Security im MWN : Aktuelle Situation, Dienste und Erfahrungen eines Uni-RZ

V. Apostolescu, E. Bötsch, P. Eilfeld
Th. Fakler, A. Haarer, M. Storz, C. Wimmer

`http://www.lrz.de/services/security/`

Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften
Barer Str. 21, 80333 München

Security im MWN : Agenda

- **Motivation und Grundregeln für Security**
- **Das Leibniz-Rechenzentrum (LRZ)**
- **Das Münchner Wissenschaftsnetz (MWN) : Überblick**
- **Aktuelle Situation und Erfahrungen**
- **Security-relevante Dienste des LRZ**
  - Netz-Security und Firewalls
  - Microsoft Update Service
  - Schutz vor Viren und Würmern
  - Spam-Mails und Viren-Filterung
  - Kurse und Online-Informationen

Warum ist System- und Netz-Sicherheit so wichtig ? (1)

Potentielle und teilweise schwerwiegende Folgen :

- **Hacker-Angriff bzw. Verseuchung mit Virus / Wurm**
  - ⇨ **Daten-Verlust und/oder Neu-Installation**
- **0190-Dialer**
  - ⇨ **Telefonrechnung von mehreren 100 - 10 000 €**
- **Geknackte Rechner sind oft Ausgangspunkt für weitere Aktivitäten**
  - "Sprungbrett" für weitere Einbrüche
  - (Distributed) Denial of Service-Angriffe ((D)DOS-Attacks)
  - "Verteil-Station" für Copyright-geschütztes oder rechtlich bedenkliches Material sowie für Viren, Würmer, Flames, Spams etc.
  - "Abhörstation"

Warum ist System- und Netz-Sicherheit so wichtig ? (2)

- **Organisatorische und/oder finanzielle Folgen (Provider kündigt Vertrag o.ä.)**
- **Technische Folgen (z.B. Probleme mit "schwarzen Listen")**
- **"Soziale" und/oder finanzielle Folgen (Image-Verlust, Umfeld-Schädigung)**
- **Zivilrechtliche Ansprüche mit u.U. finanziellen Folgen, zumindest wegen (grober) Fahrlässigkeit**
- **Strafrechtliche Folgen (z.B. bei falschem Verdacht)**

Wichtige Security-Grundregeln

- Security ist kein überflüssiger Luxus; keine Security ist teurer !!!
- Security gibt es nicht umsonst
  (⇨ Geld, Person-Power, Bequemlichkeit)
- 100% Security ist *prinzipiell unmöglich* ⇨ 80%-Lösung
- Security ist nicht dauerhaft !
  Bruce Schneier: Security is not a product; it's a process.
- Bewusstheit, Information und *Konsequenz* sind unverzichtbar
  (Kombination technischer, organisatorischer und psychologischer Maßnahmen)

Fazit :

- Jede(r) ist mitverantwortlich, nicht nur Systemverwalter(innen)
- Nerven behalten (ggfs. nachfragen) und sich regelmäßig informieren

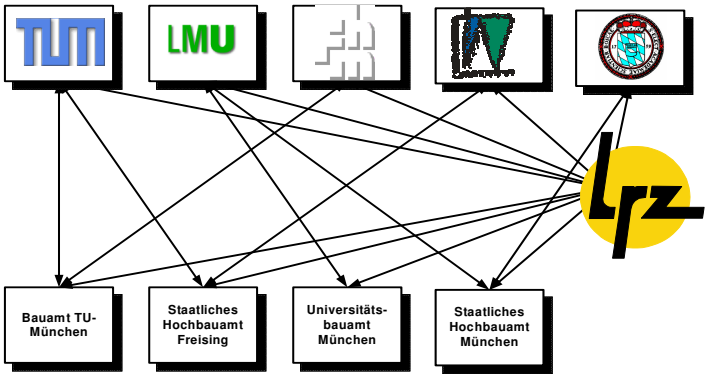
Das Leibniz-Rechenzentrum (LRZ)

Aufgaben :

- Wissenschaftliches Rechenzentrum für die Hochschulen in München und die Bayerische Akademie der Wissenschaften
- Zentrum für technisch-wissenschaftliches Hochleistungsrechnen ("Supercomputing Center")
- Zentrale für die Archivierung großer Datenmengen, die auch die automatische Datensicherung der Rechner im Münchner Wissenschaftsnetz (MWN) anbietet
- Verantwortlich für Planung, Ausbau und Betrieb des *Münchner Wissenschaftsnetzes* (MWN) und Kompetenzzentrum für Datenkommunikationsnetze

Das Leibniz-Rechenzentrum (2)

Enge Zusammenarbeit bei der Planung und dem Ausbau des Münchner Wissenschaftsnetzes



Das Münchner Wissenschaftsnetz (MWN)

<u>Betrieben vom LRZ</u> :

- **Planung, Aufbau und Betrieb**
- **Anbindung an nationale und internationale Forschungsnetze (G-Win)**
- **Zugriff auf das DV-Netz über Wählanschlüsse**
- **Bereitstellung zentraler Netzdienste :**
  DNS, IP-Adressverwaltung, E-Mail, WWW-Server, Proxies und Cache-Server, Firewall, Radius, VPN-Server, Mulicast, DHCP, FTP, Video-Server (zentral am LRZ), VoIP, Video-Conferencing, Vorlesungsübertragung innerhalb des MWN, Backup- und Archivierung (zentral am LRZ, ca. 1,6 TB/Tag, 320 TB Kapazität)
- **Beratung und Schulung in Kommunikationsfragen**

Das Münchner Wissenschaftsnetz (2)

Genutzt von :

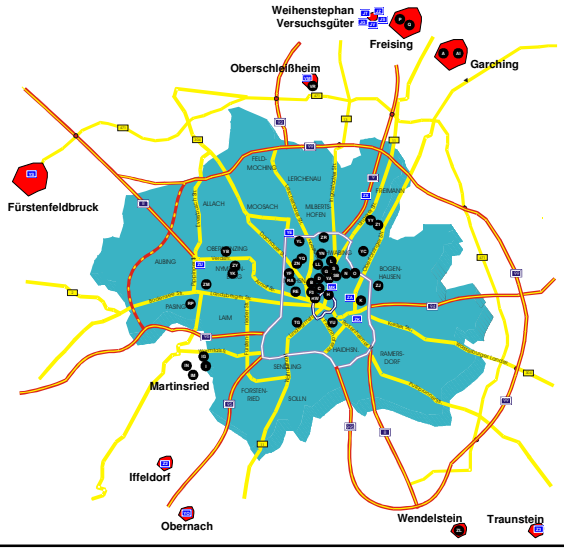
- ❒ **Bayerische Akademie der Wissenschaften**
- ❒ **Ludwig-Maximilians-Universität München**
- ❒ **Technische Universität München**
- ❒ **Fachhochschule München**
- ❒ **Fachhochschule Weihenstephan**

} Bis zur Datensteckdose

- ❒ **Max-Planck-Institute in München**
- ❒ **Fraunhofer-Gesellschaft**
- ❒ **Bayerische Staatsbibliothek**
- ❒ **Hochschule für Film und Fernsehen**
- ❒ **Studentenwerk München (inkl. Studentenwohnheime)**
- ❒ **Studentenwohnheime anderer Träger**
- ❒ **usw.**

} Bis zur Router-schnittstelle

Standorte des MWN



- ❒ **Ca. 40 Areale**
- ❒ **Ca. 200 Gebäude**

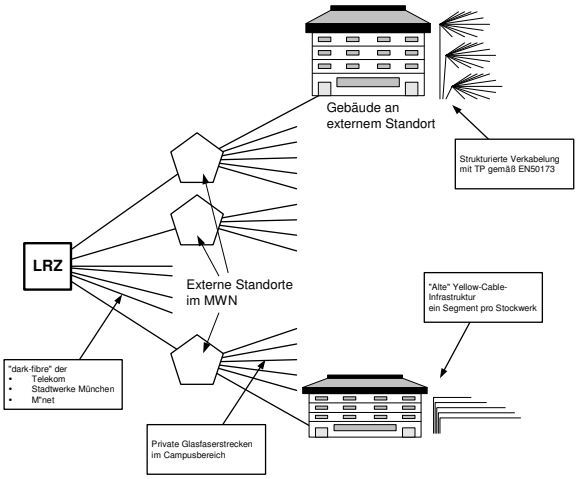
Legende :

Q Anschluß > 10 MBit/s (1000 MBit/s, 100 MBit/s)

ZR Anschluß < 10 MBit/s (Funklan, xDSL, 2 MBit/s oder 64 kBit/s)

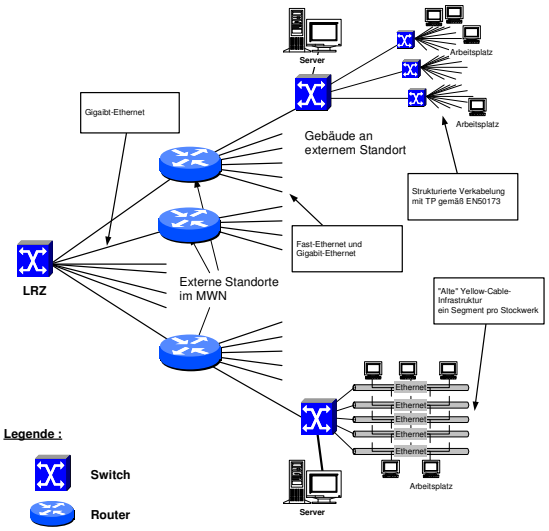
Stand : 01.07.2003 / Apo

Netzstruktur des MWN : Verkabelung



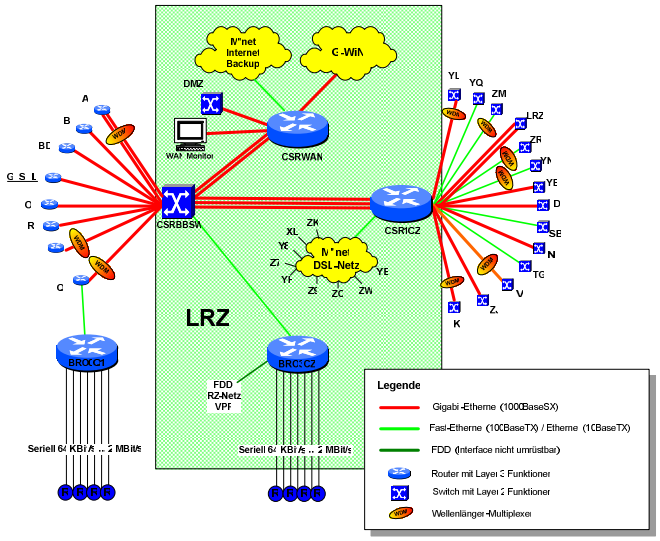
- ❒ Ca. 40 Areale
- ❒ Ca. 200 Gebäude
- ❒ Ca. 19.000 Räume
- ❒ Verkabelung :
  - Ca. 80 % Glas-faser und Twisted-Pair (strukturiert)
  - Ca. 20 % Koax

Netzstruktur des MWN : Aktiv



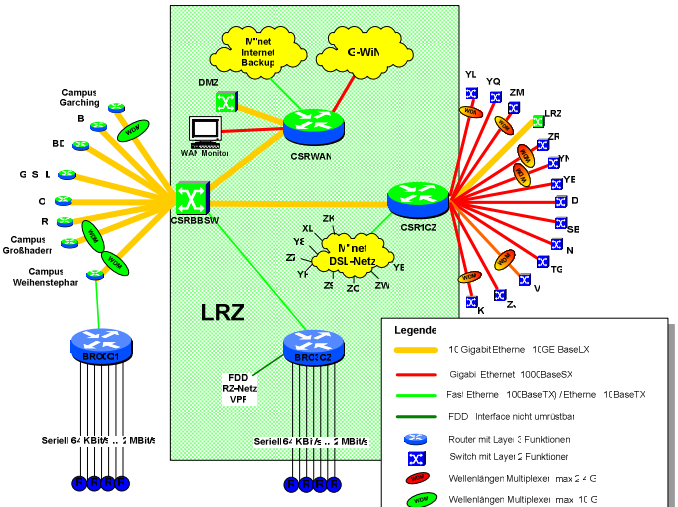
- ❒ 10 Backbone-Router
- ❒ Ca. 10 „kleine“ Router
- ❒ Ca. 400 LANs
- ❒ Ca. 800 LAN-Switches
- ❒ Ca. 35.000 Switch-Ports
- ❒ Ca. 50.000 Endgeräte

Netzstruktur des MWN : Backbone-Netz



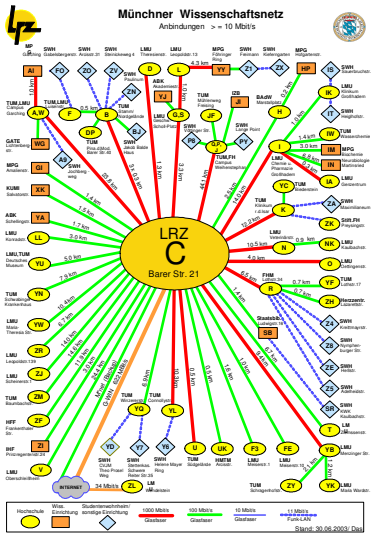
13

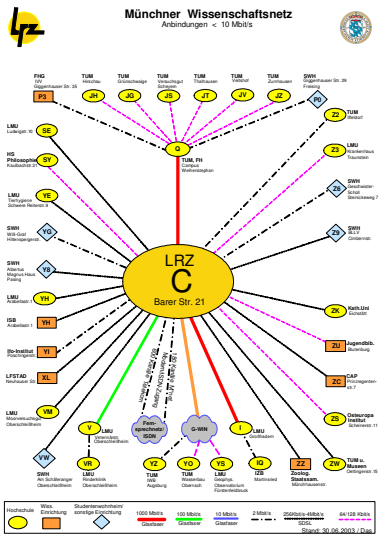
Netzstruktur des MWN : Backbone-Netz in nächster Zukunft



14

MWN : Anschlüsse





MWN : Einige Fakten für die Statistik

- **Ca. 80.000 Studenten**
- **Ca. 26.000 Personen Personal (davon 8.500 wissenschaftliches Personal)**
- **Ca. 50.000 Rechner**
- **Derzeit 30 Studentenwohnheime im MWN, ca. 8.000 Wohnheimsplätze vernetzt**
- **Außenanbindung: G-WiN (1 Gbit/s)**
  - Ca. 15.2 TByte empfangene / ca. 28.5 TByte / Monat gesendete Daten
- **Etwa 1.200.000 E-Mails pro Tag über das Mail-Relay des LRZ.**
- **Etwa 1.6 TByte werden pro Tag für Backup und Archiv über das MWN zum Archiv-Server ins LRZ transportiert und ca. 0.033 TByte abgeholt.**
- **Etwa 15.000 Wählverbindungen pro Tag über die vom LRZ-betriebenen Modemzugänge.**
- **Etwa 1000 Verbindungen pro Tag zu den VPN-Servern**
- **Kosten :**
  - Ca. 1 Mio € für den Betrieb des MWN
  - 450 T€ für die Internet-Anbindung des MWN

Partner im MWN : Arealbetreuer (LRZ) ↔ Netzverantwortliche (Institute etc.)

Richtlinien zum Betrieb des Münchner Wissenschaftsnetzes (MWN) :
➟ `http://www.lrz-muenchen.de/wir/regelwerk/`

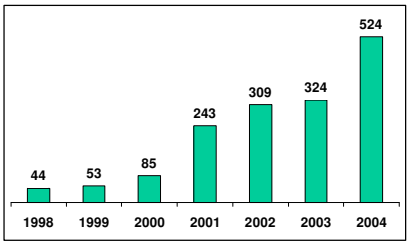
Netzverantwortliche :
- ❒ Zuständig für einen Bereich (am besten physisch, z.B. für ein Gebäude)
- ❒ (Einzige) Schnittstelle zum LRZ (Arealbetreuer) in Netzfragen
- ❒ Schnittstelle für Benutzer in seinem Bereich für Netzfragen
- ❒ Aufgaben : Dokumentation, Netzadressen, Fehlerverfolgung, Planung und Inbetriebnahme von Erweiterungen der Gebäudenetze

Arealbetreuer :
- ❒ Schnittstelle zu den Netzverantwortlichen seines Areals
- ❒ Weiterleiten von Anfragen an den Zuständigen im LRZ
- ❒ Aktives Verfolgen anstehender Installationen und Probleme

➟ `http://www.lrz.de/services/netz/`

Abuse-Fälle im MWN (1)

- ❒ **Arten von Abuse-Fällen :**
  - Von Hackern geknackte oder mit Würmern (seltener Viren) infizierte Rechner
  - Unberechtigte (Spam-)Beschwerden
  - Anfragen von MWN-Benutzern
  - Fehlverhalten von MWN-Benutzern (absichtlich und unabsichtlich)
- ❒ **Zahl der nicht automatisiert bearbeiteten Vorgänge :**



Abuse-Fälle im MWN (2)

Wie werden kompromittierte Rechner erkannt ?

- **Netzüberwachung durch das LRZ :**
  - FTP-Server auf Nicht-Standard-Ports (voll automatisiert)
  - Port-Scans (noch halbautomatisch)
  - Ungewöhnlich hohes Übertragungsvolumen eines Rechners (noch Handarbeit)
- **Hinweise / Beschwerden von außerhalb (und aus dem MWN) :**
  - SpamCop
  - Automatische Tools
  - Kollegiale / verärgerte Benutzer

Abuse-Fälle im MWN (3)

Bearbeitung eines Falls durch das LRZ :

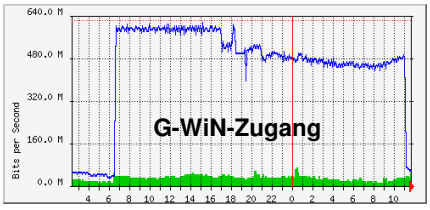
➟ `http://www.lrz.de/services/security/abuse/`

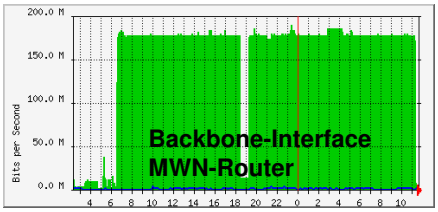
- **Antwort an den Beschwerdeführer**
- **Weiterleitung an den zuständigen Netzverantwortlichen**
- **Sperren einer Kennung oder Sperren eines Rechners am Übergang zum G-Win (etwas schwerere Fälle)**
- **Individuelles Eskalationsverfahren (Einzelentscheidungen, da sehr selten)**

Security :
Ein kleiner Wurm mit großer Wirkung

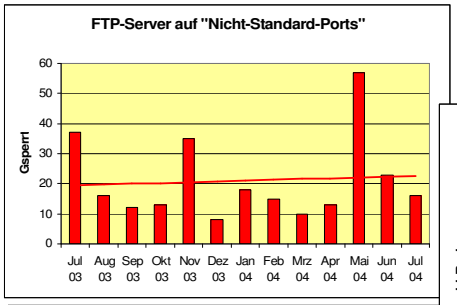
SQL-Slammer :

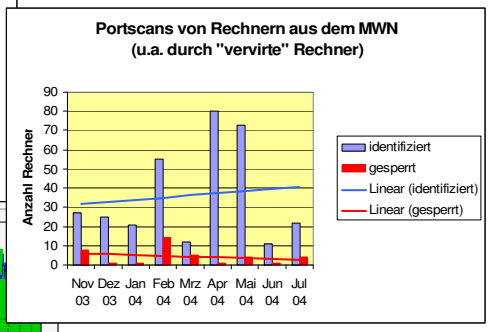
- **Vorfall vom 25.01.03**
- **Betroffen**
  - MS-SQL-Server
  - Rechner mit integriertem, abgespecktem MS-SQL-Server (!!)
- **Sicherheitspatch verfügbar seit 6 (!) Monaten**
- **Auswirkung :**

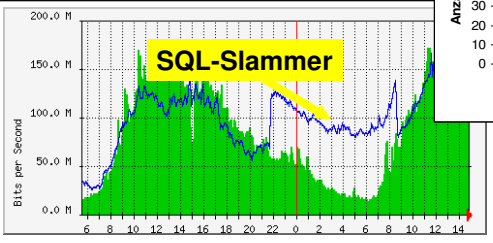




Statistiken („das reale Leben“) :
FTP-Server und Port-Scans ausgehend

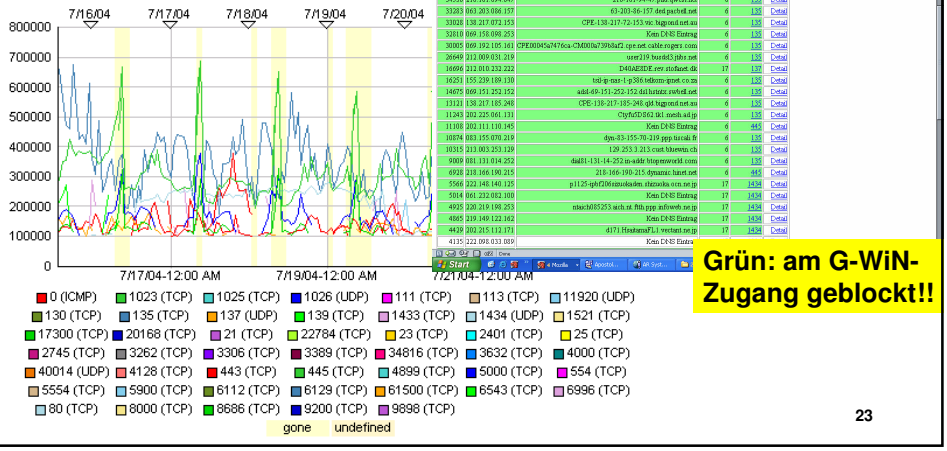






Statistik : Port-Scans eingehend

Messintervall 1 h !!



Grün: am G-WiN-Zugang geblockt!!

Indirekte Opfer von Spammern und Würmern

Spammer und die aktuellen Viren / Würmer fälschen bei den E-Mails praktisch immer die Absender-Adresse.

⇒ Für eine E-Mail, die man *nicht selbst* verschickt hat, erhält man

- eine oder mehrere Fehlermeldungen, weil
  - eine Empfänger-Adresse nicht existiert.
  - die E-Mail einen Virus / Wurm enthält.
- eine Beschwerde-E-Mail, dass man eine Spam-Nachricht oder einen Virus / Wurm verschickt hat.

⇒ Eine E-Mail mit *problematischem Inhalt* und der *eigenen Adresse* als Absender landet im Web-Archiv eines E-Mail-Verteilers und ist dann durch Such-Maschinen recherchierbar.
Beispiel : Der Wurm Sober.H hatte massenhaft Spam-E-Mails mit rassistischem und ausländerfeindlichem Inhalt verschickt.

Security-relevante Dienste des LRZ (1)

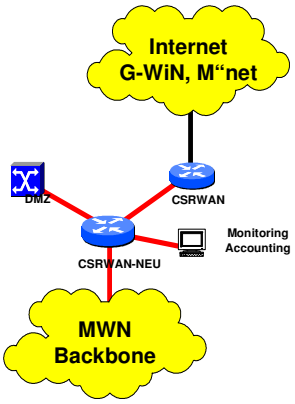
- **Informations- und Beratungs-Angebote des LRZ :**
  - Für Notfälle : Hotline des LRZ (`hotline@lrz.de` bzw. 289-28800)
  - Online-Informationen ⇨ Security-Portal des LRZ
  - Security-Kurse: für Anwender; neu: für *UNIX*-Administratoren
  - Security-Sprechstunde (*konzeptionelle* bzw. *übergreifende* Probleme)
  - Arbeitskreis "Firewall im MWN"
- **E-Mail-Adressen für :**
  - (Vermutete) Einbruchs-Versuche : `security@lrz.de`
  - (Vermutete) Angriffe aus dem MWN : `abuse@lrz.de`
  - Firewall-Probleme / -Fragen : `firewall@lrz.de`
  - Sonstige / unklare Probleme : `security@lrz.de`

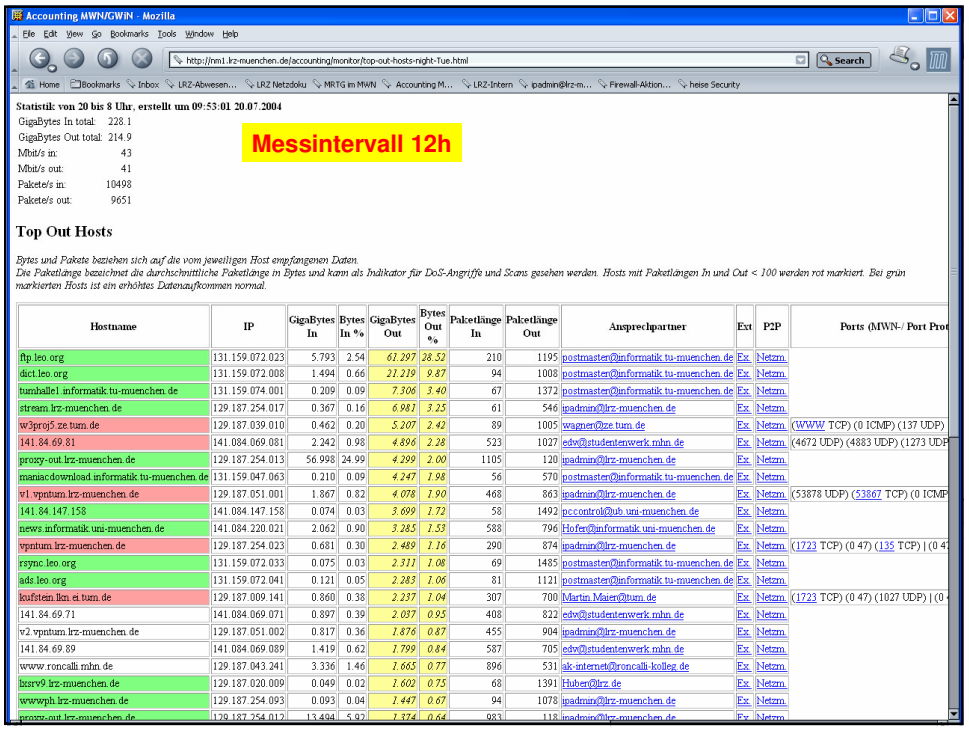
Security-relevante Dienste des LRZ (2)

- **E-Mail-Verteiler :**
  - "Repost" von Security-relevanten Informationen aus div. Quellen
  - *MWN-spezifische* Security-relevante Informationen
  - Sub-Verteiler für Infos des **C**omputer **E**mergency **R**esponse **T**eams des **D**eutschen **F**orschungs-**N**etzes (DFN-CERT)
- **Private IP-Adressen, Firewalls, Virtual Private Networks (VPN)**
- **Software-Update-Service (SUS) für Windows**
- **Antiviren-Software**

Netzseitige Sicherheit (reaktiv) : Accounting und Monitoring

- **Portspiegelung am Router**
- **Erfassung aller Pakete**
- **OS-SW IP-Audit auf Linux-PC**
- **Auswertung nach IP-Adresse (Host)**
  - Transportierte Bytes, transportierte Pakete, Portnummer, Flows (Connections)
- **Statistiken (Aufbewahrung bis zu 1 Woche)**
  - Zeitfenster: 5 min, 1 h, Tag (8:00-20:00), Nacht (20:00-8:00)
  - Top In Hosts, Top Out Hosts
- **Subnetzstatistik tageweise**





Hostname	IP	GigaBytes In	Bytes In %	GigaBytes Out	Bytes Out %	Paketlänge In	Paketlänge Out	Ansprechpartner	Ext	P2P	Ports (MWN-/ Port Prot
ftp.leo.org	131.159.072.023	5.793	2.54	61.297	38.52	210	1195	postmaster@informatik.tu-muenchen.de	Ex.	Netzm.	
dict.leo.org	131.159.072.008	1.494	0.66	21.219	9.87	94	1008	postmaster@informatik.tu-muenchen.de	Ex.	Netzm.	
turnhalle1.informatik.tu-muenchen.de	131.159.074.001	0.209	0.09	7.306	3.40	67	1372	postmaster@informatik.tu-muenchen.de	Ex.	Netzm.	
stream.lrz-muenchen.de	129.187.254.017	0.367	0.16	6.981	3.25	61	546	ipadmin@lrz-muenchen.de	Ex.	Netzm.	
w3proj5.ze.tum.de	129.187.039.010	0.462	0.20	5.207	2.42	89	1005	wagner@ze.tum.de	Ex.	Netzm.	(WWW TCP) (0 ICMP) (137 UDP)
141.84.69.81	141.084.069.081	2.242	0.98	4.896	2.28	523	1027	edv@studentenwerk.mhn.de	Ex.	Netzm.	(4672 UDP) (4883 UDP) (1273 UDP
proxy-out.lrz-muenchen.de	129.187.254.013	56.998	24.99	4.299	2.00	1105	120	ipadmin@lrz-muenchen.de	Ex.	Netzm.	
maniac.download.informatik.tu-muenchen.de	131.159.047.063	0.210	0.09	4.247	1.98	56	570	postmaster@informatik.tu-muenchen.de	Ex.	Netzm.	
w1.vpntum.lrz-muenchen.de	129.187.051.001	1.867	0.82	4.078	1.90	468	863	ipadmin@lrz-muenchen.de	Ex.	Netzm.	(53878 UDP) (53867 TCP) (0 ICMP
141.84.147.158	141.084.147.158	0.074	0.03	3.699	1.72	58	1492	pccontrol@ub.uni-muenchen.de	Ex.	Netzm.	
news.informatik.uni-muenchen.de	141.084.220.021	2.062	0.90	3.285	1.53	588	796	Hofer@informatik.uni-muenchen.de	Ex.	Netzm.	
vpntum.lrz-muenchen.de	129.187.254.023	0.681	0.30	2.489	1.16	290	874	ipadmin@lrz-muenchen.de	Ex.	Netzm.	(1723 TCP) (0 47) (135 TCP) | (0 47
rsync.leo.org	131.159.072.033	0.075	0.03	2.311	1.08	69	1485	postmaster@informatik.tu-muenchen.de	Ex.	Netzm.	
ads.leo.org	131.159.072.041	0.121	0.05	2.283	1.06	81	1121	postmaster@informatik.tu-muenchen.de	Ex.	Netzm.	
kaufstein.lkn.ei.tum.de	129.187.009.141	0.860	0.38	2.237	1.04	307	700	Martin.Mauer@tum.de	Ex.	Netzm.	(1723 TCP) (0 47) (1027 UDP) | (0
141.84.69.71	141.084.069.071	0.897	0.39	2.037	0.95	408	822	edv@studentenwerk.mhn.de	Ex.	Netzm.	
v2.vpntum.lrz-muenchen.de	129.187.051.002	0.817	0.36	1.876	0.87	455	904	ipadmin@lrz-muenchen.de	Ex.	Netzm.	
141.84.69.89	141.084.069.089	1.419	0.62	1.799	0.84	587	705	edv@studentenwerk.mhn.de	Ex.	Netzm.	
www.roncalli.mhn.de	129.187.043.241	3.336	1.46	1.665	0.77	896	531	ak-internet@roncalli-kolleg.de	Ex.	Netzm.	
bisrv9.lrz-muenchen.de	129.187.020.009	0.049	0.02	1.602	0.75	68	1391	Huber@lrz.de	Ex.	Netzm.	
wwwph.lrz-muenchen.de	129.187.254.093	0.093	0.04	1.447	0.67	94	1078	ipadmin@lrz-muenchen.de	Ex.	Netzm.	
proxy-out.lrz-muenchen.de	129.187.254.012	13.494	5.92	1.374	0.64	983	118	ipadmin@lrz-muenchen.de	Ex.	Netzm.	

Maßnahmen aufgrund der Messungen

- **Untersuchung der Rechner**
  - Gehackte Rechner (mehr als 250 in 2003)
  - Freizügige Konfiguration
  - Peer-to-Peer-Protokolle
  - FAN- und Spiele-Server
- **E-Mail an Netzverantwortliche**
  - ⇨ Gehackte Rechner werden gesperrt (Liste hat mittlerweile 312 Einträge)
- **Brief an alle Lehrstühle und weitere Institutionen**
  - ➟ `http://www.lrz.de/services/security/sec-brief/`
- **Portsperren am G-WiN Zugang**
  - ➟ `http://www.lrz.de/services/netz/einschraenkung/`
- **Erfahrungen**
  - Sehr positiv (NV), Kontrolle eigener Bemühungen

Netzseitige Sicherheit (reaktiv) : Intrusion Detection System (IDS)

- **Erfassung aller Pakete wie bei Accounting und Monitoring**
- **Analyse der Pakete auf Applikationsebene**
- **Analysewerkzeug: Snort auf Linux-PC**
  - Charakteristisches Bitmuster eines bekannten Missbrauchs heißt Signatur
  - Snort scannt Datenstrom nach gewünschten Signaturen und gibt im Erfolgsfall Warnung aus
- **Aktuelle Signaturen**
  - FTP-Server auf Nicht-Standardport
    Die Praxis zeigt, daß ein derartiger Rechner höchstwahrscheinlich kompromitiert ist
  - Port-Scans (externer Maschinen)
- **Maßnahmen**
  - FTP-Server : Automatische Sperre am G-WiN-Zugang + E-Mail an die NVs
  - Port-Scans : Automatische Generierung einer E-Mail, Versand „zu Fuß“
- **Umfassende Suche nach missbräuchlichen Aktivitäten scheitert derzeit an Performanz-Problemen**

Netzseitige Schutzmaßnahmen

- **Differenzierung zwischen Server-Systemen**
  - Dienste evtl. ans LRZ auslagern
    - WWW-Server
    - Mail-Server
    - DNS-Server
    - DHCP-Service, ...
- **und Mitarbeiterarbeitsplätzen**
- **Selektive Nutzung privater und offizieller IP-Adressen**
- **Firewalls**
  - Firewall im LRZ-Router
  - Eigene Firewall für Institution bzw. Arbeitskreis

Netzseitige Sicherheit (proaktiv) : Gibt es das sichere Netz ?

- **Nur wer sein Netz vollkommen von der Außenwelt isoliert, ist wirklich sicher !**
- **Es muss zwischen Anwenderwünschen und Sicherheit ein Kompromiss gefunden werden.**
- **Wichtig ! Es muss ein Sicherheitskonzept erstellt werden.**
- **So viel Sicherheit wie möglich, so viel Freiheit wie nötig !**
- **Sicherheit kostet ...**
  - Freiheit
  - Aufwand (Personpower für Einrichten und Betrieb)
- **... manchmal aber weniger als man denkt !**
  - Spart *viel* Arbeit, wenn man von Angriffen verschont bleibt.

Was tun ? ⇨ Abgestufte Lösungen

- **Firewall-Funktionen im G-WiN Zugang**
- **Firewall-Funktionen im Router-Interface zum Institut**
- **Änderungen im Institutsnetz :**
  - Eigenen Rechner nach Dienstschluss abschalten
    - Schont die Umwelt in mehrfacher Hinsicht
    - Reduziert die Angriffsfläche um 80 %
  - Private IP-Adressen
  - Eigene Firewall betreiben
  - ➟ http://www.lrz.de/services/security/sicherheitspakete-lrz/

Erhöhte Sicherheit durch Funktionen der Router im MWN

- **Filter**
  - Beliebige Absende- und Zieladressen können gesperrt oder erlaubt werden
  - Statische (i.d.R. für generelle Zugriffsbeschränkungen) und dynamische Filter
  - Performance-Einschränkungen
    - bei statischen Filtern i.d.R. keine
    - bei dynamischen Filtern (reflexive Filter) vorhanden (aktuelle Architektur)
  - Eine Gruppe von Filtern heißt Access-Control-List (ACL)
- **G-WiN Zugang (generelle MWN Policy)**
  - Port-Sperren, Anti-Spoofing-Filter, Filter gegen Spammer (Einschränkung von Port 25), Filter gegen Konfigurationsfehler bei DNS usw.
    ➟ `http://www.lrz.de/services/netz/einschraenkung/`
- **Übergang zum Institutsnetz (Routerinterface)**
  - Institutsspezifische ACLs sind betreuungsaufwändig
    - Fehlende Personpower am LRZ (ca. 400 Interfaces)
    - Deshalb nur generelle Filter möglich
  - Anti-Spoofing, Broadcast-Filter und Standard-Filter für Institute (generell)

Firewall durch Standard-Filter auf dem MWN-Router-Interface

- **Option 1 : Reflexive Filter**
  - Standard-Filter mit dynamischer (reflexiver) ACL auf MWN-Router
    - Dynamische Filter werden vom Router selbst erzeugt
    - Diese Filter haben nur eine begrenzte Lebensdauer
    - Die Erzeugung wird durch einen statischen Filter angestoßen
  - Aktivierung Standard-Filter vor Instituts-Subnetz
    - Instituts-Subnetz von extern nicht mehr erreichbar
    - Aus dem Instituts-Subnetz ist Kommunikation wie zuvor möglich
    - Kombination mit privaten IP-Adressen möglich
  - Optionale DMZ
    - DMZ wird **nicht** von Standard-Filter geschützt – systemseitige Absicherung
- **Option 2 : Sperrung der relevanten Microsoft-Ports**
  (135, 137, 138, 139, 445, 593, 1433 und 1434)
- **Option 3: „Veranstaltungsnetz“ (testweise auch für Institute)**
  „Alles ist verboten, was nicht explizit erlaubt ist !“

Private IP-Adressen

- **Keine Weiterleitung der IP-Pakete (Routing) ins G-WiN (Internet)**
- **Kein IP-Paket (Angriff) aus dem Internet erreicht Rechner**
- **Routing nur im MWN, Angriff aus dem MWN möglich**
- ⇨ **Nur 50.000 potentielle Angreifer statt 160.000.000**
- **Nutzung von Diensten im Internet über Proxies**
- **Am LRZ verfügbare Proxies:**
  WWW-Proxy, FTP-Proxy, Socks-Proxy, H.323-Proxy
  ➟ `http://www.lrz.de/services/netzdienste/proxy/`
- **Nicht alle Dienste werden (sofort) verfügbar sein**
- **Spezielle Konfiguration oder Software teilweise notwendig**
- **Privates IP-Subnetz wird vom LRZ zugeteilt**
- **Studentenwohnheime haben und viele Institute nutzen mittlerweile private IP-Adressen**

⇨ **Erster Schritt hin zu einer eigenen Firewall**

Änderungen am Instituts-Subnetz als Basis für eine Firewall

- **Voraussetzungen**
  - Strukturierte Verkabelung (KOAX nur in extremen Ausnahmen)
  - Instituts-Subnetz wird nicht mit anderen Instituten geteilt (außer die beteiligten Institute sind sich über Sicherheitsstrategie einig)
- **Mögliche Änderungen**
  - Auslagerung zentraler Dienste ans LRZ: WWW, E-Mail, DNS, ...
  - Einrichten eines zweiten Subnetzes (DMZ) für vom Institut betriebene Server (nicht auslagerbar, extern erreichbar)
  - Tausch des Switches
  - Einrichten und Verwalten von VLANs („arbeitsintensiv“)
  - Einrichten eines Transportnetzes für eigene Routing Firewall
- **Ziel**
  - Instituts-Subnetz ohne extern erreichbare Server
  - Separiertes Subnetz (DMZ) für Server
  - Eindeutig definierter Netzübergang

Betrieb einer eigenen Firewall

- **Kontinuität in der Wartung muß gewährleistet sein**
- **Transparente Firewall (Bridge)**
  - Vor Institutsnetz
  - Vor DMZ
  - Kombination mit Router-Filtern möglich
  - Routing übernimmt LRZ-Router
  - Bei Hardware-Defekt kann transparente Firewall problemlos überbrückt werden
- **Routing Firewall**
  - Vor Institutsnetz und DMZ
  - Flexibilität beim Einsatz weiterer (privater) Subnetze
  - Routing übernimmt eigene Routing Firewall
  - Bei Hardware-Defekt kann Routing Firewall nicht überbrückt werden

Wie kann man Rechner *selbst* schützen ?

- **Einrichten einer Firewall (auch lokal; in Windows XP bereits integriert; SP2 mit erweiterter Funktionalität)**
- **Einspielen aktueller Security-Patches:**
  Windows:
  - Software Update Service (SUS) am LRZ
    ➟ `http://www.lrz.de/services/security/mwnsus/`
  - Automatisches Einspielen durch „Windows Update“ oder SUS (siehe z.B. Beiträge in c't 21/2003)
  - MS-Security-Portal (Tipps, Tools, Bulletin, Newsletter, ...)
    ➟ `http://www.microsoft.com/germany/ms/security/`

  Informationen zu allen Betriebssystemen:
  - E-Mail-Verteiler „win-sec-ssc“ des DFN-CERT.
    Archiv ➟ http://www.lrz.de/services/netzdienste/email/email-archive/
    (mit Informationen zum Eintragen in den Verteiler)
- **Verwendung aktueller (!) Anti-Viren-Software**

Grundsätzliches zur LRZ-Landeslizenz für Sophos-Anti-Virus

- Anti-Virus-Seite
  ➟ http://www.lrz.de/services/security/antivirus/
- Das LRZ hat für alle Hochschulen und Fachhochschulen Bayerns eine Landeslizenz für die Anti-Viren-Software von Sophos abgeschlossen
  ➟ http://www.lrz.de/services/security/antivirus/institute/
- Die Nutzung durch Mitarbeiter und Studenten zu privaten, Studien- und Forschungszwecken ist ausdrücklich gestattet (sowohl auf heimischen als auch auf mobilen Rechnern)
  ➟ http://www.lrz.de/services/security/antivirus/werdarf/
- Sophos Anti-Virus gibt es für alle wichtigen Plattformen (u.a. für Windows, Macintosh, Netware, Linux, andere Unix-Varianten)

Klassische Verfahren für die Weitergabe

Verfahren :

- Verkauf von CDs (über das LRZ-Benutzersekretariat)
- Bereitstellung auf einem (vom MWN aus zugänglichen) FTP-Server

Gravierende Nachteile dieser Verfahren :

- *Regelmäßige* Aktualisierung (d.h. Einspielen neuer Virensignaturen) ist ziemlich aufwändig
- *Monatliche* Aktualisierung (z.B. bei Erscheinen der neuen CD) bietet keinen ausreichenden Virenschutz

„Virenschutz macht nur richtig Sinn, wenn er aktuell ist; dies können obige Verfahren nicht leisten, deshalb automatisierte Verfahren zur Verteilung und zur Aktualisierung“

Automatisierte Aktualisierung auf einen Klick

Erstinstallation und Aktualisierung nach dem Client/Server-Prinzip :

- „Remote-Update-Client“ (auf jedem PC)
- Zentraler Server mit „EM-Library“ (am LRZ, und ggf. an weiteren Einrichtungen)

Installation und Nutzung des Remote-Update-Client :

- Download des Clients (knapp 5 MByte groß, ist auch auf der neuesten Internet-CD des LRZ enthalten)
- Installation und Konfiguration (im wesentlichen Angabe des EM-Servers, von dem die Anti-Viren-Software geladen werden soll)
- (Erst)Installation der Sophos-Anti-Viren-Software durch den Remote Update Client („Jetzt aktualisieren“)
- Laufende Aktualisierung entweder durch den eingebauten Scheduler oder manuell.
- Auf Rechnern ohne lokalen Benutzerbetrieb (Servern) Aktualisierung über Skript und z.B. cron/at-Job

Unterstützte Plattformen

Einen „Remote-Update“ fähigen Client von Sophos gibt es zurzeit für :

- Windows
- Macintosh OSX 10.2+

Das LRZ bietet zusätzlich Remote-Update-Scripten für :

- Netware
- Linux (kann eventuell auch unter anderen Unix-Varianten laufen)

Für Plattformen, für die es keinen Remote-Update-Client gibt, müssen weiterhin die alten Verfahren (CD, FTP) genutzt werden :

- Downloads ➟ `http://sophos.lrz-muenchen.de/download/`
- ➟ `http://www.lrz.de/services/swbezug/lizenzen/sophos/`

Betrieb einer eigenen EM-Library (Enterprise Manager)

Der Betrieb einer eigenen EM-Library kann sinnvoll sein, wenn das betreffende Subnetz

- durch eine Firewall, die keine http-Anfragen zulässt, vom MWN getrennt ist
- nur eine sehr schmale Bandbreite zum MWN hat (z.B. Funkstrecke oder Modem)

Die EM-Library finden Sie im Download-Bereich

Viren und Würmer : Abwehr (1)

Sicherheits-Lücken im Betriebssystem **und in** allen installierten Software-Komponenten **durch** Patches **beseitigen !!!**

- Alle **Patches** **"einfahren"** und **zwar** **so schnell wie möglich**
- **Probleme :**
  - Aufwand durch die Vielzahl von Patches
  - Patches manchmal fehlerhaft
  - Manchmal Konflikte mit wichtigen Software-Paketen
  - Patches in seltenen Fällen zu spät verfügbar (wird aber zunehmend schlimmer)

  Dennoch : Patches sind unverzichtbar !
- **Irrglaube :**
  " Bei meinem *neuen* Rechner bin ich für einige Zeit sicher, da der Händler doch sicher alle aktuellen Patches aufgespielt hat. "

Viren und Würmer : Abwehr (2)

Viren-Scanner :

- **Immer** **aktuelle Software**
- **Immer** **aktuelle Signaturen** **zur Erkennung der "Schädlinge" !**
  - Faustregel für die Aktualisierung :
    - Mindestens 1-mal pro Tag !
    - Nach jedem Boot
    - Vor oder spätestens kurz nach dem Anschluss an das Internet (evtl. Sogar an ein lokales Netz)
    - Am besten durch einen Automatismus !
  - Problem : Die Hersteller von Viren-Scannern benötigen i.a. Stunden und manchmal sogar Tage, bis sie nach dem Auftreten eines neuen Virus entsprechende Signaturen (allgemein) zur Verfügung stellen !
    Vorher sind Sie aber ungeschützt !!!

Viren und Würmer : Abwehr (3)

Viren-Scanner : […]

- **Konfiguration des Arbeits-Modus :**
  - " **On-Access** ", d.h. Überprüfung automatisch bei jedem Datei-Zugriff !
    " **On-Demand** " (d.h. Überprüfung der vorhandenen Dateien von Fall zu Fall) reicht nicht aus !
  - **Alle** Datei-Typen müssen überprüft werden !
- **Viren-Scanner erkennen auch oft Trojaner, Adware, Spyware und andere unerwünschte Software.**
- **Probleme :**
  - Kein Scanner erkennt alle Viren und Würmer !
  - Probleme bei Schädlingen in Archiven (zip etc.)
  - Große Probleme bei verschlüsselten Archiven

Viren und Würmer : Abwehr (4)

- **Extrem** vorsichtiger **Umgang mit dem Internet !!!**
  - Dateien nur von seriösen Quellen herunterladen !
  - Sichere / defensive Konfiguration von Web-Browsern, E-Mail-Clients, Chat-Programmen etc. !
    Voreinstellungen leider oft zu großzügig / zu unsicher !!!
  - ***NIEMALS*** Anhänge (Attachments) öffnen, außer
    - sie wurden vorher explizit angekündigt.
    - ein Begleit-Text macht plausibel, dass die E-Mail auch wirklich vom angeblichen Absender geschickt wurde.

    Und selbst dann kann ein Anhang infiziert sein !
- **Evtl. sogar Installation bzw. Aktivierung einer Personal-Firewall**

E-Mail-Protokoll

- **Das E-Mail-Protokoll (Verfahren) wurde der gewohnten Briefpost nachempfunden :**
  - Keine Abprüfung der Absender- und Empfangsadresse
  - Missbrauch im Internet durch geringe Kosten beim Versand und leichte Vervielfältigung

  → Z.B. E-Mail mit gefälschter Absenderadresse und rassistischem Inhalt
- **Kontrolle im MWN (zum Teil seit 1997)**
  - ➟ `http://www.lrz.de/services/netzdienste/email/policy/`
  - Kontrolle der Empfänger-Domains (ist Domain im MWN?)
  - Kontrolle der absendenden Rechner (Mail-Server)
  - Kontrolle der Syntax der Adressen
- **Sichere E-Mail-Protokolle weltweit in Vorbereitung (oder Diskussion)**
  - Auch am LRZ

Spam- und Viren-Filterung an den LRZ-Mailrelays

Wer profitiert von den Filtermaßnahmen ?

Alle Personen, deren E-Mails explizit oder implizit bei Empfang oder Versand über die Mailrelays des LRZ geleitet werden, also alle,

- **die ihre Mailbox auf LRZ-Systemen haben**
- **die mailout.lrz-muenchen.de zum Versand benutzen**
- **die ein lokales Mailsystem nutzen, dessen E-Mails beim Empfang aus dem Internet per MX-Record über die Mailrelays geleitet werden**
- **die ein lokales Mailsystem nutzen, das zum Versenden von E-Mails die Mailrelays als Forwarder eingetragen hat**

Viren-Filterung an den LRZ-Mailrelays

- **Die derzeitige Viren-Filterung ist eine provisorische Lösung**
  (weil sich die Integration der Antiviren-Software von Sophos in die Mailrelay-Software von Syntegra immer weiter verzögert hat)
- **Einer Viren-Prüfung werden unterzogen:**
  - E-Mails mit (unter Windows) ausführbaren Attachments (exe, bat, ...)
  - E-Mails mit zip-Attachments
- **Für die Viren-Prüfung wird die Scan-Engine von Sophos eingesetzt**
- **E-Mails, bei denen ein Virus/Wurm festgestellt wird,**
  - werden zur Sicherheit noch eine Woche aufbewahrt
  - und dann weggeworfen
- **Bei ausgefilterten E-Mails erfolgt weder eine Benachrichtigung des Absenders noch des Empfängers**

Warum keine Benachrichtigung ?

- **Es handelt sich „so gut wie sicher“ um Würmer (nicht um Viren), da nur E-Mails mit bestimmten Attachment-Typen untersucht werden (z.B. keine doc- oder xls-Attachments)**
- **Würmer enthalten (im Unterschied zu Viren) keinerlei Nutzinformationen**
- **Benachrichtigung des Empfängers?**
  - Im besten Fall lästig („Spam“); für unbedarftere Benutzer möglicherweise auch irritierend oder beunruhigend
- **Benachrichtigung des Absenders?**
  - Würde den Falschen erreichen, da bei Wurm-Mails die Absendeadressen gefälscht sind

Ausführliche Informationen dazu finden sich in der Mail-Policy
➟ **http://www.lrz.de/services/netzdienste/email/policy/policy-10.html**

Ein paar Zahlen zur Viren-Filterung

- **Anzahl ausgefilterter Wurm-Mails :**
  - E-Mails pro Tag Mitte Juni 2004 :
    - montags bis freitags ca. 45.000
    - samstags/sonntags ca. 30.000
  - Zurzeit gesunken auf ca. 25.000 bzw. ca. 15.000 pro Tag
  - Bis zu 5% des gesamten Mail-Aufkommens

- **Top 5 der aktuell am häufigsten vorkommenden E-Mail-Würmer**
  (Stand 27.7.2004, ca. 38.000 Mails ausgefiltert)

MyDoom-O	30,5%
W32/Netsky-P	30,0 %
W32/Netsky-D	10,1 %
W32/Lovgate-V	7,8 %
W32/Netsky-Q	4,2 %

Spam-Filterung an den LRZ-Mailrelays

- **Produktionsbetrieb seit Anfang Oktober 2004**
- **Auf der Basis von SpamAssassin**
- **Kein Löschen von vermeintlichen Spam-Mails, sondern Aufnahme zusätzlicher Header-Zeilen mit Spam-Bewertung**
- **Ausfilterung (Löschung oder Ablage in Spam-Folder) durch das jeweilige Mailprogramm des Benutzers**

➟ **http://www.lrz.de/services/netzdienste/email/spam-filter/**

Eingefügte Header-Zeilen (Beispiel)

X-Spam-Status: Yes, hits=9.7 tagged_above=-999.0 required=5.0
tests=BAYES_80, HTML_30_40, HTML_FONT_COLOR_NAME,
HTML_MESSAGE, HTML_TABLE_THICK_BORDER,
HTML_WITH_BGCOLOR, HTTP_USERNAME_USED,
MAILTO_TO_REMOVE, MIME_HTML_ONLY

X-Spam-Level: *******

X-Spam-Flag: YES

Hintergrundinformationen zur Konfiguration des SpamAssassin

- **Startkonfiguration :**
  - Default Scores
  - Klassifizierung als Spam ab 5.0 Hits
  - Zentrale Bayes-Datenbank mit Autolearn
    (Ham < 0.1 Hits, Spam > 12.0 Hits)
  - Zentrales AWL (Auto-White-Listing)
  - Einbindung der RBL+ von MAPS

- **Geplant :**
  - DCC-Server (Distributed Checksum Clearinghous)
  - Einbindung weiterer RBLs, sobald diese als Zonen lokal vorliegen (übers Netz zu lange Zugriffszeiten)

Beispiele für Filter-Möglichkeiten

- **Am einfachsten :**
  Auf „`X-Spam-Flag: YES`“ prüfen und gegebenenfalls in Spam-Folder verschieben
- **Zweistufig :**
  - E-Mail sofort löschen,
    falls „`X-Spam-Level`“ mehr als (z.B.) 12 Sterne enthält
  - E-Mail in Spam-Folder verschieben,
    falls „`X-Spam-Flag`“ mit „`YES`“ belegt ist
- **Beliebig konfigurierbar (im Rahmen der Möglichkeiten des verwendeten Mail-Programms) ...**

Andere / zusätzliche Möglichkeit : Lokale Filterung mit Netscape oder Mozilla

- **Nutzung der in Netscape (ab Vs. 7.1) bzw. Mozilla (ab Vs. 1.3) integrierten Spam-Filter**
  - ➟ **`http://www.lrz.de/fragen/faq/mail5/`**
  - ➟ **`http://www.rz.uni-augsburg.de/connect/2003-01/spam/`**
- **Gute Spam-Erkennung**
  (liegt nach entsprechendem Training bei ca. 90 bis 95%)
- **Nachteile:**
  - **Jede Installation muss separat trainiert werden**
  - **Bei IMAP werden nicht nur die Header, sondern die kompletten Mails geladen**

Security-Einführungskurs für Anwender (1)

Motivation und Zielsetzung :

- **Einstieg in die System- und Netz-Sicherheit**
- **Voraussetzungen:**
  Anwender-Grundkenntnisse in der Rechnerbenutzung sowie Internet-Grundkenntnisse
- **Zielsetzung:**
  Hilfestellung, *sich selbst* so gut wie irgend möglich zu schützen
  ⇨ 80%-Lösung

Security-Einführungskurs für Anwender (2)

- **Kurs-Aufbau (3 Teile, der letzte nur auf Wunsch)**
  - Grundlagen und allgemeine Maßnahmen (Plattform-unabhängig), z.B.:
    - Wichtige Begriffe und grundlegende Prinzipien
    - Sicherer Umgang mit Kennungen und Passwörtern
    - Internet-Sicherheit, insbesondere WWW und E-Mail
  - Wichtige Tools am Beispiel von UNIX:
    Secure Shell (SSH), Pretty Good Privacy (PGP)
  - Kryptographische Grundlagen
- **2 mal pro Jahr, zusätzlich nach Bedarf vor Ort (mindestens 10-15 Interessenten)**
- **Folien-Handouts (`*.pdf`) über WWW zugänglich**

Security-Kurs für UNIX-Systemverwalter (1)

Motivation und Status :

- Security-Management wird immer wichtiger
- Security-Mechanismen sinnvoll (konfiguriert) einzusetzen, ist für (nebenamtliche / ehrenamtliche) Administratoren oft schwierig
- ***Ausschließlich*** **für** ***UNIX-Systemverwalter(innen)***
- Erste Staffel im Frühjahr 2004
- Folien-Handouts und Begleitschrift über WWW zugänglich

Security-Kurs für UNIX-Systemverwalter (2)

Kurze Inhalts-Übersicht :

- Organisatorische Maßnahmen
- Passwort-Schutz
- Datei-Zugriffsrechte, Integritäts-Checker
- Netz-Dienste, TCP-Wrapper, OpenSSH
- Tools zur System-Überwachung, Security-Scanner
- Firewalls
- Vorgehen nach einem (vermuteten) Angriff

Security-Portal des LRZ : Ausgewählte Themen

System-Security :

- "Bauernregeln"
- Passwort-Sicherheit
- MS-Windows : Überblick
- Schutz gegen Viren
- Vorgehen nach einem (vermuteten) Angriff

Netz- und Internet-Security :

- E-Mail-Sicherheit, WWW-Sicherheit
- Secure Shell (SSH)