklassen:
  1. Legitimer Mailserver (Adresse in Ausnahmeliste)
  2. Sonstige Rechner (Adresse **nicht** in Ausnahmeliste)
- Grenzwerte für Sonstige:
  - Soft-Limit: 20 Mails in 5 Min oder 80 Mails in der Stunde
  - Hard-Limit: 300 Mails/Minute oder 1000 Mails/h
- Überschreitungen:
  - Mehrmaliges Überschreiten des Soft-Limits
  - ➡ Information an Netzverantwortlichen
  - Einmaliges Überschreiten des Hard-Limit
  - ➡ Sperrung der Adresse am X-Win Übergang; Information an Netzverantwortlichen

Urheberrechtsverletzungen

- Z.B. Anbieten von geschütztem Material über BitTorrent
- Rechteinhaber ermittelt (über spezialisierte Firma) IP-Adresse des Anbieters
- Evtl. Einschaltung von Strafverfolgungsbehörden
- Beschwerde oder Anfrage der Ermittlungsbehörden beim LRZ (da LRZ Inhaber der Adresse (whois))
- Weiterleitung der Beschwerde an zust. Netzverantwortlichen

Port Scan oder Denial of Service (DoS) Angriff

- Grenzwerte:
  - Portscan: 1000 Verbindungsversuche / 5 min.
    5000 Verbindungsversuche / 1 h
  - DoS; Asymmetrisches Verkehrsverhalten:
    - Durchschnittliche Packetlänge < 100 Byte UND
    - Verhältnis eingehender Verkehr zu ausgehendem Verkehr > Faktor 1500
- Überschreitungen:
  - Bei wiederholter Überschreitung:
    - ➡ Information an Netzverantwortlichen
  - Erhebliche Überschreitung
    - ➡ Sperre am X-Win
    - ➡ Information an Netzverantwortlichen

Erhöhter Datenverkehr

- Grenzwerte:
  - 2 Gigabyte / h
  - 3 Gigabyte / Halbtag
- Überschreitung
  - ➡ Information an Netzverantwortlichen

(Re-) Aktion des Netzverantwortlichen auf Info

- Information an Netzverantwortlichen (NV)
- NV ermittelt lokalen Administrator der Maschine
  - Administrator wird informiert
  - Administrator überprüft und säubert (ggf.) den Rechner
  - Administrator meldet Ergebnis an NV
- NV meldet Ergebnis an LRZ, abhängig davon:
  - LRZ hält Sperre aufrecht
  - LRZ schaltet Rechner wieder frei
  - LRZ sperrt Rechner erstmalig
- NV reagiert **nicht** zeitnah auf die Info:
  - IP Adresse wird gesperrt (falls nicht eh schon gesperrt wurde)

Information und Beratung

- Netzdoku für Netzverantwortliche:
  http://netzdok.lrz-muenchen.de:8080/Netzdoku/index_extern_html

- Security-Seiten des LRZ: www.lrz.de/services/security/
- Diverse Mail-Adressen: <abuse@lrz.de>, security@lrz.de
- Security-Einführungskurs für Anwender
  (wird auf Wunsch auch vor Ort angeboten!)
- Security-Kurs für UNIX-Systemverwalter
- Diverse Mail-Verteiler: DFN-CERT-Subverteiler,
  security-news@lists.lrz.de

Vielen Dank

Fragen?