Leibniz-Rechenzentrum, Garching b. München

Security-Bausteine für das Münchner Wissenschaftsnetz (MWN)

Dr. Victor Apostolescu,
Dr. Ernst Bötsch, Dr. Helmut Reiser

(März 2007)

www.lrz.de/services/security/

Das Leibniz-Rechenzentrum (LRZ)

Wissenschaftliches Rechenzentrum
für die Hochschulen in München
und die Bayerische Akademie der Wissenschaften

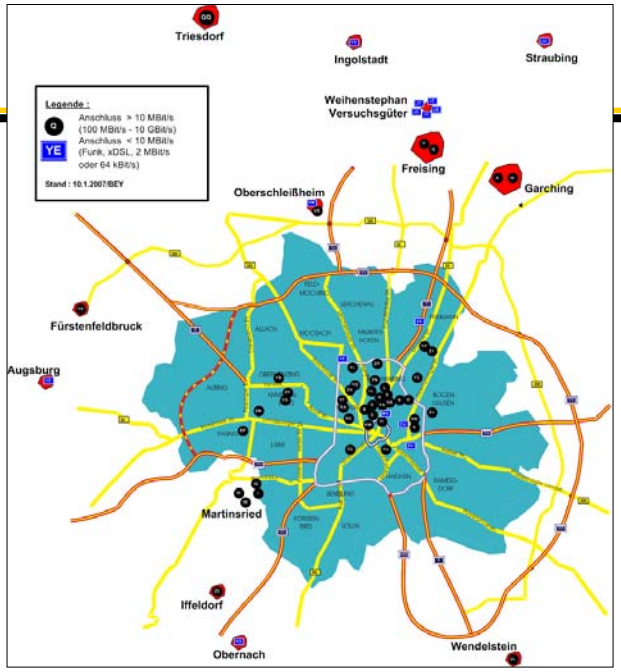
Aufgaben:

- Planung, Ausbau und Betrieb
  des Münchner Wissenschaftsnetzes (MWN),
  Kompetenzzentrum für Datenkommunikationsnetze
- Betrieb von zentralen Diensten
- Betrieb von Hoch- und Höchstleistungsrechnern

Das Münchner Wissenschaftsnetz (MWN)

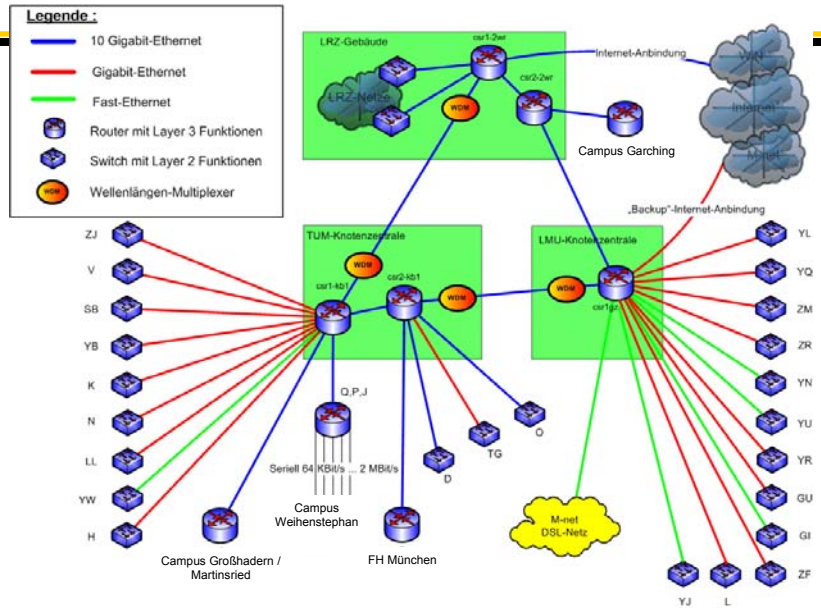
- Planung, Aufbau und Betrieb durch das LRZ
- Beratung und Schulung in Kommunikationsfragen
- Anbindung an nationale und internationale Forschungsnetze
- Zugang über
  - Fest angeschlossene Endsysteme
  - Internet
  - VPN-Server: Internet + mobile Rechner (lokal)
  - M-net
  - Modem- / ISDN-Einwahl

MWN: Ausdehnung

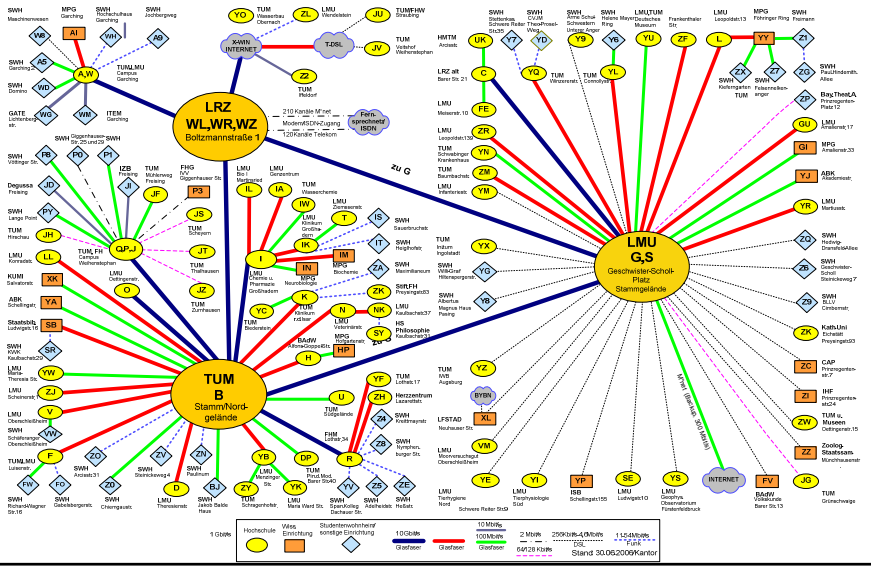


4

MWN: Backbone-Struktur

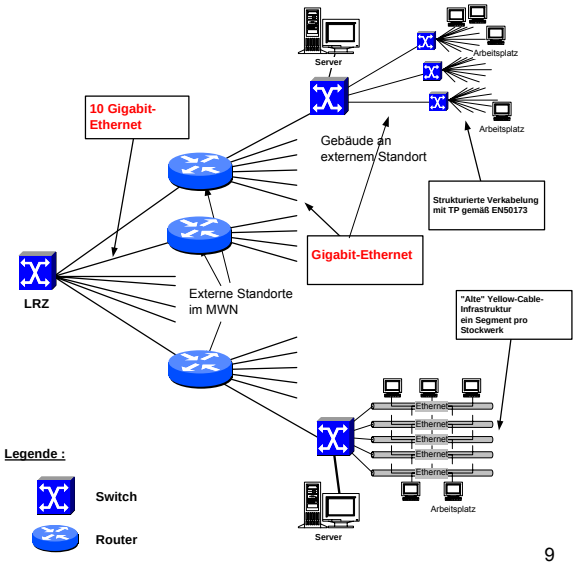


MWN: Logische Struktur der Areale



MWN: Verkabelung

10	GE	Internet (X-WiN)
300	Mbit/s	Internet-Fallback
10	GE	Backbone
10	GE	Große Standorte
1	GE	Mittlere Standorte
100	Mbit/s	Kleinere Standorte
DSL / ISDN		Kleine Standorte
> 40		Glasfaserleitungen
1	GE	Gebäude
1	GE	Switches
10	GE	Große Server
1	GE	Server
100	Mbit/s	Clients



9

MWN: In München ist alles etwas „größer“

>	5	Hochschulen
ca.	30	Institutionen
>	700	Institute
ca.	100.000	Nutzer (potentiell)
>	40	Studentenwohnheime
>	10.000	Wohnheimplätze
>	60	Areale
>	220	Gebäudekomplexe
>	440	Gebäude
>	21.000	Räume

	10	Router
>	260	Router-Interfaces
>	780	Switches
>	47.000	Switch-Ports
>	680	WLAN-Access-Points
>	55.000	Rechner; ca. 5% Server

Trotzdem nur **beschränkte** Personalkapazität vorhanden !

MWN: Aufgabenverteilung

❒ Planung:	Netzabteilung des LRZ zusammen mit Bauämtern, Instituten usw.
❒ Bereitstellung von Räumen:	Betroffene Organisationen
❒ Verkabelung:	Fremdfirmen
❒ Installation und Wartung der Netzkomponenten:	Netzwerkstatt des LRZ
❒ Betrieb:	Netzabteilung des LRZ
❒ Betreuung von Arealen:	Netzabteilung des LRZ → “Arealbetreuer”
❒ Lokale Ansprechpartner für die Unterbezirke:	Mitarbeiter der Organisationen → “Netzverantwortliche”

MWN: Mengen-Problemematik an vielen Stellen

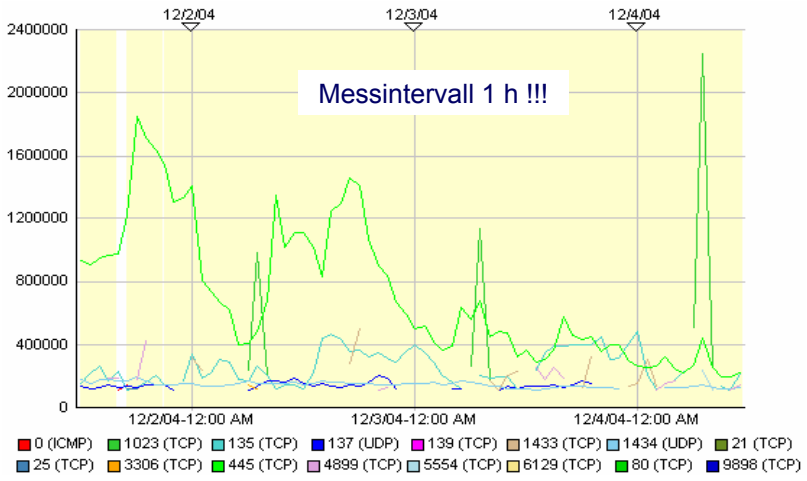
- ❒ Bandbreiten
- ❒ Datenvolumen
- ❒ Zahl der Netzkomponenten und Endgeräte
- ❒ Geographische Ausdehnung
- ❒ Zahl der Kunden (Nutzer)
- ❒ Zahl der beteiligten Organisationen
- ❒ Zahl der Netzverantwortlichen (> 770)

⇨ Qualitativ neuartige Probleme
⇨ Automatisierung, Automatisierung, Automatisierung, ...

Übersicht

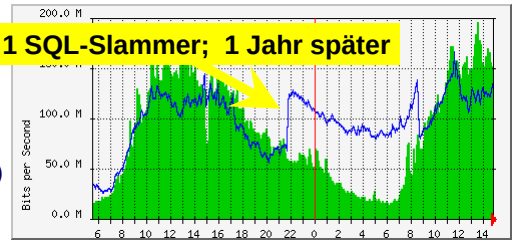
- Das Leibniz-Rechenzentrum (LRZ)
  Das Münchner Wissenschaftsnetz (MWN)
- Wandel der Bedrohungen
- Security-Dienste des LRZ (Überblick)
- Bearbeitung von Abuse-Fällen, Abuse-Monitoring
- Der NAT-o-Mat
- Todo

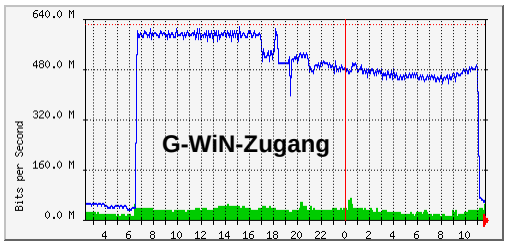
Portscans eingehend

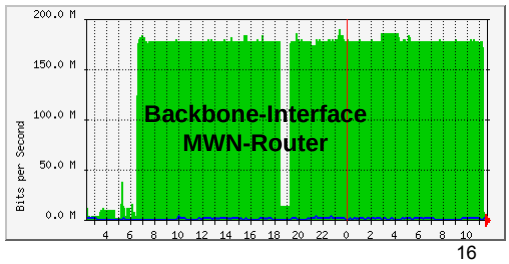


SQL-Slammer: Kleiner Wurm mit großer Wirkung

- Vorfall vom 25.1.03
- Betroffen
  - MS-SQL-Server
  - Rechner mit integriertem, abgespecktem MS-SQL-Server (!!)
- Security-Patch verfügbar seit 6 (!) Monaten







16

Generationenwechsel bei den Angreifern

1) Prä-Kommunikationsnetz, Akustik-Koppler: 2600

2) Über Standleitungen vernetzte Uni-Rechner: Hacker ↔ Cracker
   Robert T. Morris, Jr. (1988)

3) Allgemein zugängliches Internet: Script-Kiddies

4) Kommerzialisiertes Internet: Kriminalisierung

Generationenwechsel im Jahr 2005: Kriminalisierung der Szene

- Große Spannbreite: Spam, Phishing, Betrug, Sabotage (z.B. mit DDoS), Erpressung (mit DDoS), (Industrie-)Spionage, …
- Infektion durch E-Mail / Web
- Botnets
- Abnahme von aggressiven und großflächigen Ausbrüchen
- Vielzahl von Angriffen mit kleinen Zielgruppen
  → Ca. 16.000 neue Schädlinge; ca. ⅔ Windows-Trojaner

2006: Fortschreitende Professionalisierung der Angreifer (1)

Anheuern von vielen und teilweise hoch qualifizierten Experten

- Automatisierte Suche nach Lücken (Fuzzer)
  → Zero-Day-Attacks
- Hoch spezialisierte, trickreiche Malware:
  Trojaner, Würmer, Spyware, Adware, …
- Angriff auf Anwendungen:
  Browser, Web-Server-Anwendungen, Word, Excel, …
- Infektion durch Web / E-Mail / Chat

2006: Fortschreitende Professionalisierung der Angreifer (2)

- Neue Methoden:
  - Tarnung durch Inaktivität und Rootkit-Funktionen
  - Cross-Site-Scripting (XSS) usw. → Anfang der URL stimmt !
  - Pharming → Bookmarks sind wertlos !
- Riesige Zahl von Schädlingen:
  - Mehrere 10.000 Varianten von Sdbot oder Spybot; pro Tag kommen 50 – 100 neue hinzu.
  - Täglich 1000 – 2000 neue Schädlinge
  - ⇨ Viren-Scanner erkennen nur ca. die Hälfte !

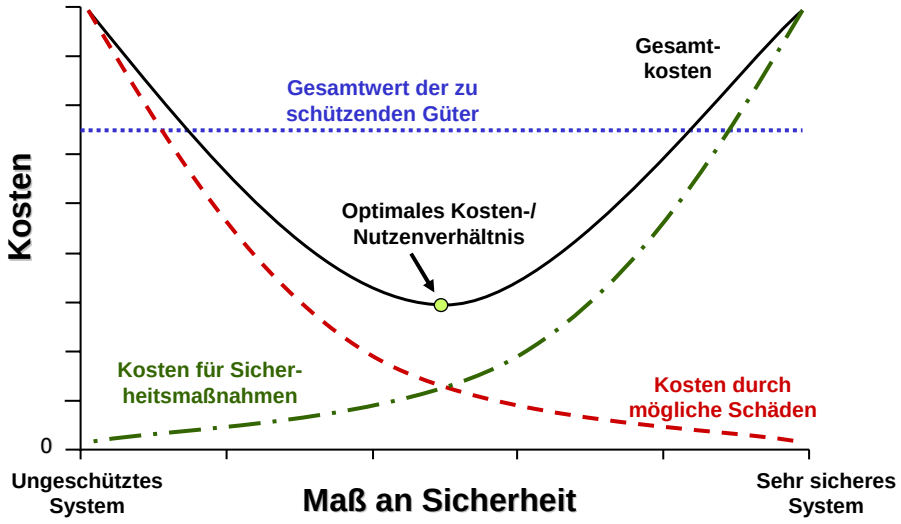
2006: Fortschreitende Professionalisierung der Angreifer (3)

- Optimiertes Social-Engeneering:
  - Begleit-Texte immer besser
  - Layout täuschend ähnlich
  - Einbeziehung des Opfer-Kontexts (Spear-Phishing)
- Botnets boomen: Vint Cerf:
  Ein Viertel der Internet-PCs ist Mitglied eines Botnet.
  → 100 – 150 von 600 Millionen !

Security-Leitlinie des LRZ

- 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
- ⇨ Verärgerte Nutzer sind seeehhhr erfinderisch ! …

Security: Ja – aber mit Maß und Ziel !



28

Security-Dienste des LRZ: Überblick (1)

- Betrieb zentraler Dienste:
  - E-Mail, Web, DNS, Backup / Archivierung, Directory (LDAP), File-Service, DHCP, RADIUS, FTP, VoIP, Video-Server, Video-Conferencing, Vorlesungsübertragung innerhalb des MWN, IP-Adressverwaltung, Lizenz-Server, ...
  - Produktionsbetrieb in größerem (bzw. großem) Rahmen
    - Synergieeffekte
    - Person-Power (→ Vertretungsproblematik)
    - Know-How
    - (Teure) kommerzielle Software
    - Nachhaltiger Betrieb, Kontinuität
    - ⇨ Nebeneffekt:
      (Zumindest teilweise) Vermeidung von Security-Problemen

Security-Dienste des LRZ: Überblick (2)

- Private IP-Adressen
- VLANs:
  - > 630 lokale (d.h. bis zum nächsten Router) für Nutzer
  - > 230 für das Management von Netzkomponenten
  - 7 MWN-weite für globale Nutzergruppen
- VPN
- Antiviren-Software (Sophos):
  - Campus-Lizenz für Bayern. Explizit auch für die private Nuztung !
  - Betrieb eines Update-Servers
- Betrieb des Windows-Server-Update-Service (WSUS)
- Bearbeitung von Abuse-Fällen, Abuse-Monitoring

Security-Dienste des LRZ: Überblick (3)

- Firewalls
  - Firewalls für die eigenen LRZ-Rechner
  - Übergang zum Internet (X-WiN):
    - IP-Spoofing-Filter
    - SMTP-Empfang nur für ausgewählte Server
    - Sperren: Microsoft-Protokolle (Netbios), SNMP, einige P2P-Protokolle, einige weitere TCP-/UDP-Ports
    - Bandbreitenbeschränkungen der restlichen P2P-Protokolle
  - Router:
    - Generelle Filter: IP-Spoofing, Broadcast, ...
    - Standard-Firewall-Pakete auf Wunsch (dynamische, reflexive Filter)
  - Mandantenfähige Firewalls für die Kunden durch Spezial-Blades in den Routern (ab 2007)

Security-Dienste des LRZ: Überblick (4)

- E-Mail:
  - Nur professionell betriebene Mail-Server vom Internet aus erreichbar
  - Jeder MWN-Rechner darf E-Mails direkt ins Internet schicken.
  - Zentrale Mail-Relays des LRZ:
    - Relay-Blocking
    - Spam-Abwehr durch Greylisting (☺ extrem erfolgreich ☺)
    - Spam-Tagging (SpamAssassin)
    - Blocken diverser Attachment-Typen
    - Viren-Filterung der Attachments (keine Benachrichtigung !)

Security-Dienste des LRZ: Überblick (5)

- Bereitstellung von Informationen und Beratung:
  - Security-Seiten des LRZ: www.lrz.de/services/security/
  - Diverse Mail-Adressen: <abuse@lrz.de>, <security@lrz.de>
  - Security-Einführungskurs für Anwender
  - Security-Kurs für UNIX-Systemverwalter
  - Diverse Mail-Verteiler: DFN-CERT-Subverteiler, <security-news@lists.lrz.de>
  - Security-Sprechstunde
  - Hotline

Bearbeitung eines **gemeldeten** Abuse-Falls

- 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

Durchsetzung der Nutzungsrichtlinien (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-Monitoring durch das LRZ (1)

Unterschiedlicher Automatisierungsgrad

- Vollautomatisch:
  - Sensor erkennt Ereignis
  - Monitor benachrichtigt Ansprechpartner oder Verursacher (E-Mail oder Web-Seite)
  - Monitor sperrt optional verdächtigen Rechner
- Halbautomatisch:
  - Sensor erkennt Ereignis
  - Monitor bereitet Benachrichtigungs-Mail vor
  - Abuse-Response-Team schickt E-Mail ab
  - AR-Team sperrt optional verdächtigen Rechner

Abuse-Monitoring durch das LRZ (2)

Unterschiedlicher Ort des Sensors

- Am Übergang zum Internet
- Integriert in den NAT-o-Mat

Unterschiedliche Methoden

- Spezialisiertes IDS:
  - FTP-Verkehr auf einem Nicht-Standard-Port (d.h. Port 21)
  - Erkennung von Botnet-Sklaven (charakteristische Signaturen bei IRC-Verbindungen)

Abuse-Monitoring durch das LRZ (3)

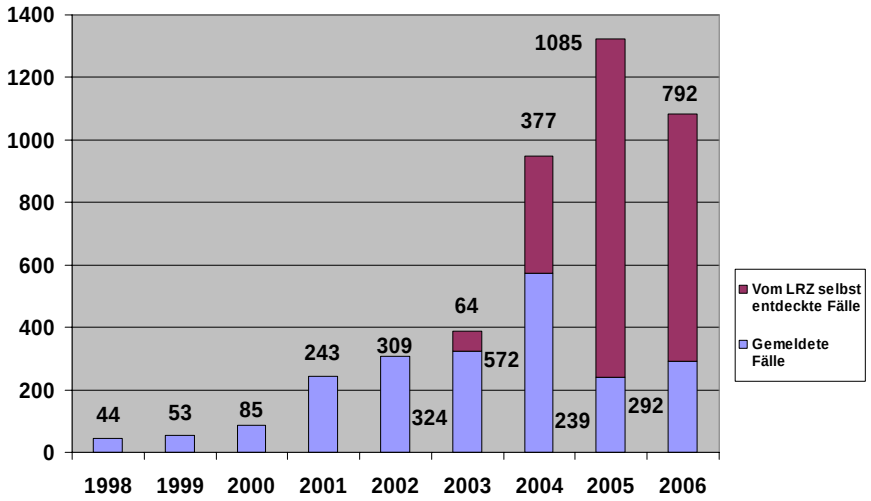
Unterschiedliche Methoden (…)

- Statistische Auswertung von Verkehrsdaten:
  - Zahl von SMTP-Verbindungen (Port 25) → Quelle von Spam- und Phishing-Mails, sich per E-Mail verbreitende Würmer
  - Viele ausgehende Verbindungen → Net- / Application- / Port- / Vulnerability-Scan
  - Viele Verbindungen zu *einem* Ziel → (D)DoS
  - Übertragenes Datenvolumen → Wurm, Verteilzentrale

Abuse-Fälle im MWN: Arten

- Gehackte oder mit Würmern / Trojanern / … infizierte Rechner; sehr oft Botnet-Slaves
- (Un)berechtigte (Spam-)Beschwerden
- Copyright-Verletzungen (externe Hinweise)
- Hinweise und Anfragen von MWN-Benutzern
- Fehlverhalten von MWN-Benutzern (absichtlich oder unabsichtlich)

Abuse-Fälle im MWN
www.lrz.de/services/security/abuse/



Abuse-Fälle im MWN: Von außerhalb gemeldet (1)

Art des Missbrauchsfalls	Anzahl der Fälle	Involvierte Rechner / Benutzer des MWN	Eingegangene Beschwerden, Anfragen usw.
Fälle im Bereich „E-Mail“:			
Unberechtigte Spam-Beschwerden	75	–	75
Spam-Versand über kompromittierte Rechner	28	28	44
Beschwerden an die „falsche Stelle“	8	–	8
Sonstige Mail-Fälle	7	1	7
Teilsumme	118	29	134

Abuse-Fälle im MWN: Von außerhalb gemeldet (2)

Art des Missbrauchsfalls	Anzahl der Fälle	Involvierte Rechner / Benutzer des MWN	Eingegangene Beschwerden, Anfragen usw.
Sonstige kompromittierte Rechner:			
Beschwerden wegen Port-/Vulnerability-Scans	40	113	58
Vom DFN-CERT gemeldete Fälle	21	173	21
Sonstige Beschwerden (u. a. DoS)	18	22	26
Teilsumme	79	308	105

Abuse-Fälle im MWN: Von außerhalb gemeldet (3)

Art des Missbrauchsfalls	Anzahl der Fälle	Involvierte Rechner / Benutzer des MWN	Eingegangene Beschwerden, Anfragen usw.
Fälle mit rechtlichen Aspekten:			
Anfragen von Strafverfolgungsbehörden	10	14	11
Copyright-Verletzungen	9	10	10
Sonstige Fälle	4	3	4
Teilsumme	23	27	25
Organisatorische Fälle	30	40	27
Allgemeine Anfragen	18	–	18
Sonstige Fälle	24	5	24
Summe der gemeldeten Fälle	**292**	**409**	**333**

Abuse-Fälle im MWN: Selbst entdeckt

Art des Monitoring, durch das die verdächtigen Rechner entdeckt wurden	Anzahl der Fälle	Anzahl der Rechner
Entdeckte kompromittierte Rechner:		
NAT-o-MAT (schwere Fälle)	270	270
FTP-Server, der auf einem Nicht-Standard-Port arbeitet	179	179
Viele Mail-Verbindungen zu anderen Rechnern im Internet	154	229
Portscans	124	124
Botnet	24	46
DoS	18	18
Extrem hoher Datenverkehr	10	10
Teilsumme	779	876
False-Positives	13	13
Summe der vom LRZ endeckten Fälle	**792**	**889**

Security-Einführungskurs für Anwender (1)

- Einstieg in die System- und Netz-Sicherheit
- Zielsetzung:
  - Problembewusstsein wecken (Awareness)
  - Hilfestellung, sich selbst so gut wie irgend möglich zu schützen ⇨ 80%-Lösung
  - Vermittlung grundlegenden Know-Hows
- Voraussetzungen: Anwender-Grundkenntnisse in der Rechnerbenutzung sowie Internet-Grundkenntnisse

Security-Einführungskurs für Anwender (2)

- Behandelte Themen (weitgehend plattformunabhängig):
  - Grundlegende Prinzipien, allgemeine Maßnahmen
  - System-Security
    (sicherer Umgang mit Kennungen und Passwörtern)
  - Netz-Security (v.a. E-Mail und WWW)
  - Kryptographische Grundlagen (optional, auf Wunsch)
- 2-mal pro Jahr im LRZ.
  Zusätzlich nach Bedarf vor Ort (ab 20 Interessenten).
- Folien-Handouts über WWW zugänglich (PDF)

„Kurs-Botschaft“: Was tun ?

Menschliche Firewall

- ⇨ Sich der Gefahr bewusst werden
- ⇨ Sich **kontinuierlich** informieren
- ⇨ Vorsicht, Vorsicht, Vorsicht, …

Technik

- ⇨ Patches, Patches, Patches, …
- ⇨ Viren-Scanner mit **aktuellen** Signaturen
- ⇨ Personal Firewall: Nur etwas für Profis

Der NAT-o-Mat

Ein transparentes NAT-Gateway mit

- integriertem, automatischem Abuse-Monitoring
- Traffic-Shaping

Nat-o-Mat: Ausgangssituation (Anfang 2005) (1)

- Vielfaches Angebot an Proxy- und Gateway- Diensten:
  - HTTP / FTP (Web-Proxy)
  - Socks-Proxy
  - VoIP-Proxies für H.323 und SIP
  - VPN-Zugang
- Entwicklungen:
  - Stetig steigender Verkehr
  - Zunehmender Missbrauch von Proxy-Diensten (z.B. HTTP-Tunneling, P2P über SOCKS)
  - Neue Anwendungen ungeeignet für bestehende Proxies

Nat-o-Mat: Ausgangssituation (Anfang 2005) (2)

- Bisherige Strategie:
  - Weiterer Ausbau bestehender Dienste
  - Sperrung von Ports und Subnetzen, neue Skripte
  - Installation weiterer Proxies für neue Anwendungen
  - ⇨ Teilweise hohe Kosten
  - ⇨ Viele Komponenten
  - ⇨ Fehleranfälligkeit
  - ⇨ Erhebliche Person-Power für den Betrieb erforderlich !

Nat-o-Mat: Zielsetzung (1)

- Vereinfachung der Strukturen (Betreibersicht)
  - Geringerer Aufwand beim Betrieb
  - 1 Plattform
  - Größeres Dienstangebot
  - Einfache Festlegung von Policies
  - Gut skalierbar für zukünftigen Ausbau

Nat-o-Mat: Zielsetzung (2)

- Kontrolle über die Netznutzung (Betreibersicht)
  - bei Netzwerksicherheit
  - bei Volumina und Bandbreiten
- Vereinfachung für den Benutzer:
  - Keine speziellen Vorkenntnisse
  - Keine speziellen Client-Programme oder Konfigurationen
  - ⇨ Geringerer Dokumentationsaufwand: Keiner ! ☺
  - ⇨ Weniger Fragen bei der Hotline

Nat-o-Mat: Randbedingungen

- I.a. keine administrative Kontrolle des LRZ über die angeschlossenen Endsysteme
- Mobile Systeme werden im und außerhalb des MWN betrieben
  → Studenten, reisende Wissenschaftler, …
- Primäres Ziel: Akzeptables Kommunikationsverhalten
- Kompromittierte Systeme werden in Kauf genommen, wenn sie nicht besonders auffallen.

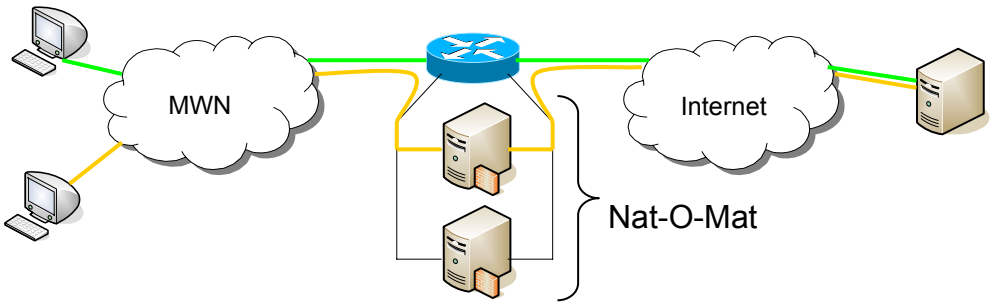
Nat-o-Mat: Idee

- Erkennung von Auffälligkeiten durch
  - Analyse des Kommunikationsverhaltens (z.B. Paketraten)
  - Zahl der Kommunikationspartner
- Minimierung der „teuren“ Aktionen
  - Deep-Packet-Inspection, d.h. vollständige Protokollanalyse
  - Nur für Packete die nicht eindeutig als „gut“ bzw. „böse“ klassifizierbar
- Begrenzung der False-Positive-Rate
  - durch sanfte Sperrungen (sog. Soft-Limits)
  - Begrenzung der erlaubten Paketrate / Bandbreite
  - Vollständige Sperrung nur im Fall einer Eskalation

Nat-o-Mat: Komponenten

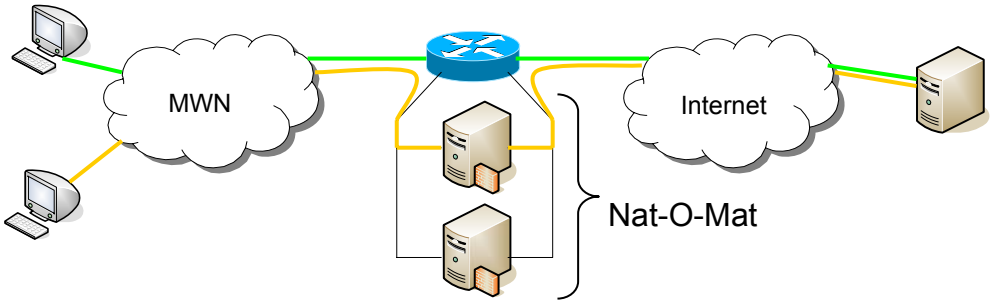
- Router → Linux
- Stateful-Firewall → iptables
- NAT-Gateway → iptables
- Intrusion-Detection- & Prevention-System (IDS/IPS) → bro
- P2P-Traffic-Shaper → iptables + tc
- Status- & Incident-Reporting → Web-basiert
- Benutzerinformation → Web-basiert
- Lösung für Hochverfügbarkeit und Skalierbarkeit → Linux-HA

Nat-o-Mat: Einbindung (1)



- Nat-O-Mat ist selbständiger Router
- Umleitung ausgewählter Pakete per Policy-based-Routing zum Nat-O-Mat

Nat-o-Mat: Einbindung (2)



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

Nat-o-Mat: Verkehrsanalyse

- Verhalten von Hosts im Netzwerk klassifizierbar durch
  - Rate erfolgloser Verbindungsaufbauversuche
  - Anzahl aktiver Kommunikationspartner
  - Paketrate und Bandbreite
  - Typische Ports
  - Typische Signaturen
- Problemstellung:
  - Welche Kombination obiger Parameter liefert griffige Anhaltspunkte ?
  - Wo liegen die Grenzwerte ?
- Festlegung der Grenzen anhand empirischer Daten

Nat-o-Mat: 3 Arten von Policies

1. Anzahl der Kommunikationsverhältnisse
   - z.B. Anzahl von IP- / UDP- / TCP-Flows
   - Unterscheidung bestätigt / unbestätigt
2. Paketraten und Bandbreiten
   - z.B. pro Quell-IP-Adresse oder pro Verbindung
   - Traffic-Shaping für P2P Protokolle
3. Signaturen
   - Art und Verwendung von diversen Protokollen (z.B. P2P)
   - Erkennung von Würmern, Botnets

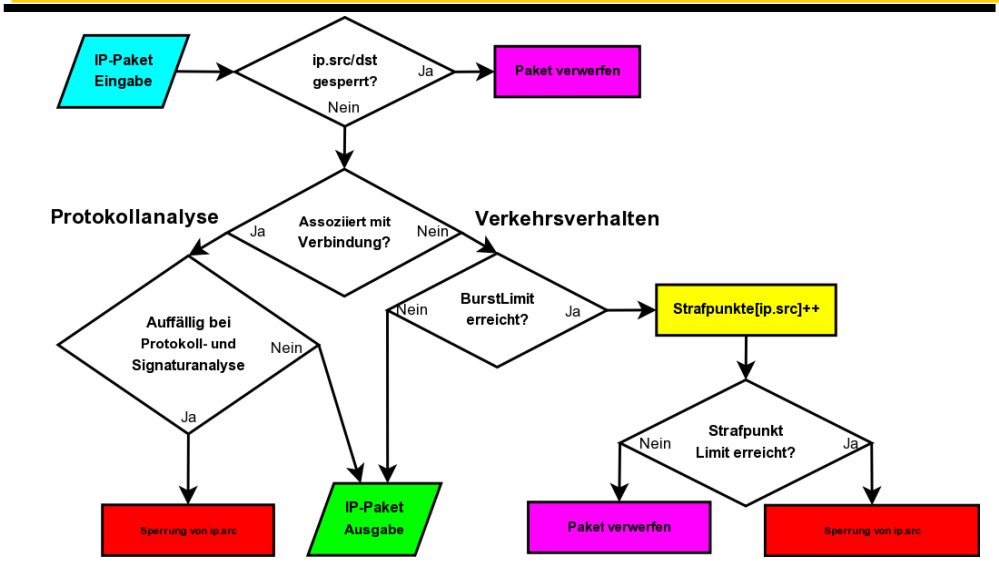
Nat-o-Mat:
Analyse des Verkehrsverhaltens (Beispiele)

- IP-Pakete, keinem bestehenden Flow zuzuordnen:
  - Pakete mit hoher Rate von einem Host an viele Hosts
    → Denial of Service (DoS) / Net-Scan
  - Pakete von vielen Quellen zu einem Ziel-Host
    → Distributed Denial of Service (DDoS) / Port-Scan
- IP-Pakete, aus bestehendem Flow:
  Protokoll- und Signaturanalyse von
  - Typischen Signaturen von Würmern und Viren
  - Shell-Code
  - Botnet-Kommunikation
  - P2P-Protokollen

Nat-o-Mat:
Policy-Enforcement – Grundlagen

- Strafpunkte pro MWN-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
- Traffic-Shaping für P2P-Protokolle

Nat-o-Mat: Policy-Enforcement – Ablaufdiagramm



Nat-o-Mat: Policy-Enforcement – 4-stufiges Eskalationsprinzip (1)

Beispiel: Application-Scan, d.h. 1 Absender-IP auf 1 Ziel-Port bei mehreren Ziel-Systemen

① Bei kurzzeitigen Überschreitungen:

- Keine Einschränkung unterhalb der "Burst-Bedingung"
- ≤ 30 Versuche/s

② Bei Überschreitung der "Burst-Bedingung":

- Beim 31. Versuch
- Soft-Limit: Blockierung der verursachenden IP-Pakete
- Inkrement der Strafpunkte

⇨ 1 Punkt je 10 Versuche

Nat-o-Mat: Policy-Enforcement – 4-stufiges Eskalationsprinzip (2)

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:

- ≥ 1.000 Punkte
- Mail-Benachrichtigungen:
  - Netzverantwortliche
  - Evtl. Zusatzinformationen (d.h. vollständiger IDS-Report) an das AR-Team

Nat-o-Mat: Automatischer 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

Nat-o-Mat: Policy-Enforcement – Traffic-Shaper

- Bandbreiten- und Paketratenbegrenzung für P2P-Protokolle (z.B. Filesharing via Kazaa oder Bittorrent)
- Verschiedene Bandbreitenklassen möglich:
  - Pro Protokoll / pro Verbindung / pro Adresse / pro Subnetz
- Zur Zeit realisiert:
  Gemeinsame Bandbreitenklassen für alle Nutzer:
  - 2 Mbit/s für BitTorrent
  - 1 Mbit/s für alle anderen P2P-Protokolle

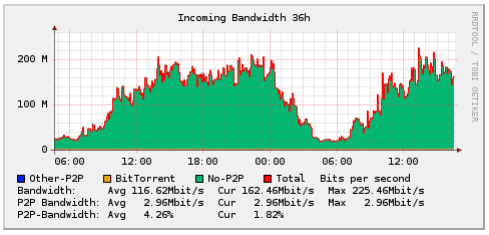
Nat-o-Mat: Loadbalancing & High-Availability

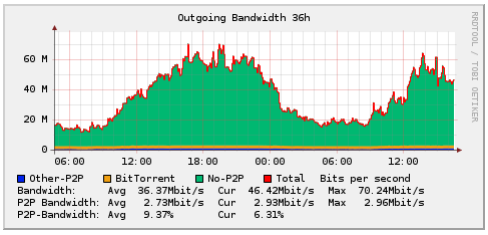
- Betrieb als Cluster aus gleichberechtigten Nodes
- Zuordnung von Subnetzen zu einem Node
- Jeder Node kann Funktion eines anderen übernehmen
- Selbsttests und gegenseitige Prüfungen zur Sicherstellung der Funktionalität

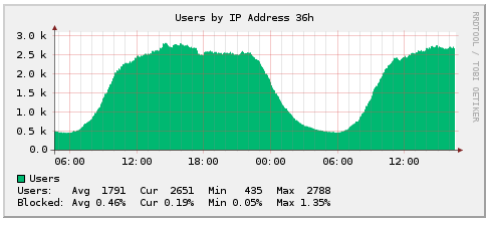
Nat-o-Mat: Management-Interface

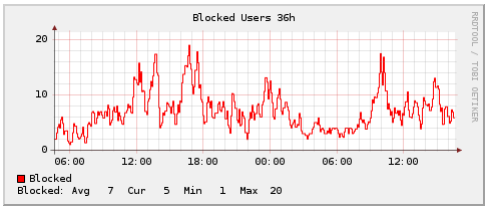
- Analyse des laufenden Verkehrs:
  - Top-Listen aller auffälligen Rechner
  - Suchfunktionen
- Reporting:
  - Verteilung von Bandbreiten
  - Anzahl aktiver Verbindungen
  - Anzahl IP-Adressen
- Detaillierte Benutzerinformation bei Verstoß

Nat-o-Mat: Management-Interface – Bandbreiten









Nat-o-Mat: Praxiseinsatz (1)

- Betroffene Subnetze:
  - Private IP-Adressen
  - Subnetze des VPN-Servers
  - Subnetze der Einwahl-Server (Modem, ISDN, M-net)
- Keine Auffälligkeiten am Internet-Übergang
- Leicht gestiegenes Volumen:
  - Durch Abschaltung der Web-Proxies
  - Neuhinzugekommene Anwendungen
- Sehr hohe Akzeptanz durch die Nutzer

Nat-o-Mat: Praxiseinsatz (2)

- Kennzahlen (23.10.2006):
  - Anzahl der Hosts: ~ 2.500
  - Anzahl Sessions: ~ 100.000
  - Durchsatz: ~ 220 Mbit/s (in)
~ 100 Mbit/s (out)
  - P2P-Anteil: 1 % bis 3 % (in)
2 % bis 5 % (out)
  - Durch Hard-Limits gesperrte Hosts: 0,1 bis 1,1 %
  - CPU-Last, Speicherverbrauch: ~ 15 %

Todo: Security – ein weiter, endloser Weg ... (1)

- (Re-)Zentralisierung von Server-Diensten (z.B. IntegraTUM)
- Generelle Authentifizierungspflicht am „Netzrand“ (802.1x)
  - Funktionalität in den Endsystemen gegeben (90-95%)
  - Funktionalität in den Netzkomponenten (Rest)
- Ausweitung des Abuse-Monitoring:
  - An allen Backbone-Übergängen
  - Weitere Verfahren
- Verbesserte Reaktion:
  - Automatisierung
  - “Näher am Verursacher” (→ Isolation ab dem Switch-Port)

Todo: Security – ein weiter, endloser Weg ... (2)

- Werkzeuge zur Überprüfung des Zustandes eines Rechners:
  - (Pro-)Aktive Überprüfung von Rechnern auf Systemschwächen (z.B. mit Nessus)
  - Zugang zum Netz nur nach Überprüfung des Sicherheitszustands
    - Cisco Network Admission Control (NAC)
    - Microsoft Network Access Protection (NAP)
- Intrusion-Detection/-Prevention (IDS/IPS)
  - Mehr Signaturen („as much as possible“)
  - Reaktion auf aktuelle Incident-Meldungen (CERT)
  - Zentraler Betrieb auf der Backbone-Router-Infrastruktur

Todo:
Security – ein weiter, endloser Weg ... (3)

- Bewusstseinsbildung der Nutzer
  („Steter Tropfen höhlt den Stein“)
  - Veranstaltungen in Verbindung mit den Instituten
  - Sensibilisierung durch aktuelle Vorfälle
- MWN-CERT (Computer Emergency Response Team)
  - Personal fehlt (noch)
  - Noch ein Traum, bei anderen bereits Realität:
    DFN-CERT, RUS-Stuttgart, Bürger-CERT, Bayern CERT,
    mCERT, CERT-Bund, ...

Organisatorisches Ziel:
Globale Security-Policy für das MWN (1)

Status

- ⇨ Minimaler Konsens
- ⇨ Policy: „Alles ist erlaubt, was nicht explizit verboten ist !“

Ziel

- ⇨ Globale Security-Policy für das MWN
- ⇨ Policy: „Alles was nicht explizit erlaubt ist, ist verboten !“

Rechtliche Problematik allgemein

- ⇨ Datenschutz, Personalräte, ...
- ⇨ Abstimmung mit der DFN-Rechtsstelle

Organisatorisches Ziel: Globale Security-Policy für das MWN (2)

Probleme bei der Aufstellung einer globalen Security-Policy

- Anzahl der Institutionen
  - ⇨ Abstimmung, ein langer (mühsamer ?) Weg durch die Instanzen
- Freiheit der Wissenschaft („offener Ansatz“)
  - ⇨ Das hat sich aufgrund der Ereignisse der letzten Zeit deutlich gebessert, aber ...
- Person-Power im LRZ als Dienstleister (derzeit ca. 2-3 Personen)
  - ⇨ Daran wird sich nichts ändern
  - ⇨ Gemeinschaftsaufgabe der am MWN-beteiligten Institutionen

Organisatorisches Ziel: Globale Security-Policy für das MWN (3)

Arbeiten hierfür sind (trotzdem) im Gange

- ⇨ Was tun andere vergleichbare Institutionen ?
- ⇨ Konzeptarbeiten propagieren (Firewall-Konzept für das MWN)
- ⇨ Pilothafte Lösungen im Produktionsbetrieb testen
- ⇨ Flankenhilfe des BSI (Bundesamt für die Sicherheit im Informationswesen)
- ⇨ Überzeugungsarbeit bei den Entscheidungsträgern