



WESTFÄLISCHE  
WILHELMS-UNIVERSITÄT  
MÜNSTER

# Sicherheit in Netzwerken - Intrusion Prevention

Raimund Vogl



wissen.leben  
WWU Münster

Raimund Vogl / ZIV



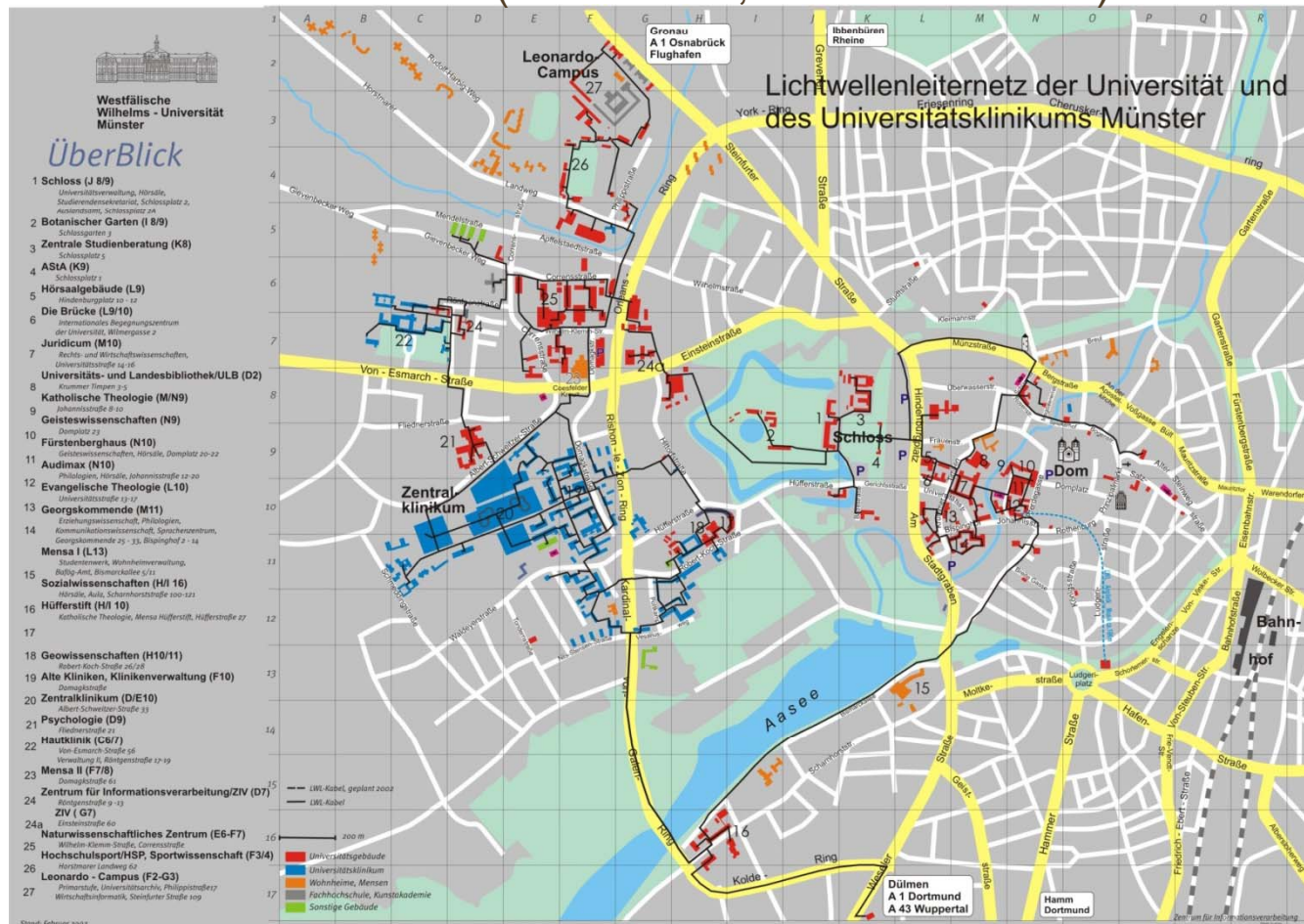
ZENTRUM FÜR  
INFORMATIONSS  
VERARBEITUNG

## Münster University (WWU), University Hospital (UKM)

- WWU: independent legal entity since 2007
  - 7 Faculties, 15 departments;
  - focus on humanities; science excellence in math, chemistry, physics - no engineering!
  - 5.000+ employees (600 professors)
  - ~40.000 students
  - No campus university – 280 buildings across Münster
  - Budget ~ 240 Mio € pa (2006)
- UKM: university hospital independent entity from WWU since 2007
  - ~ 7.500 employees
  - 1.500 beds, 370.000 outpatients/50.000 inpatients pa.
- ZIV (Zentrum für Informationsverarbeitung) of WWU is Network Service Provider for UKM



ca. 280 Gebäude; 240km LWL Backbone in Münster;  
ca.40.000 Netz-Dosen (26.000 Uni; 14.000 Klinikum)



# Eckpfeiler der IT/Netzwerksicherheit an der WWU Münster

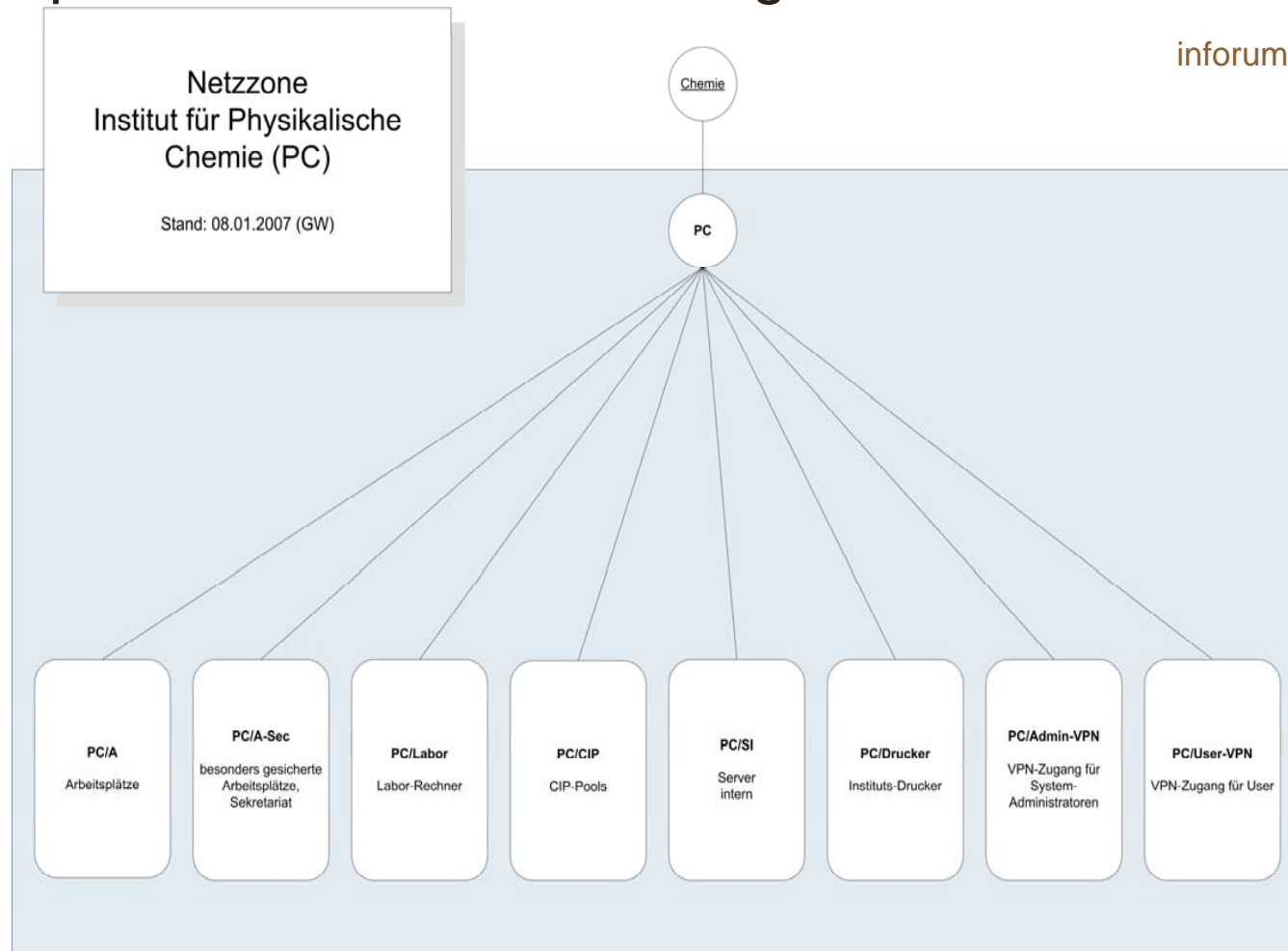
- IT Sicherheitsteam (Rektoratsbeschluss, 2002)
- IT Sicherheitsaudit – BSI Empfehlungen
- IT Sicherheitskonzept (Handbuch)
- CERT Team (derzeit ca. 420 Fälle pa.; Maximum in 2004 mit 1.500! 77% Copyright; Rest: DoS, Trojaner, Viren, SPAM Störungen)
- Netz-Strukturierung als kontinuierlicher Beratungs- und Entwicklungsprozess
- Nur personalisierte Accounts für Netzzugang und Windows-Domäne
- Nur registrierte Endgeräte werden an ihren Netzdosen ins LAN der Uni gelassen – sonstige Netzdosen liegen in einem Remote Access Bereich (abgeschottet)
- Nur WPA2 verschlüsseltes WLAN mit 802.1x Authentifizierung
- Einsatz von Anti-Virus Software verpflichtend für Geräte im Uni-Netz (Campuslizenz) – und dienstlich genutzten Heimgeräten (Heimnutzungsrecht)
- LANbase – Netzwerk-Datenbank: aktuelle qualitativ hochwertige Dokumentation: LAN Anschluss/Konfig/Ort/CAD Plan/Endgerät/Verantwortlicher Kontakt/Schutzbedarf
- Self service tools für Netzwerk-Konfiguration (switch port configuration, speed/VLANs/ACLs/Firewall rules) für lokale Administratoren

## Werkzeuge zur Umsetzung der Sicherheitskonzepte

- VLAN (Virtual LANs) Routing: Bedarfsgerechte Segmentierung (nicht Gebäudeorientiert!)
- Stateless firewalling mit ACLs (Access Control Lists) für VLANs
- Stateful firewalling
- Zentraler virtueller VPN Server (Virtual Private Network) für Remote-Zugriff (keine Backdoors!)
- IPS – Intrusion Prevention System: Virus Filtering; PortScans; DoS; attack pattern detection
- Zentrales Logging aller Sicherheitsevents (syslog-Server: data aggregation)
- Event Correlation Tool zur Erkennung von Attacken auf Basis aggregierter Daten
- NAC (Network Access Control) / NAP (Network Access Protection)
- Email SPAM/Virus Filtering appliance: Benutzer müssen diese Filter jedoch in eigenem Willensakt aktivieren!
- Content Filtering/Secure Web Proxy: Verschlüsselte Web-Verbindungen; Jugendschutz; ...
- **Virus-Check also an 3 Stellen:**

- **auf IPS -> im E-Mail SPAM/Virus-Filter bzw. Content Filter -> im Virus Filter am**

## Beispiel für Netz-Strukturierung



inforum 1/2006

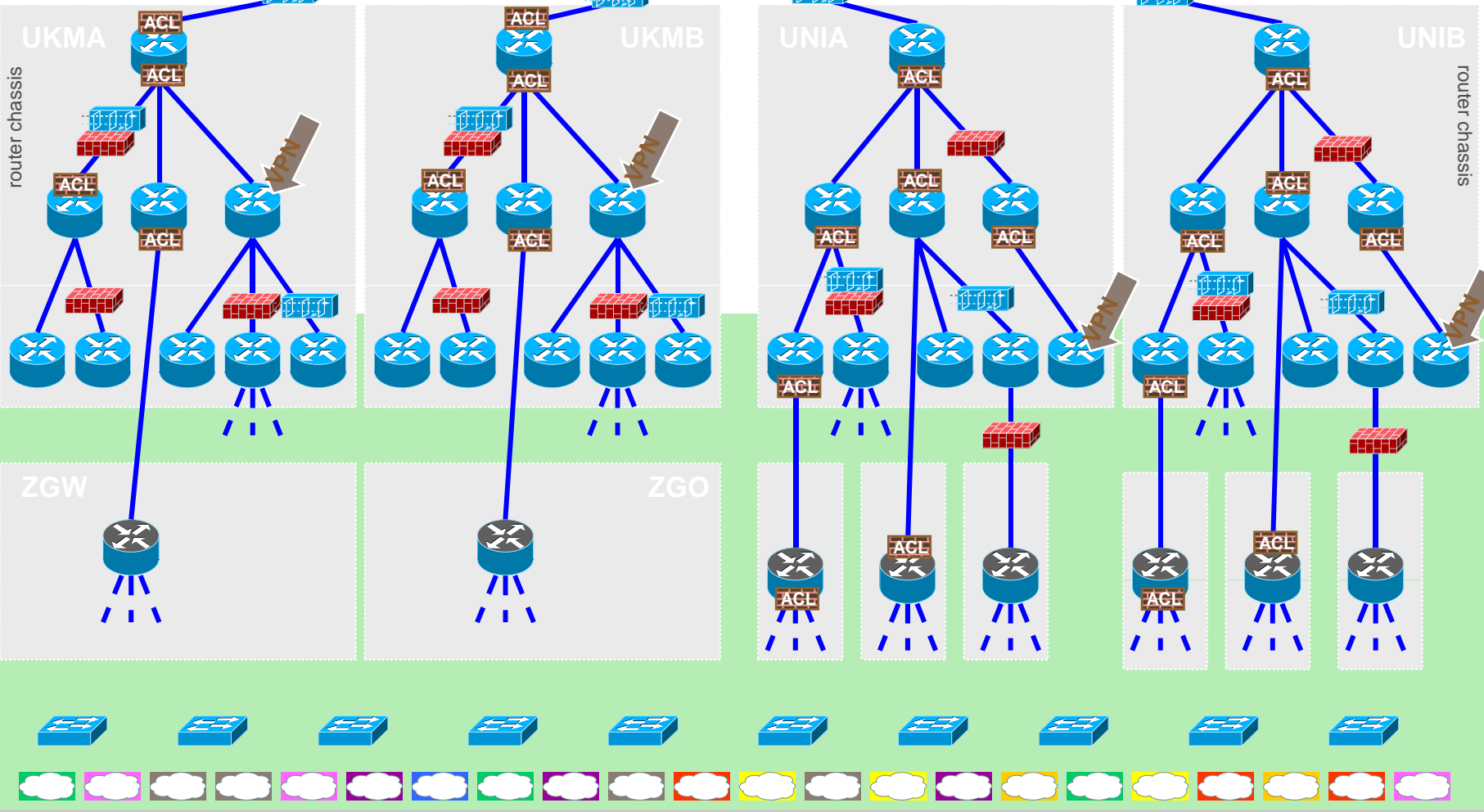


WESTFÄLISCHE  
WILHELMS-UNIVERSITÄT  
MÜNSTER

X-WiN

ZENTRUM FÜR  
INFORMATIONEN  
VERARBEITUNG

(exemplarily)



www.Umünster  
L2 distribution

## Intrusion Prevention Systems (IPS) - Bestandteile

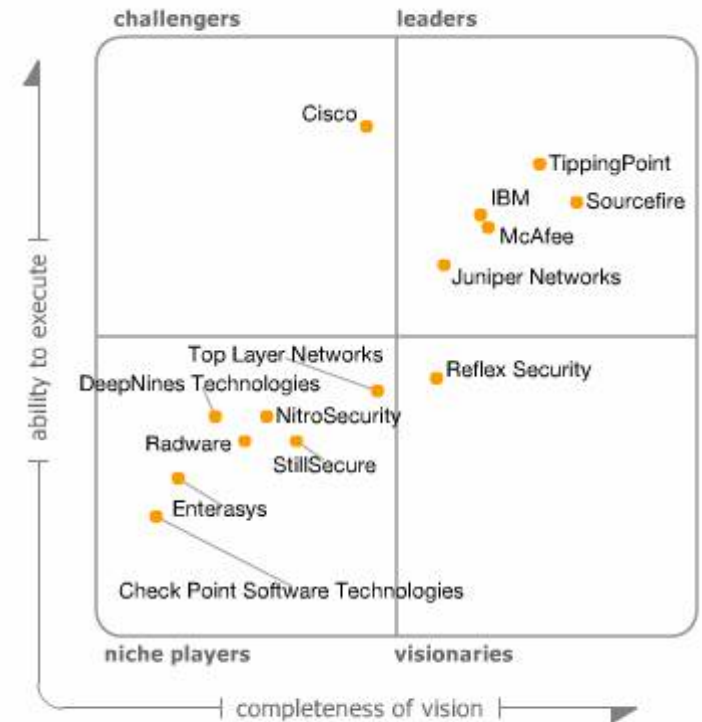
- Netzbasierende Systeme, Netzsensoren
  - NIDS ... Network Intrusion Detection System
  - NIPS ... Network Intrusion Prevention System
  - **VIPS ... *Virtual Intrusion Prevention System***
- Hostbasierende Systeme, Hostsensoren, HIPS
- Managementstationen
  - *Datenbankkomponenten*
  - *Auswertungsstationen*
  - Die meisten Systeme weisen eine integrierte Funktion auf.

## Aufgaben und Anforderungen an NIPS/VIPS

- überwachen des Verkehr zwischen Datennetzen
- „unsichtbar“ im Netz
- Arbeiten in wirespeed, minimale Latenzzeiten
- Schutz von großen Datennetzen vor netzwerkbasierenden Angriffen z.B. DoS- und DDoS-Attacken, syn-flood
- Schutz vor Viren, Würmern,
- Unterdrückung des Ausnutzen von Sicherheitslücken durch exploits
- Einfache Installation
- Mandantenfähigkeit:
  - Trennung verschiedener Netzzonen durch Virtualisierung innerhalb eines Gerätes, z.B. UKM, Universität, RAS-Bereich, IVV'en
  - Eigene Sicherheitspolicy für eigene Netzzonen

## Netzsensoren

- überwachen den Verkehr zwischen Datennetzen
- Typische Vertreter (CPU and ASIC basiert) sind:
  - McAfee Intrushield 4000
  - 3Com TippingPoint 2400
  - Sonicwall Pro 5060
  - Top Layer Attack Mitigator IPS 5500
  - etc... siehe Gartner Studie  
<http://mediaproducts.gartner.com/reprints/tippingpoint/154849.html>
- als appliance im Netzwerk integriert



As of February 2008



GARE – Global Attack Response Editor: ca. 1000 Signaturen bekannt.  
Individuell nach virtueller IPS (Mandant) blockierbar/freigebbar

Configure Attack Detail for Attack Category: All Protocols

View/Search Option View / Edit Bulk Edit

Att...	Ale...	Attack Name	Attack ID ▲	Sev...	C...	Pa...	S...	Bl...	N...	# ...
✓	✓	DCERPC: Microsoft Windows LSASS B...	Ox47601c00	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft Windows NETDDE ...	Ox47601d00	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft Message Queuing ...	Ox47601f00	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft Plug and Play Servi...	Ox47602000	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft NetWare Client Ser...	Ox47602100	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft TAPI Service Buffer ...	Ox47602200	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft SPOOLSS Service ...	Ox47602300	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft MSDTC buffer overfl...	Ox47602500	5 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	DCERPC: Microsoft Plug and Play Servi...	Ox47602600	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft Plug and Play Servi...	Ox47602700	4 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	DCERPC: Microsoft SrvSvc Service DoS	Ox47602800	4 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	DCERPC: Microsoft Webclient Overflow	Ox47602900	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft Message Queue M...	Ox47602a00	7 (High)	✓		✓ (P)	✓ (P)	✓ (G)	6
✓	✓	DCERPC: Microsoft MSDTC BuildConte...	Ox47602c00	5 (Medi...	✓		✓ (D)	✓ (R)		5
✓	✓	DCERPC: SRVSVC Buffer Overflow	Ox47602e00	5 (Medi...	✓		✓ (D)	✓ (R)		5
✓	✓	RDP: Microsoft Terminal Services RDP ...	Ox47900100	5 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	RDP: Microsoft Remote Desktop Protoc...	Ox47900200	4 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	UPnP: NOTIFY Buffer Overflow	Ox47a00200	5 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Dabber Worm	Ox48301700	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Stdbot.B Worm	Ox48301900	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Mytob.gen@MM	Ox48303900	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Klez.h@MM	Ox48304400	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/MyWife.d@MM	Ox48304500	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Zafi@MM Worm	Ox48304900	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Polybot	Ox48304a00	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Bagle@MM Worm Variants I	Ox48304b00	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Bagle@MM Worm Variants II	Ox48304c00	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Netsky@MM Worm	Ox48304d00	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Lovgate@MM Worm	Ox48304e00	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Mydoom@MM Worm Varia...	Ox48304f00	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5
✓	✓	WORM: W32/Sober@MM	Ox48305000	6 (Medi...	✓		✓ (G)	✓ (R)	✓ (G)	5

Done

Java Applet Window

# Vorteile von Netzsensoren

- Entlastung/geringere Gefährdung von Endsystemen
- Schutz von Netzwerkkomponenten
- Plattformunabhängig
- Schutz großer Bereiche
- Einfache Installation
- Laufende Pflege Signaturen-Datenbank durch Hersteller

## Nachteile von Netzsensoren

- Angriffserkennung durch Netzsensor fehlerbehaftet, finetuning notwendig
- Störungen im Netzverkehr möglich (Sequenzänderung Datenpakete; neu hinzukommende nicht erprobte Verkehrstypen; ...)
- Kann zum Flaschenhals werden (Option: Bypass durch Policy Based Routing)
- Angriffsverhalten kann nur begrenzt nachvollzogen werden
- Schwierige Implementierung bei redundanten Systemen

## McAfee IntruShield 4010



- intrusion detection and prevention
- signature based (e.g. anti virus)
- behavior based (e.g. anti DoS)
- combined (day-zero-attacks)
- blocking in real time (if required)
- up to 2 Gbps throughput
- up to 1000 virtual systems (e.g. vlan based)
- transparent mode (“in-line mode”)
- management front end multi-subscriber capable (“administrative domains”)