

Gibraltar Firewall



Rene Mayrhofer

OS04

Graz, 22. Oktober 2004

14:00-16:00

Vortragsinhalt

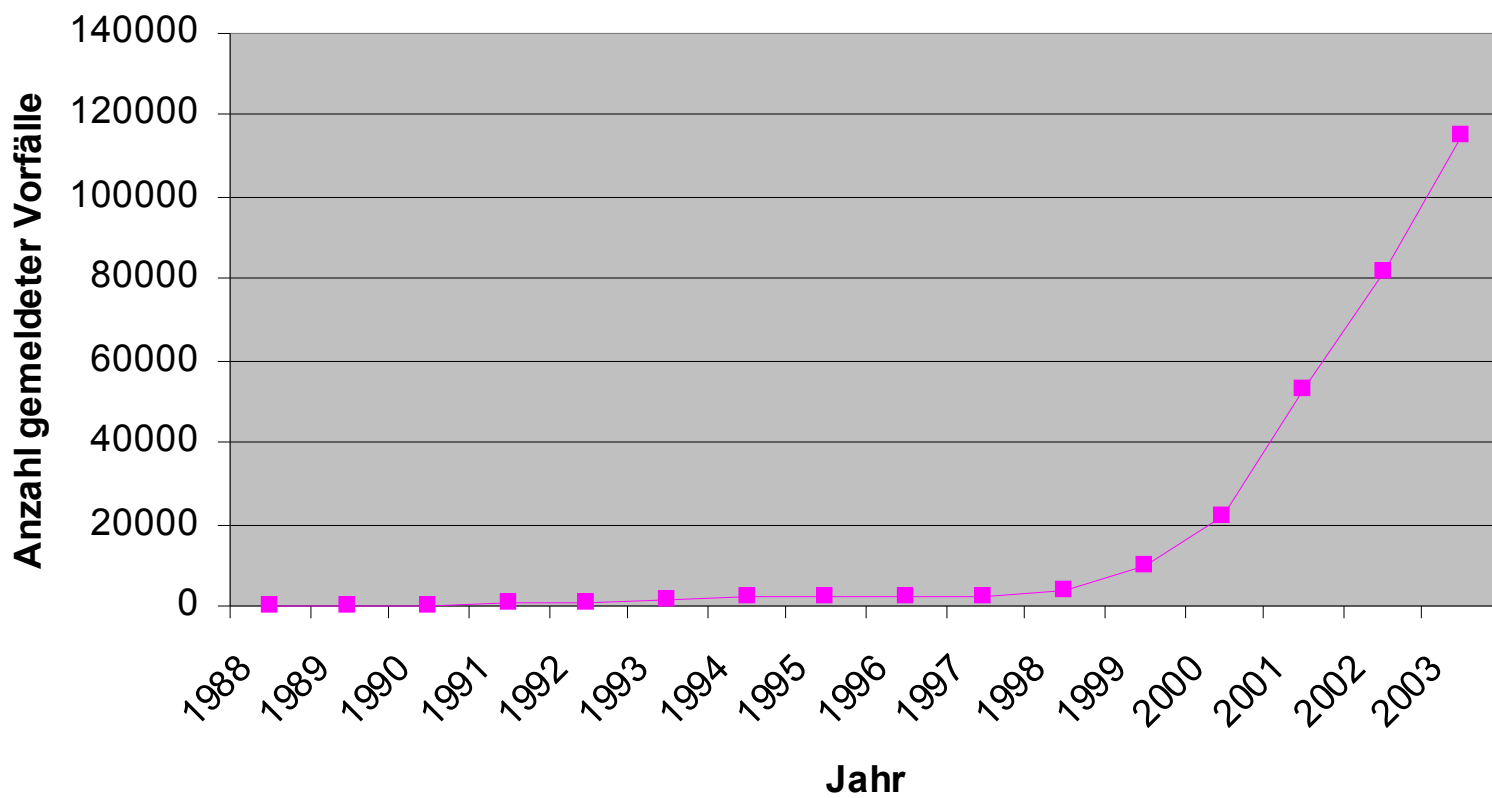
- **Warum Firewalls ?**
- Prinzipielle Firewalltechniken und Netzwerktopologien
- Anti-Spam Techniken auf Mail-Gateway/Firewalls
- Gibraltar
- Praxisbeispiel
- Tipps & Tricks, Details zu Linux mit read-only Root-Filesystemen

Internet – Die Bedrohungen



*Von Viren, Würmern und
Trojanern*

Sicherheitsvorfälle



Abgrenzung

- Grenze zwischen Viren, Würmern und Trojanern manchmal fließend
 - **Viren:** Verbreiten sich innerhalb von PCs
 - **Würmer:** Nutzen die Infrastruktur eines Netzwerkes, um sich zu verbreiten
 - **Trojaner:** Tarnkappenbomber unter den Viren. Sie tarnen sich meistens als nützliche Programme, um im Verborgenen ihre Schadensfunktion auszuüben.
- Virus kann generell auch als Oberbegriff der Schädlinge verwendet werden
- Unterschied liegt genau genommen in der Verbreitung

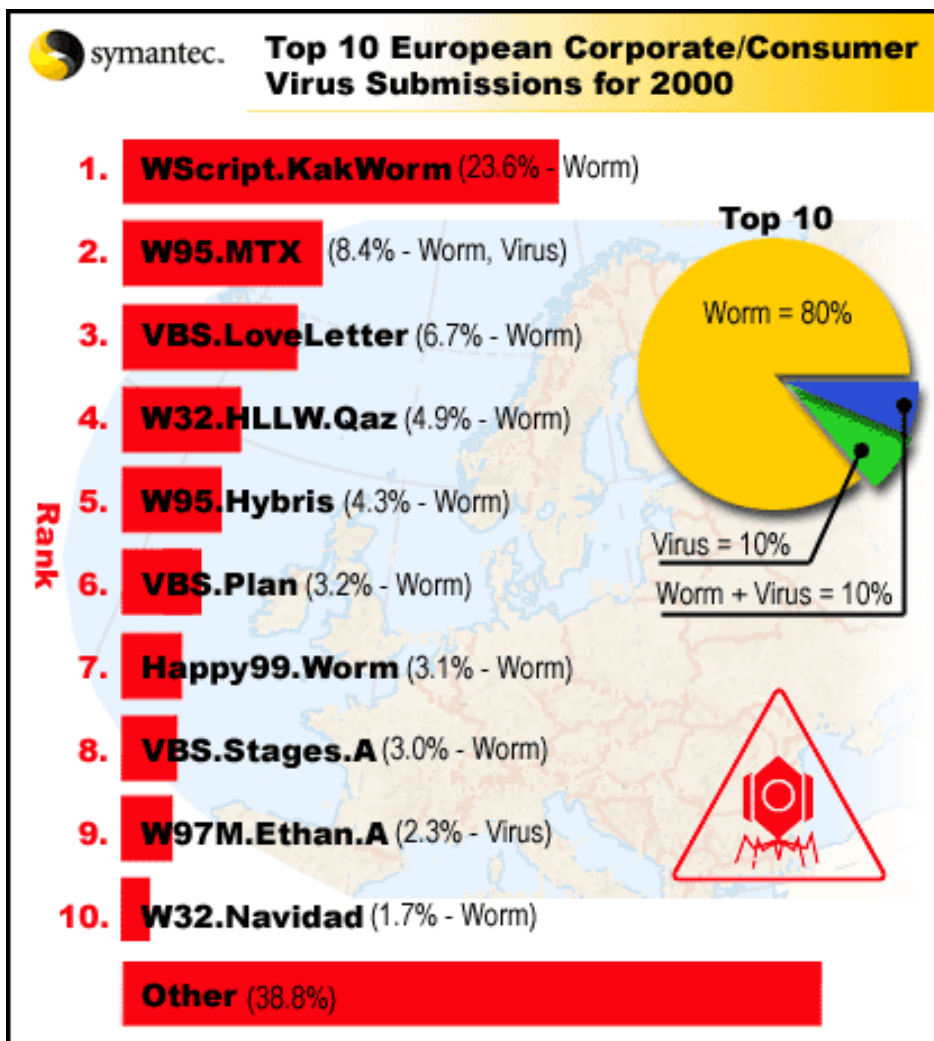
Virus

- Schadensprogramm (Programmcode), dass sich von Datei zu Datei auf einem Computer ausbreitet
- Virus repliziert sich selbst
- Virus muss aktiviert werden
- Strategie: den Wirt beherrschen
 - So viele Dateien wie möglich infizieren
 - Funktionen blockieren
 - Übertragung durch Diskette, E-Mail ...
 - Langsame Infektion
- Technisch gesehen
 - Ausführbarer Code, also ein Programm von meist geringem Umfang
 - Viren werden programmiert
 - 2 Komponenten
 - Verbreitungsmechanismus
 - Nutzlast oder Schadensroutine

Virus (2)

- Was können Viren
 - Viren verursachen Schäden in Millionenhöhe
 - Viren führen zu Arbeitszeitverlusten
- Was können Viren nicht
 - Dateien auf schreibgeschützten Datenträgern infizieren
 - Infizieren keine Dokumente (Ausnahme: Word...)
 - Infizieren keine komprimierten Dokumente
- Anzahl der Viren im Umlauf
 - Gesamtzahl der derzeit bekannten Viren: über 50.000
 - Nur 1 bis 2 Prozent auch im Umlauf, Rest: Laborviren
- Typen von Viren
 - Dateiviren: infizieren Programmdateien
 - Bootsektorviren: zerstörerisch, setzt sich auf einem Teil der Festplatte fest, und wird beim Starten in den Speicher geladen
 - Makroviren: Fortpflanzung unabhängig vom Betriebssystem, Austausch über E-Mails und Dokumente

Viren – TOP 10



Quelle: Symantec
<http://www.symantec.at>

Würmer / Trojaner

- Würmer: **Selbstständige Verbreitung über Netzwerk**
- Gründe für die rasche Verbreitung
 - Homogene Softwarelandschaft
 - Früher mehr verschiedene Betriebssysteme und individuelle Anwendungen
 - Ende 2000: 380 Millionen PC-Benutzer mit Internetzugang
 - Fehlende Anonymität: „Ich war hier Syndrom“
 - Einfachheit der Programmierung (Makro-Sprachen, z.B. VBA)
- Trojaner: tarnen sich als nützliche Anwendung
 - Aushorchen sensibler Daten
 - Übermittlung an Urheber des Trojaners
 - Backdoor-Trojaner: richten Hintertüren auf befallenem System ein
 - Fernkontrolle

Trends

- „Blended Threats“: gemischte Bedrohungen
 - Kombiniert Virus, Wurm und Trojaner
 - Nutzung von bekannten Schwachstellen

Blended Threat	Bugtraq ID of Targeted Vulnerability	Vulnerability Name	CVE Reference Number	Date of Vulnerability Discovery	Date of Blended Threat Outbreak	Time Delay from Discovery to Outbreak
W32.Klez	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	25 Oct 2001	210 days
W32.Sobig	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	9 Jan 2003	651 days
W32.Bugbear	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	30 Sep 2002	550 days
W32.Yaha	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	15 Feb 2002	349 days
W32.Nimda	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	18 Sep 2001	538 days
	2708	Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability	CVE-2001-0333	15 May 2001	18 Sep 2001	126 days
	1806	Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability	CVE-2000-0884	17 Oct 2000	18 Sep 2001	336 days
W32.Opaserv	1780	Microsoft Windows 9x / Me Share Level Password Bypass Vulnerability	CVE-2000-0979	10 Oct 2000	30 Sep 2002	710 days
W32.Lirva	2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	29 Mar 2001	7 Jan 2003	649 days
W32.SQLExp.Worm	5311	Microsoft SQL Server Resolution Service buffer overflows allow arbitrary code execution	CAN-2002-0649	25 Jul 2002	24 Jan 2003	208 days
CodeRed.Worm	2880	Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability	CVE-2001-0500	18 Jun 2001	16 Jul 2001	28 days

Aktuelle Bedrohungen

- Blended Threats: stark steigende Anzahl
- Ausnutzung von bekannten Schwachstellen
 - Systeme werden nicht gepatcht
 - Bsp: Klez, SoBig, Bugbear, Yaha, Nimda haben alle die selbe Schwachstelle wiederholt ausgenutzt (CVE-2001-0154)
 - Strategien gegen diese Bedrohungen
 - Unternehmensweite Patch-Strategie
- W32 Viren und Würmer
 - Win32 API wird genutzt
 - Anzahl stark steigend
 - 1. HJ 2001: 445, 2. HJ 2002: 687, 1. HJ 2003: 994
- Linux
 - 1998: erster Linux-Wurm: Linux.ADM.Worm
 - OpenSSL-Schwachstellen
- Neue Faktoren
 - Instant – Messaging und Peer-to-Peer Applications
 - Massen-Mailer mit integrierter E-Mail-Engine
 - Diebstahl von vertraulichen Daten

Beispiel: Blaster Worm

- Schwachstelle
 - MS03-026: Pufferüberlauf in RPC kann Ausführung von Code ermöglichen
 - **16. Juli 2002**
 - Ports 135, 139, 445: Systeme: NT, 2000, XP, Server 2003
- Bedrohung
 - Port 135, XP und 2000
 - msblast.exe in %windir%\system32
 - DoS gegen Microsoft Windows Update-Server (windowsupdate.com)
 - Entdeckung: **11.8.2003**
- Technische Details
 - Überprüfung ob bereits infiziert?
 - Registry-Eintrag: „windows auto update=„msblast.exe“
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
 - IP-Adresse wird generiert, und versucht zu infizieren
 - Port 135, DCOM RPC Sicherheitslücke, 80% XP, 20% 2000

Blaster Worm (2)

- Auswirkungen
 - lokales Teilnetz wird mit Anfragen auf Port 135 überlastet
 - auch NT und 2003 kann abstürzen
 - RPC-Dienst kann abstürzen
 - bei Absturz RPC: Standardverfahren XP und 2003: Computer neu starten (kann deaktiviert werden)
- Technische Details
 - Shell-Prozess wird gestartet, der Port 4444 überwacht -> ermöglicht dem Angreifer auf dem infizierten System Befehle einzugeben
 - Überwacht UDP-Port 69: bei Anfrage: sendet msblast.exe
 - bei gewissem Datum: DoS-Angriff
 - Port 80 von windowsupdate.com wird mit SYN-Paketen geflutet
 - jede Sekunde 50 HTTP-Pakete
 - Jedes Paket 40 Byte lang
 - Text:
 - I just want to say LOVE YOU SAN!! billy gates why do you make this possible ? stop making money and fix your software!!

Linux am Desktop – Virenproblem gelöst ?

- Herbst 1996: Staog (erster bekannter Linux Virus)
- 17.1.2001: Ramen (wuftpd, rpc.statd, lprng)
⇒ Lion (+Cheese), Adore
- März 2001: Lindose (Cross-Plattform Win32- und ELF-Virus)
- 13.9.2002: Slapper (Apache mod_ssl, Schwachstelle im August 2002 entdeckt): > 14000 Rechner infiziert
⇒ Devnull
- 2004: Phatbot ?
- ...

Hackerangriffe

- Bedrohung durch Hacker im Vergleich zu Viren, Würmer und Trojaner eher gering
- Problem: werden meistens **nicht** bemerkt
- stark steigend: Script Kiddies
- Nur ein geringer Prozentsatz verursacht Schäden
- Motivation: Herausforderung, Thrill
- Spezialwissen öffentlich verfügbar
 - Hunderte von professionellen Tools
 - Schwachstellen sind bekannt
- Social – Hacking
 - ermitteln von Benutzerbezogenen Daten (SV-Nr, Gebdat, Name, Kinder, Frau, Hobbys, ...)
- WLAN – Hacking
 - Meistens nicht verschlüsselt
 - War – Driving
- Angriffe von innen

Quellen

- Sicherheitslücken
 - Microsoft Security-Bulletins
 - Symantec
 - www.securityfocus.com
 - Klassifikation nach CVE-ID, BugTrack ID, ...
- Viren
 - Kaspersky
 - Symantec
 - McAfee
 - F-Prot
- Schwachstellenanalyse
 - Qualys
 - Nessus (GPL)

Die 4 Säulen der Netzwerksicherheit

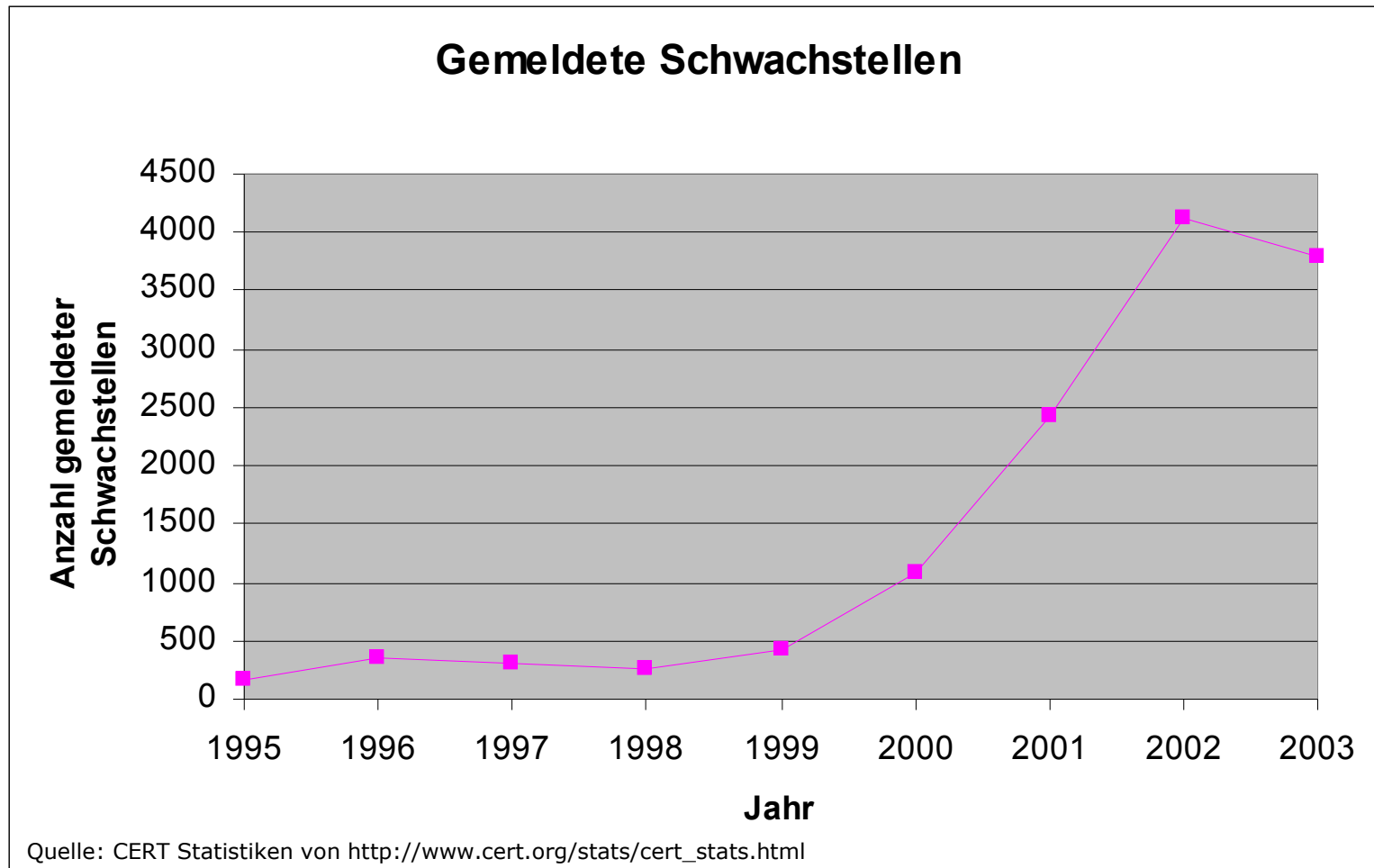
Perfekte Sicherheit gibt es nicht. Sicherheit ist immer eine Kombination aus mehreren Maßnahmen

- **Firewalls**
 - Regelt die sichere Kommunikation zwischen dem unternehmensinternen Netzwerk und dem Internet unter Berücksichtigung definierter Regeln
 - Ausgewählter Datenverkehr wird von Firewalls bewusst erlaubt. Diese offenen Zugangspunkte sind der „optimale“ Punkt für eine gezielte Attacke.
- **Intrusion Detection (IDS)**
 - Meldet dem Administrator unberechtigte Eindringversuche in das firmeninterne Netzwerk oder anomalen Datenverkehr.
 - Der Administrator wird erst beim Auftreten der Attacke informiert. Oft kann es zu diesem Zeitpunkt bereits zu spät für eine wirkungsvolle Behebung der Sicherheitslücken sein.
- **Vulnerability Scanning**
 - Ermöglicht Unternehmen, Schwachstellen zu beheben, bevor sie ausgenutzt werden. Identifiziert Schwachstellen und schlägt Lösungen zum Beheben der vorhandenen Lücken vor.
 - Informiert nicht über Eindringversuche und Viren. Diese Aufgaben werden von IDS und Virensclannern wahrgenommen
- **Virenschutz**
 - Überwacht Dateiserver und E-Mail-Server auf Viren und hindert sie daran, in einem System aktiv zu werden.
 - Kann keine Sicherheitslücken entdecken oder beheben, die von Hackern, Internetwürmern oder automatisierten Angriffen ausgenutzt werden.

Schwachstellenanalyse (Vulnerability Management)

- über 90% aller Angriffe basieren auf bekannten Schwachstellen
- derzeit tausende bekannte Schwachstellen
 - sämtliche Betriebssysteme und Anwendungen betroffen
 - pro Woche werden mehrere Dutzend Schwachstellen entdeckt
- Zeit von der Entdeckung bis zur Ausnutzung sinkt drastisch
 - Bsp: Blaster: keine 4 Wochen
 - früher: teilweise mehrere Monate
- automatisierte Schwachstellenanalyse gibt einen regelmäßigen Überblick über aktuelle Schwachstellen in den eigenen Systemen
- ausführliche Beschreibung der Schwachstelle
- Lösungsansätze
- Zeitaufwand und Kosten sind sehr gering
- Trendanalyse
- Behebung der Schwachstellen wird protokolliert
- Ergänzung zu Firewall, IDS und Virensclannern

veröffentlichte Schwachstellen



Vortragsinhalt

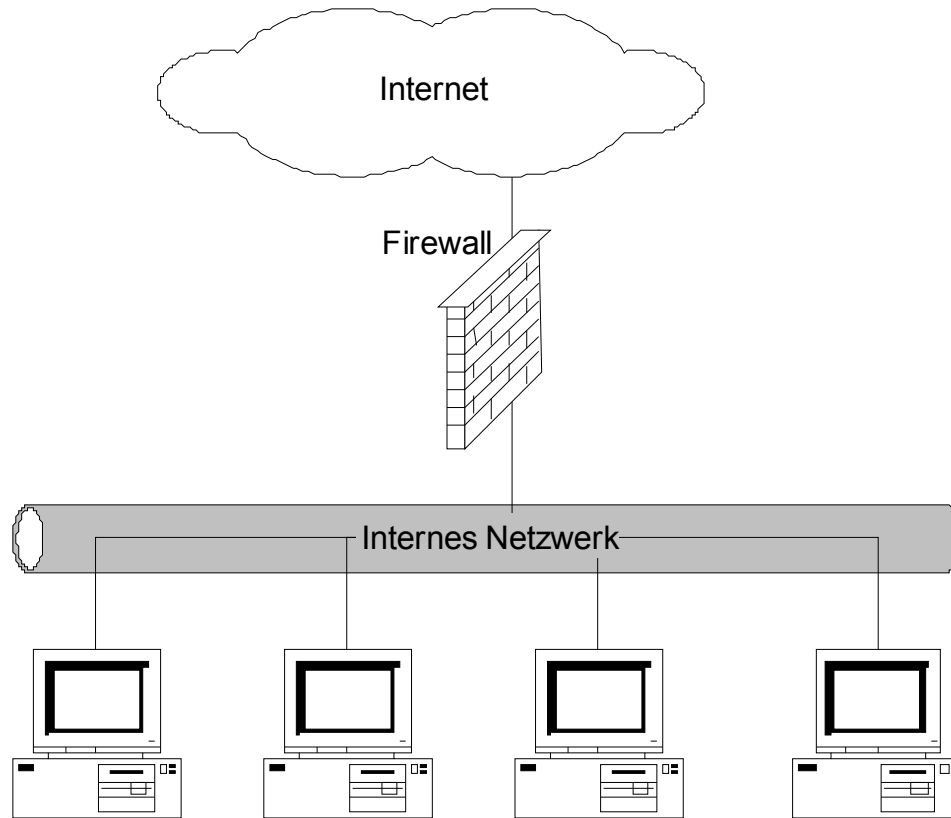
- Warum Firewalls ?
- **Prinzipielle Firewalltechniken und Netzwerktopologien**
- Anti-Spam Techniken auf Mail-Gateway/Firewalls
- Gibraltar
- Praxisbeispiel
- Tipps & Tricks, Details zu Linux mit read-only Root-Filesystemen

Einführung in Firewalltechnologien



*Firewall, Paketfilter, Proxy-
Server, NAT, VPN*

Was ist eine Firewall?



Firewall - Grundlagen

- Eine Firewall ist der Schwerpunkt der Sicherheitsmaßnahmen
 - gesamter Verkehr muss Kontrollpunkt passieren
 - Verkehr kann überwacht werden
- Durchsetzen der Sicherheitspolitik
 - verhindert, dass Daten nach außen gelangen
- Protokollierung
 - protokolliert den laufenden Netzwerkverkehr
- Verkleinerung der Angriffsfläche
 - trennt verschiedene Bereiche des Firmennetzwerks
 - DMZ (Demilitarisierte Zonen)
- **schützt nur Verbindungen, die durch sie hindurchgehen**
- schützt nicht / nur bedingt gegen Angriffe von innen
- bietet keinen vollständigen Virenschutz
- kann sich nicht selbst einrichten

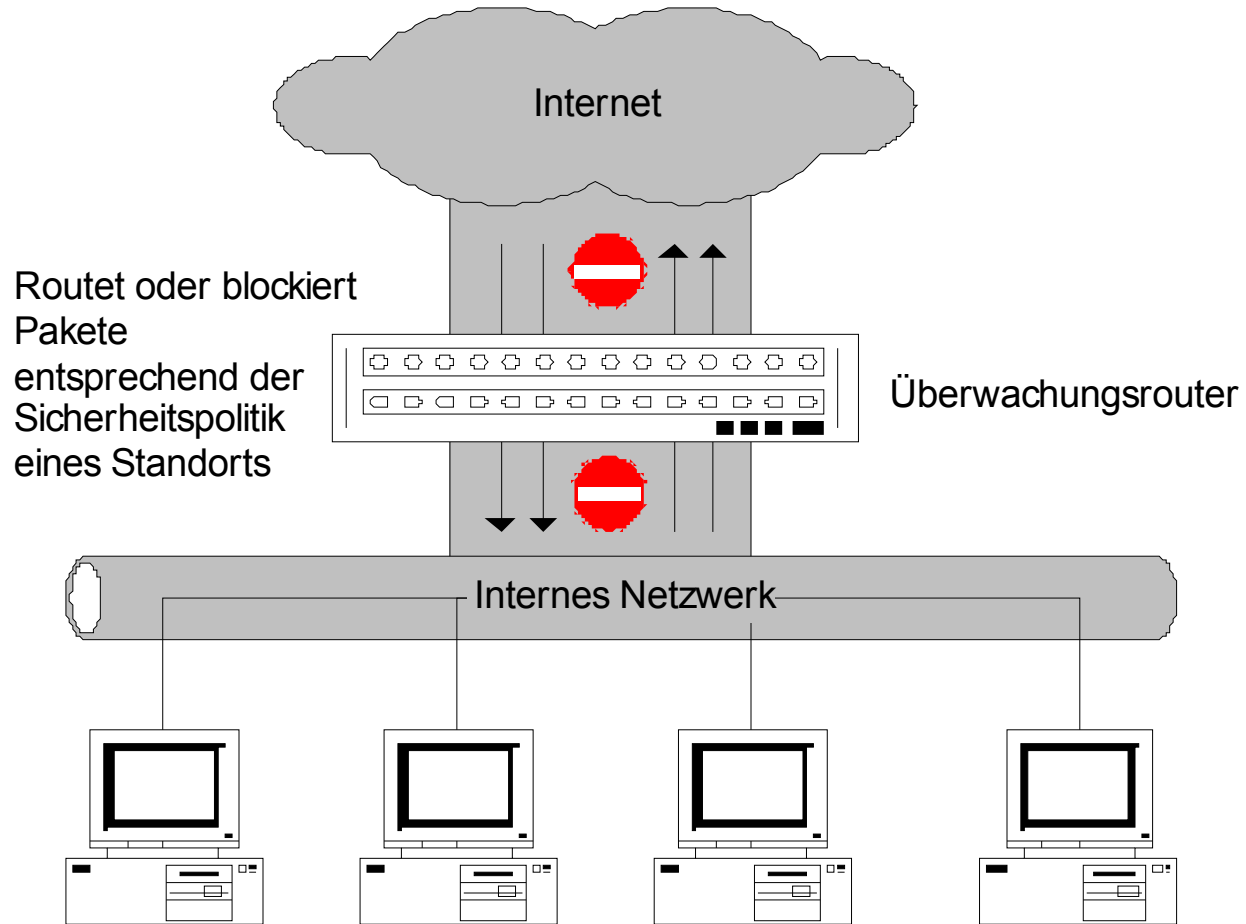
Firewall - Techniken

- **Paketfilterung:** Kern einer jeden Firewall, Umsetzung der Sicherheitsrichtlinien und Überwachung des Netzwerktraffics
- **Proxy-Dienste:** Sicherheits- und Performancefunktion. Application-Level-Inspection, Deep Inspection
- **NAT** (Network – Adress – Translation): Adressübersetzung
- **VPN** (Virtuelle Private Netzwerke): **IPSec**

ISO/OSI – 7-Schichtenmodell

Schicht	ISO/OSI-Modell		TCP/IP-Modell
7	Applikationsschicht	Applikations- Protokolle	telnet, ftp, nfs rlogin, DNS smtp, snmp X-Windows Socket library
6	Präsentationsschicht		
5	Kommunikations- Steuerungsschicht		
4	Transportschicht	Transport- Protokolle	TCP UDP
3	Netzwerkschicht	Internetwork- Protokolle	IP EGP, RIP ICMP ARP, RARP
2	Sicherungsschicht	Network- Access- Protokolle	Ethernet CSMA/CD Token Ring FDDI
1	Bitübertragungsschicht		

Paketfilterung



Paketfilter

- Paketfilter arbeiten auf Ebenen 3 und 4 des ISO/OSI Schichtenmodells
- routen Pakete zwischen internen und externen Hosts
- arbeiten selektiv
- erlauben und blockieren Pakete

- Paket-Header für IPv4:
 - IP-Quelladresse
 - IP-Zieladresse
 - Protokoll
 - TCP oder UDP-Quellport
 - TCP oder UDP-Zielport
 - ICMP-Meldungstyp
 - Paketgröße
 - ...

ISO/OSI – 7-Schichtenmodell

Schicht	ISO/OSI-Modell		TCP/IP-Modell
7	Applikationsschicht	Applikations- Protokolle	telnet, ftp, nfs rlogin, DNS smtp, snmp X-Windows Socket library
6	Präsentationsschicht		
5	Kommunikations- Steuerungsschicht		
4	Transportschicht	Transport- Protokolle	TCP UDP
3	Netzwerkschicht	Internetwork- Protokolle	IP EGP, RIP ICMP ARP, RARP
2	Sicherungsschicht	Network- Access- Protokolle	Ethernet CSMA/CD Token Ring FDDI
1	Bitübertragungsschicht		

Paketfilter

- prinzipielle Unterscheidung in stateless und stateful inspection
- **Stateless**
 - statische Paketfilterung
 - unabhängig von bereits eingetroffenen Paketen
 - Entscheidung über Aktion (Durchlassen oder Blockieren) für jedes einzelne Paket
- **Stateful**
 - dynamische Paketfilterung
 - zustandsabhängig
 - untersucht nicht nur den Header eines Pakets, sondern auch den Inhalt
 - beobachtet den Status der Verbindung
 - Kontext-Analyse der Verbindung

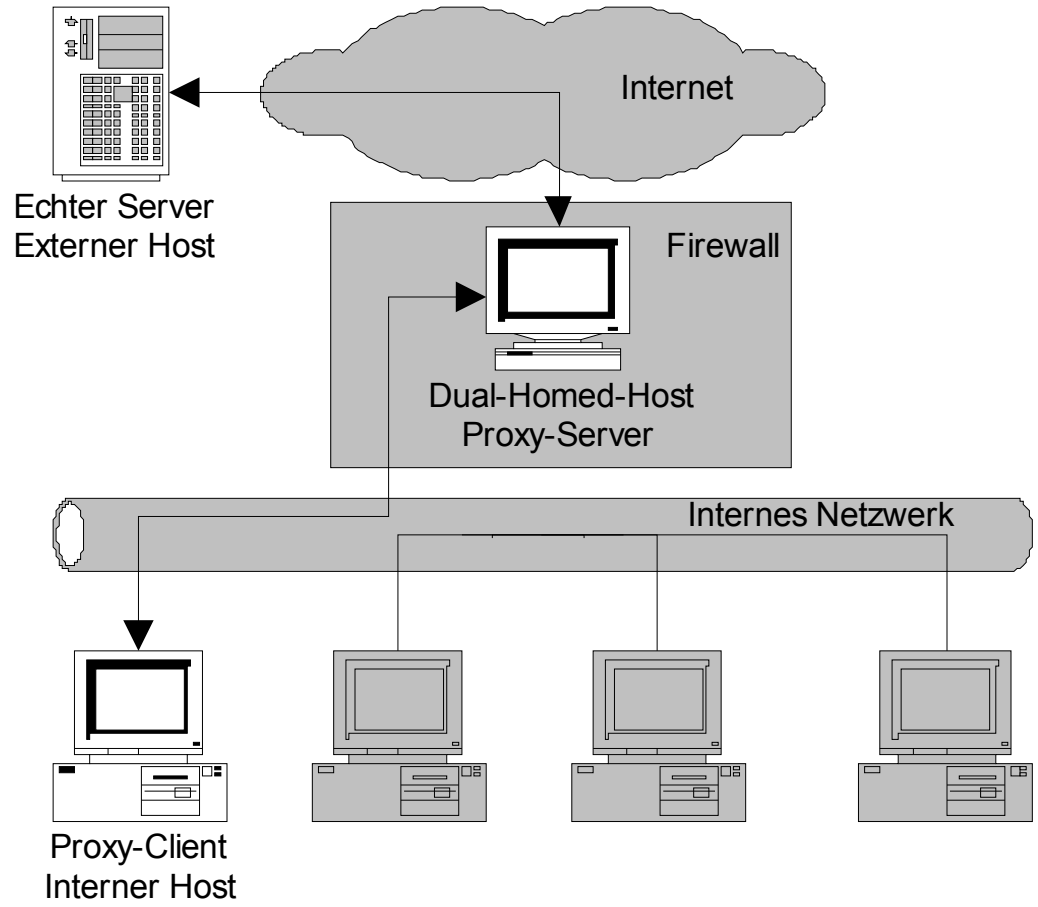
Paketfilter

- bekannte Daten
 - Schnittstelle, an der das Paket empfangen wurde.
 - Schnittstelle, an die das Paket weitergeleitet werden soll.
 - ob das Paket eine Antwort auf ein anderes Paket war (**stateful**)
 - wie viele andere Pakete zuvor zu oder von dem gleichen Host übertragen wurden (**stateful**).
 - ob das Paket identisch mit einem zuvor gesendeten Paket ist.
 - ob das Paket Teil eines größeren Pakets ist, das in einzelne Teile zerlegt (fragmentiert) wurde (deshalb sehr oft Defragmentierung auf Firewalls, weil die weiteren Fragmente außer dem ersten keinen IP-Header mehr haben).

Paketfilter - Aktionen

- Standard
 - Paket schicken (ACCEPT)
 - Paket verwerfen (DROP)
 - Paket mit Fehlermeldung zurückweisen (REJECT)
 - Informationen über Paket aufzeichnen (LOG)
- Erweitert
 - einen Alarm auslösen
 - Bei stateful: neue Verbindung in Verbindungstabelle eintragen
 - Optionale Zusatzfunktionen: Paket in bestimmter Klasse zählen, Paketgröße zu Quota addieren, Paket in Liste von kürzlich gesehenen Host eintragen,
 - Paket vor dem Weitersenden verändern !
 - Paket an einen lokalen, transparenten Proxy weitergeben

Proxy - Dienste



Proxy - Dienste

- Proxys arbeiten auf den Ebenen 5 bis 7
- Stellvertreter
- spezielle Anwendungen oder Server-Programme, die Benutzeranfragen an Internet-Dienste entgegennehmen und sie an den eigentlichen Dienst weiterleiten.
- Application-Level-Gateways
- Erhöhung der Sicherheit
- höhere Effektivität des Netzwerks bei caching Proxys
- transparent oder nicht transparent
- Kann für bestimmte Protokolle nötig sein, da Eingriff auf Ebenen 5 bis 7 bei NAT nötig sind (z.B. FTP, H.323)

ISO/OSI – 7-Schichtenmodell

Schicht	ISO/OSI-Modell		TCP/IP-Modell
7	Applikationsschicht	Applikations- Protokolle	telnet, ftp, nfs rlogin, DNS smtp, snmp X-Windows Socket library
6	Präsentationsschicht		
5	Kommunikations- Steuerungsschicht		
4	Transportschicht	Transport- Protokolle	TCP UDP
3	Netzwerkschicht	Internetwork- Protokolle	IP EGP, RIP ICMP ARP, RARP
2	Sicherungsschicht	Network- Access- Protokolle	Ethernet CSMA/CD Token Ring FDDI
1	Bitübertragungsschicht		

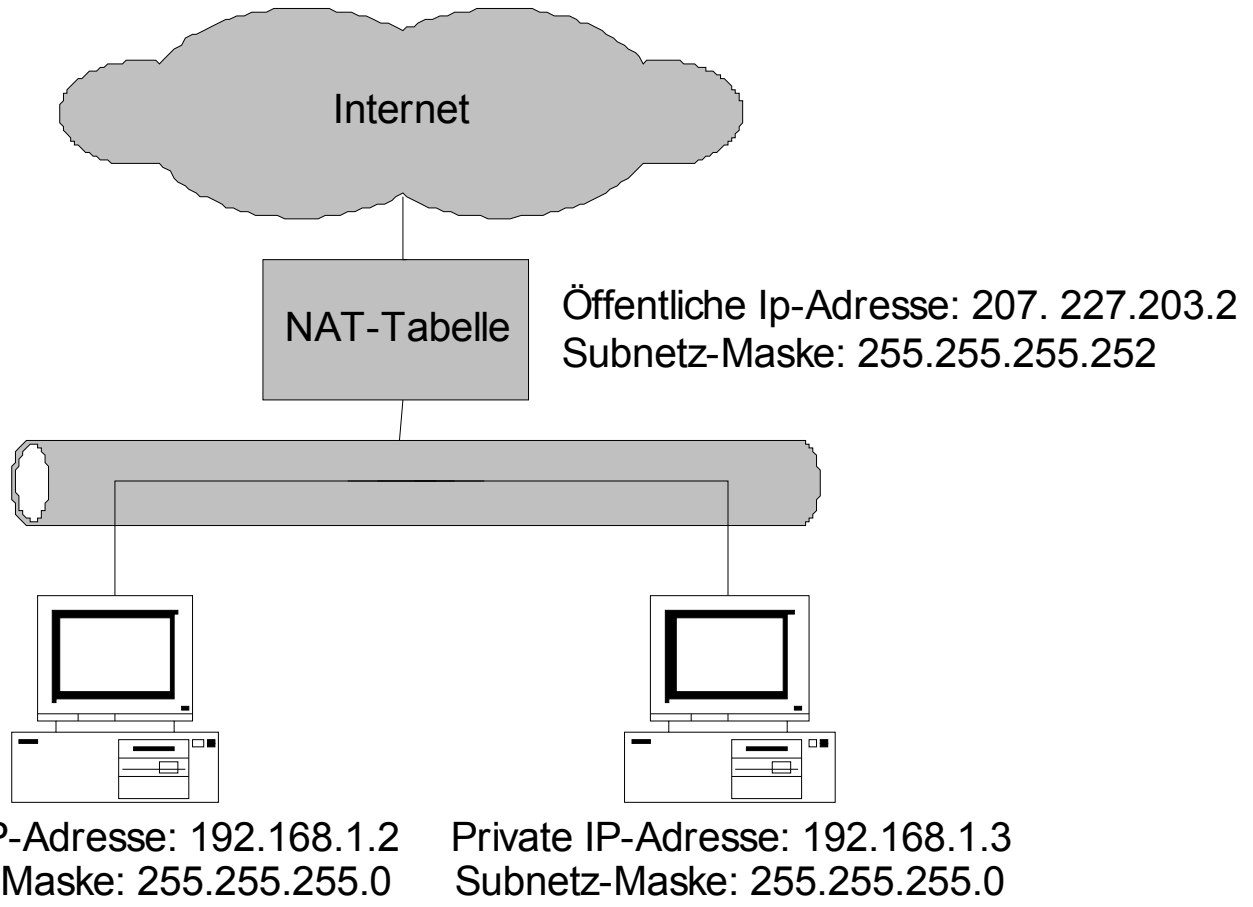
NAT – Network – Address Translation

- Veränderung von Netzwerkadressen
- Router verändert Pakete
 - nach außen: Quelladresse wird verändert
 - nach innen: Zieladresse wird verändert
- Häufigste Anwendung: Masquerading / Maskierung:
 - Problem: Durch IPv4-Adressknappheit wird von Providern oft nur eine einzige IP-Adresse zur Verfügung gestellt, obwohl mehrere Computer angebunden werden sollen
 - Lösung: Interne Rechner bekommen private, im Internet nicht verwendbare Adressen. Bei der Weiterleitung ins Internet ersetzt die Firewall die Quelladresse aller Pakete durch ihre eigene, Antwortpakete gehen daher direkt an die Firewall. Durch interne Zuordnungstabellen können die Antwortpakete an die richtigen internen Rechner weitergeleitet werden.

NAT (2)

- Vorteile
 - NAT unterstützt die Kontrolle der Firewall über nach außen gerichtete Verbindungen
 - eingehender Verkehr kann eingeschränkt werden
 - interne Konfiguration des Netzwerks wird verborgen
- Nachteile
 - ev. Problem mit eingebetteten IP-Adressen
 - Verschlüsselung und Authentifizierung erschwert
 - Protokollierung bei dynamischer Adresszuweisung
 - Dynamische Zuweisung von Ports stört Paketfilterung
 - Diverse Protokolle übertragen IP-Adressen der Clients auf Anwendungsebene (z.B. FTP, H.323) ⇒ spezielle Unterstützung muss in NAT eingebaut werden

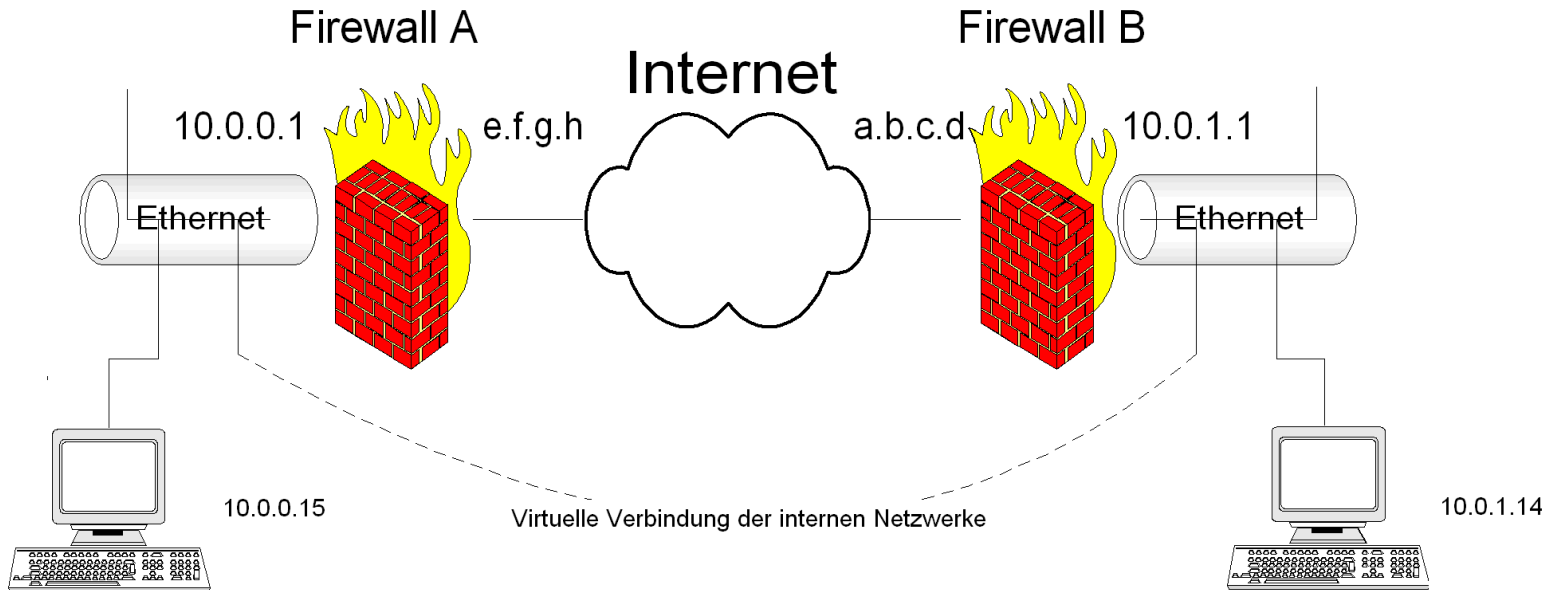
NAT - Beispiel



Virtuelle Private Netzwerke (VPN)

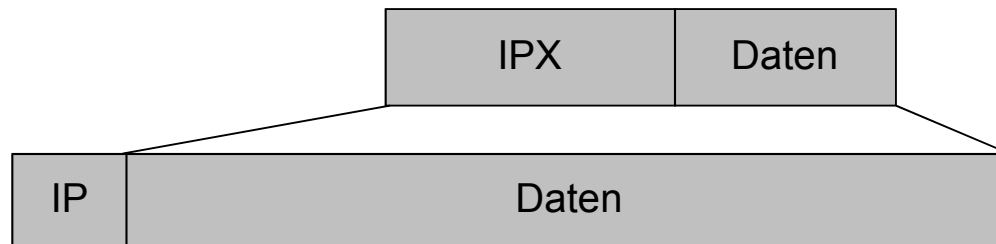
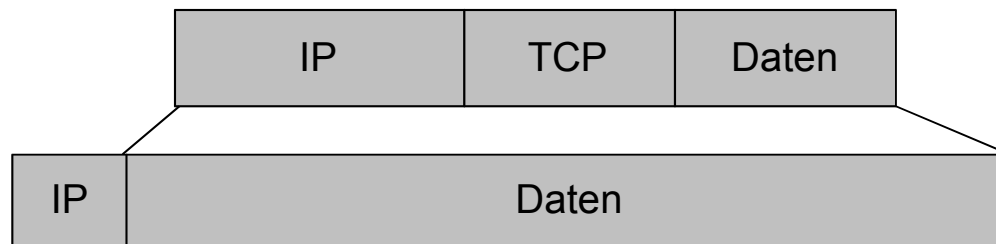
- öffentliches Netz wird privat genutzt
- Verschlüsselung
- Integrität wird geschützt
- Authentizität wird sichergestellt
- Daten werden gekapselt
- Methoden
 - End-zu-End Verschlüsselung
 - Tunnel
- Zeitpunkt der Ver- bzw. Entschlüsselung
 - Behandlung durch den Paketfilter

VPN - Prinzip



VPNs

- Meist im Tunnel-Modus betrieben: Rechner hinter den jeweiligen Gateways können transparent miteinander kommunizieren, obwohl die Gateways keine direkte Verbindung haben
- Methode: „Verpacken“ der Pakete, die zwischen den internen Rechnern ausgetauscht werden sollen in IPv4-Pakete

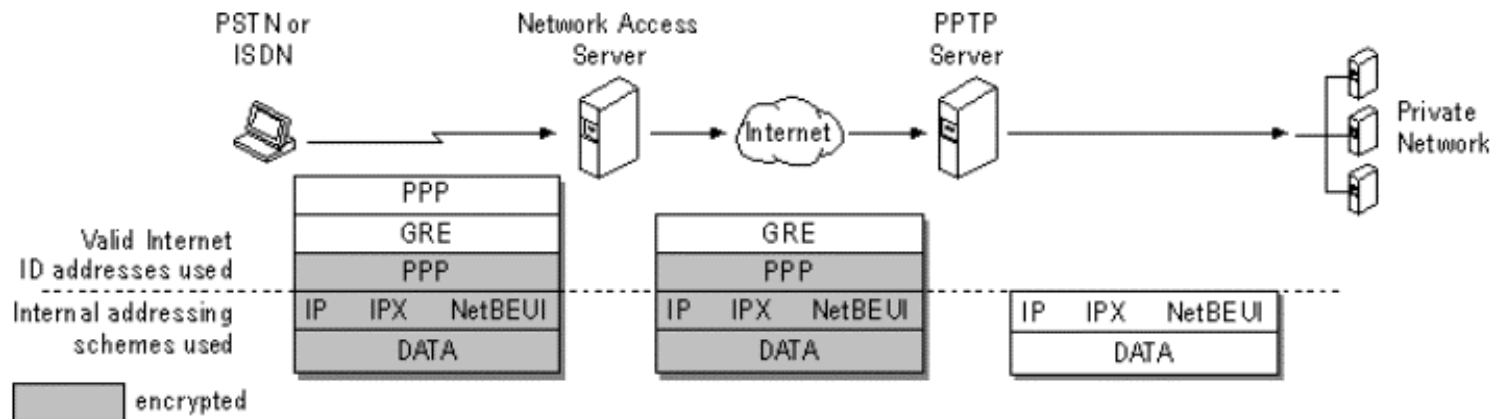


Tunneling

- Verschiedene Implementierungen von Tunneling (Beispiele):
 - GRE (unverschlüsselt)
 - IPv6-in-IPv4 (unverschlüsselt, Übergangsmaßnahme zu IPv6)
 - PPP-over-Ethernet
 - PPP-over-ATM
 - L2TP
 - PPTP
 - **IPSec**
 - OpenVPN
 - VTun
 - CIPE
 - Tinc
 -

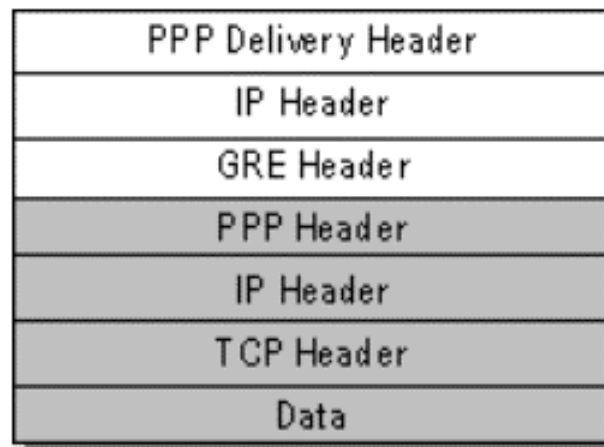
PPTP

- Von Microsoft entwickelt, zur IETF-Standardisierung eingereicht
- Kombiniert GRE-Tunneling mit PPP, um beliebige Protokolle (nicht nur IP) im Tunnel transportieren zu können
- Authentifizierung durch PPP (typisch Benutzername/Passwort)
- Optionale Verschlüsselung auf GRE-Paketebene



PPTP (2)

- Signifikanter Overhead wenn IP im Tunnel transportiert werden soll:
Beispiel PPP-Dialin mit PPTP-Tunnel



- UNSICHER !

IPSec

- IETF-Standard (International Engineering Task Force)
- Garantiert Interoperabilität zwischen Herstellern (zumindest theoretisch)
- Gilt in der Wissenschaft als sehr sicher, **keine bekannten Angriffe**
- Ursprünglich für IPv6 entwickelt, dann für IPv4 adaptiert
- Für IPv6 Implementierungen ist IPSec-Unterstützung „vorgeschrieben“
- Allerdings: komplex !

- IPSec
 - definiert in 12 verschiedenen RFCs
 - entwickelt 1998

IPSec

- IPSec besteht aus verschiedenen Protokollen
- Implementierung
 - Endhost
 - Router / Gateway
- Host Implementierung
 - End-to-End Security
 - Alle Modes von IPSec können implementiert werden
 - laufende Sicherheit gewährleistet
 - Userbezogene Authentifizierung
- Klassifizierung in
 - Integration im Betriebssystem – Host implementation
 - Schicht zwischen Netzwerk- und Datenschicht – „Bump in the Stack“

IPSec

- Integration im Betriebssystem
 - Teil der Netzwerkschicht
 - ähnlich ICMP
 - Vorteile
 - vollständige Integration in die Netzwerkschicht
 - Fragmentation, PMTU, Sockets
 - Alle Modes unterstützt
- Bump in the Stack (BITS)
 - Schicht zwischen Netzwerk- und Sicherungsschicht
 - großer Aufwand bei der Implementierung
 - Vorteile
 - Möglichkeit von vollständigen Lösungen
 - eigene Firewall-Clients (z.B. CheckPoint SecureClient)
 - abgestimmte Funktionalität

IPSec - Routerimplementierung

- Paket wird über einen Teil des Netzwerks gesichert
- Tunneling von Daten über das Internet
- Vorteile
 - Pakete können zwischen 2 privaten Netzwerken über ein öffentliches Netzwerk getunnelt werden.
 - Benutzerauthentifizierung für Client-to-network VPN
- 2 Typen der Router-Implementierung
 - Integration in die Router-Software
 - Bump in the Wire: analog zur BITS-Implementierung. Zusätzliches Gerät ohne Routingfunktionalität zur Sicherung
- mögliche Probleme
 - Effizienz
 - Kapazität
 - Schnelligkeit der Übermittlung

IPSec - Modes

- Protokolle: AH und ESP
- Modes: Tunnel und Transport-Mode
- Kombination aus Protokoll und Mode
- Transport-Mode:
 - AH und ESP schützen den Transport-Header. Pakete werden zwischen Netzwerkschicht und Transportschicht abgefangen
- Tunnel-Mode
 - wird verwendet, wenn Endziel des Pakets nicht dem Ende der gesicherten Verbindung entspricht
 - VPNs
 - IPSec kapselt IP Pakete mit IPSec Headern

IPSec - Modes

Transport Mode IPSec	Tunnel Mode IPSec
Applikation	Applikation
TCP, UDP oder anderes IP Protokol	TCP, UDP oder anderes IP Protokol
IPSec Security Layer	Innere IP Adresse (das wirkliche Ziel das Pakets nach dem IPSec Gateway)
IP Adresse	IP Security Layer
Data Layer	Äußere IP Adresse (IPSec gateway or firewall)
Physical Layer (Hardware)	Data Layer
	Physical Layer (Hardware)

IPSec

- Authentifizierung zwischen Hosts anstatt Benutzerauthentifizierung wie bei PPTP
- Authentifizierung über:
 - Preshared Keys (PSK)
 - X.509 Zertifikate
- X.509 Zertifikate bieten viele Vorteile:
 - Bessere Skalierbarkeit für viele Tunnel (bei N Teilnehmern nur N Zertifikate anstatt $N * (N-1)$ Keys)
 - Integration in PKI (z.B. CRL)
 - Sehr gute Unterstützung von „Road-Warriors“, da Zertifikate nicht auf Gateway installiert werden müssen, CA-Zertifikat genügt \Rightarrow Einrichtung neuer Zugänge ohne Umkonfiguration des IPSec-Gateways
- Aber: oft problematisch bei verschiedenen Implementierungen

IPSec - Kompatibilität

	PSK	RSA	X.509	NAT-Traversal	Manual keying
Gibraltar Firewall (FreeS/WAN)	Green	Green	Green	Green	Green
FreeS/WAN	Green	Green	Green	Green	Green
Open BSD	Green	White	Green	White	Green
Kame (FreeBSD, NetBSD, MacOSX)	Green	White	Green	White	Green
McAfee VPN was PGPnet	Green	Green	Green	White	White
Microsoft Windows 2000 / XP	Green	White	Green	White	White
CheckPoint FW	Green	White	Green	White	White
Cisco with 3DES	Green	Yellow	White	Yellow	White
F-Secure	Green	White	White	Yellow	Green
Gauntlet GVPN	Green	White	Green	White	White
IBM AIX	Green	White	Yellow	White	White
IBM AS/400	Green	White	White	White	White
SonicWall	Green	White	White	White	White
Symantec	Green	White	White	White	White
Watchguard Firwall	Green	White	White	White	Green

Vortragsinhalt

- Warum Firewalls ?
- Prinzipielle Firewalltechniken und Netzwerktopologien
- **Anti-Spam Techniken auf Mail-Gateway/Firewalls**
- Gibraltar
- Praxisbeispiel
- Tipps & Tricks, Details zu Linux mit read-only Root-Filesystemen

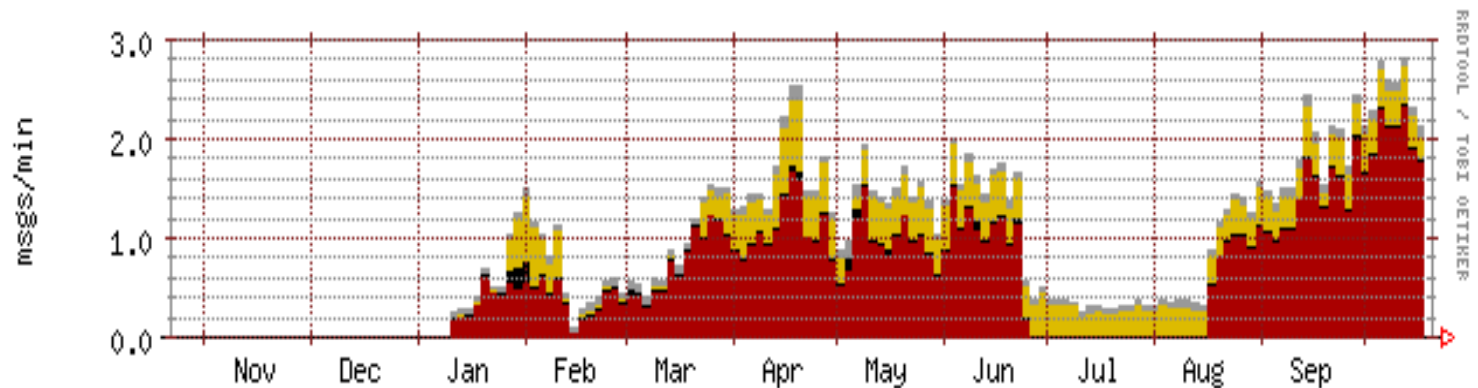
Anti-Spam Techniken



*Aktuelle Ansätze auf
verschiedenen Ebenen*

SPAM

- nicht nur unangenehm, sondern
 - verursacht Hardware-, Software- und Transfer-Kosten zur Übertragung und Speicherung von Emails sowie zum Zustellen von Bounces
 - verschwendet Arbeitszeit
 - bringt immer öfter Trojaner, Würmer oder Spyware mit
- Tendenz steigend ...



Wie wird SPAM erzeugt und versendet?

- Prinzipielle Möglichkeiten zum Versenden:
 - eigener Mailserver: wird schnell in Blacklists eingetragen, trotzdem häufig eingesetzt
 - fremder Mailserver: kann jederzeit deaktiviert werden, aber derzeit immer noch viele offene Relays auffindbar
 - Botnetz
- Inhalt der Mails:
 - Absender gefälscht, Fehlermeldungen können nicht zugestellt werden
 - oft bekannte Absendedomain verwendet
 - Empfänger nur in SMTP Envelope, aber nicht in Mail-Header (daher nicht durch Mailprogramm angezeigt)
 - prinzipiell alle Felder des Mail-Headers gefälscht
 - einzig zuverlässige Information: IP-Adresse des ausliefernden Rechners wird üblicherweise vom empfangenden Mailserver in der SMTP Envelope festgehalten
 - enthält oft „Web-Bugs“, die ein Anzeigen der Emails beim Spammer bekanntgeben
- Grundprinzip: **Masse**

Abwehrmaßnahmen (1)

- verschiedene Ebenen der Email-Zustellung werden von Spammern „attackiert“
- daher: Abwehr muss ebenfalls auf verschiedenen Ebenen erfolgen
- Ebene 1: SMTP Envelope (RFC 2821)
 - Blacklists/Whitelists auf IP/Domain Basis
 - RBL
 - korrekter Hostname (HELO:), Forward- und Reverse-DNS
 - Absende-Domains prüfen, “Rückruf” (MAIL FROM:)
 - nur Mails für eigene Empfänger akzeptieren (RCPT TO:)
 - **SPF/SenderID** (allgemein: MARID Gruppe, leider gescheitert)
Vorteil: einfach, sicher, funktioniert
Nachteil: kann durch „Wegwerfdomains“ umgangen werden
z.B.: aol.com, amazon.com, ebay.com, gmail.com, gmx.net, gibraltar.at
 - großer Vorteil: **sofortiges Zurückweisen noch während SMTP-Session möglich!**
 - Zusatztechnik: “Teergrube”
 - wichtig, damit mobile Benutzer weiterhin Emails versenden können:
SMTP Authentifizierung

Abwehrmaßnahmen (2)

- Ebene 2: Mail Header (RFC 2822)
 - Vergleich von “From:” mit “MAIL FROM:” aus SMTP Envelope
aber: Probleme mit Mailing-Listen etc.
 - Vergleich mit “To:” mit “RCPT TO:” aus SMTP Envelope
aber: wiederum Probleme mit Mailing-Listen etc.
 - **DomainKeys** (allgemein: Signatur Verfahren)
z.B.: yahoo.com, gmail.com
 - Zurückweisen u.U. auch noch während SMTP-Session möglich

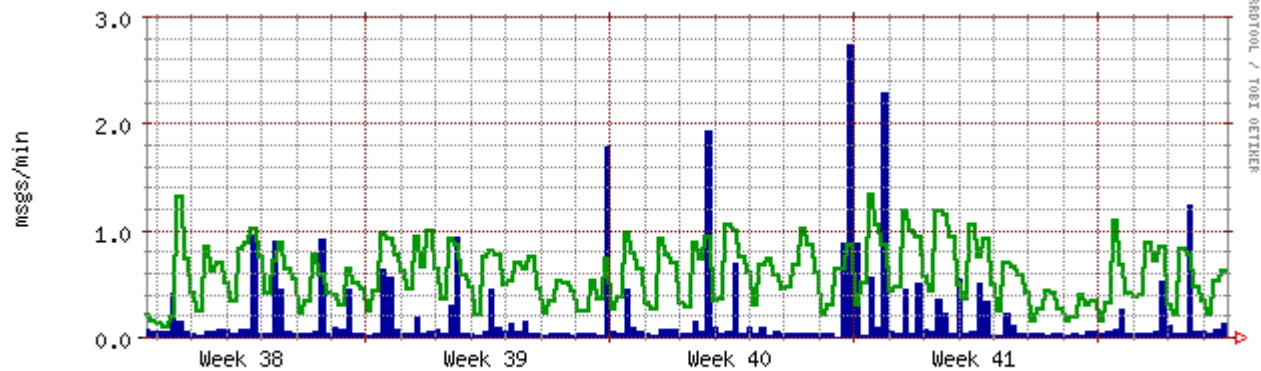
Abwehrmaßnahmen (2)

- Ebene 3: Inhalt
 - beste Lösung: starke kryptographische Signatur von Endbenutzer zu Endbenutzer (nicht von Server zu Server)
 - verbreitetste Standards: **OpenPGP** und **S/MIME**
 - nicht immer möglich, daher automatisierte Prüfungen:
 - Attachments (EXE, PIF, JPG, etc.)
 - Viren
 - Web-Bugs
 - Javascript
 - ...
 - Analyse des Mail-Inhalts nach Kriterien (schließt auch Felder von Ebenen 1 und 2 mit ein)
 - verteilte Erfassung von Email-Häufigkeiten basierend auf dem Inhalt: **Razor** und **DCC**
 - statistische Analyse des Mail-Inhalts: Bayes Klassifikation

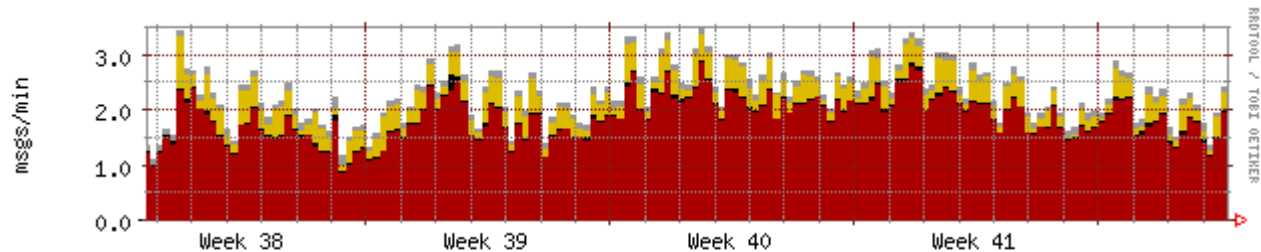
Kombination der meisten Abwehrmaßnahmen

- Maßnahmen aus Ebenen 1 – 3
 1. allgemeine Konformitätsprüfungen, RBL, SPF, “Rückruf”, Teergrube, SMTP Authentifizierung
 2. Prüfung von Mail Headern über Kriterien
 3. Attachments, Bewertung über Kriterien, Razor, DCC, Bayes
- Großteil bereits während SMTP-Session zurückgewiesen, Rest danach

In Kombination erfolgreich



■ Sent	total:	7762 msgs	avg:	0.20 msgs/min	max:	243 msgs/min	
■ Received	total:	23120 msgs	avg:	0.58 msgs/min	max:	82 msgs/min	[Thu Oct 21 16:29:22 2004]



■ Rejected	total:	74389 msgs	avg:	1.87 msgs/min	max:	43 msgs/min	
■ Bounced	total:	1588 msgs	avg:	0.04 msgs/min	max:	33 msgs/min	
■ Viruses	total:	12632 msgs	avg:	0.32 msgs/min	max:	9 msgs/min	
■ Spam	total:	2932 msgs	avg:	0.07 msgs/min	max:	6 msgs/min	[Thu Oct 21 16:29:23 2004]

Vortragsinhalt

- Warum Firewalls ?
- Prinzipielle Firewalltechniken und Netzwerktopologien
- Anti-Spam Techniken auf Mail-Gateway/Firewalls
- Gibraltar
- Praxisbeispiel
- Tipps & Tricks, Details zu Linux mit read-only Root-Filesystemen

Gibraltar Firewall



*Geschichte, Prinzip, Vor-/
Nachteile*

eSYS Informationssysteme GmbH

- Gegründet 2002
- Gesellschafter:
 - Thomas Mayrhofer, Mag. Reinhard Mayrhofer, DI Richard Leitner, Mag. Andreas Wöckl
- Derzeit 5 Mitarbeiter
- Schwerpunkte
 - Entwicklung von Individualsoftware
 - Netzwerk – Sicherheit
 - Entwicklung von Gibraltar
 - IT – Consulting
 - Netzwerkbetreuung

Gibraltar - Entstehung

- Projektbeginn Juli 2000 von Rene Mayrhofer
- 2000 – 2002: permanente Weiterentwicklung, gestützt auf Verbesserungsvorschläge aus der wachsenden Community
- 2002: erste Ideen zu einer kommerziellen Version
- 2/2003: Partnerschaft von Rene Mayrhofer mit der eSYS Informationssysteme GmbH. Start der kommerziellen Entwicklung
- 11/2003: Präsentation der Version 1.0. Erste Version mit Webinterface
- 5/2004: Gibraltar v2
- 11/2004: Gibraltar v2.1

Gibraltar – Zahlen und Fakten

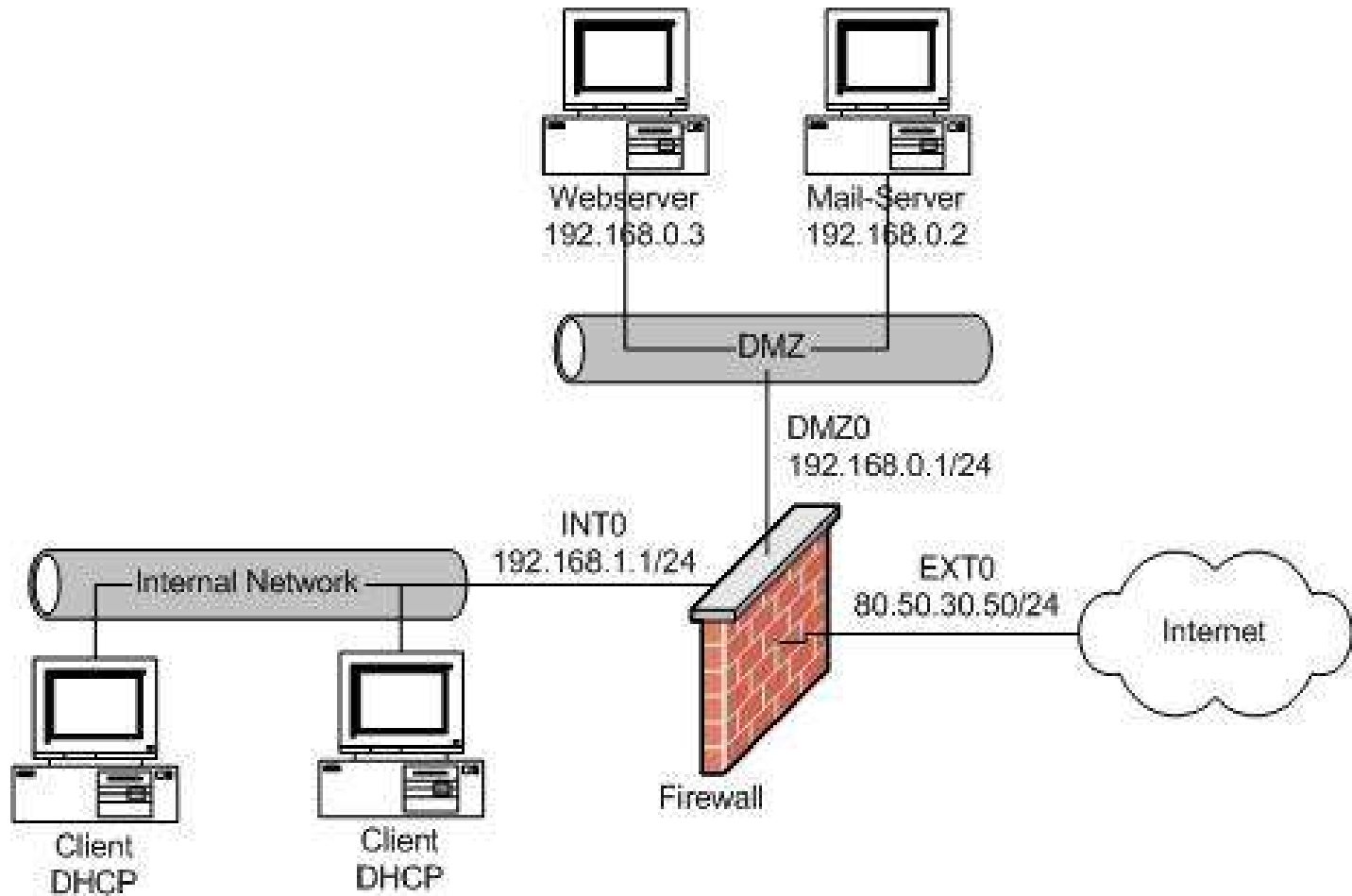
- geschätzte Installationen der freien Version: über 1000
- kommerzielle Installationen (eigene Kunden): ca. 50
- Testinstallationen (Testlizenzen) seit 11/2003: > 2000
- tägliche Anzahl von Zugriffen auf Homepage: 600-1000
- Mailingliste: knapp 500 Mitglieder

- seit 11/2004: ca. 20 Vertriebs- und Supportpartner in
 - Österreich
 - Deutschland
 - Schweiz
 - Italien
 - USA
 - Finnland
 - Griechenland

Professionelle All-in-One Security Lösung

- Router
- Stateful Inspection Firewall
- Deep Inspection Firewall
- Professioneller Viren Schutz
- Erweiterter Spam Schutz
- Secure Proxy Server
- Inhaltsfilter
- URL-Filter
- Virtuelle Private Netzwerke

Firewall - Schema



Grundprinzipien

- basierend auf Debian GNU/Linux 3.0 (**woody++**)
- bootet und läuft vollständig von CD-ROM
- minimale Hardwareanforderungen
- vollständig mittels Webinterface konfigurierbar
- sicher durch Verwendung von gängigen Open-Source-Komponenten und Live CD Technology
- Extras
 - Virtuelle Private Netzwerke
 - Kaspersky Antivirus Engine
 - State-of-the-art Spamschutz

7 gute Gründe für Gibraltar

- Open-Source-Entwicklung
- Komfortabel durch Webinterface
- Sicher und einfach zu handhaben durch Live-CD-Technology
- Flexible Sicherheit durch Virtuelle Private Netzwerke
- Hervorragend in Preis und Leistung
- Überall einsetzbar durch Lauffähigkeit auf jeder Hardware
- Dual Safety durch Virenschutz und Spamschutz

Das Webinterface

Gibraltar-WebInterface - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

GIBALTAR FIREWALL

Gibraltar GIBADMIN 2.0-test2 [Upload license](#) | [Support](#) | [Update](#) | [Help](#) | [Logout](#) English

Home
System
Services
Network
Dial-in
Firewall
NAT
Mail
IPSec
PPTP
DHCP server
SSL
HTTP proxy
FTP proxy
POP3 proxy
Configuration management

Firewall rules ?

Firewall rules

Interface: incoming: outgoing:

State: Allow established Allow related

Move: From index: To index:

Firewall rules:

	Active	Source address	Dest. address	Protocol	Source port	Dest. port	Action	
1.	<input checked="" type="checkbox"/>			TCP			flood-protect	<input type="checkbox"/> <input type="button" value="i"/> <input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/> <input type="button" value="del"/>
2.	<input checked="" type="checkbox"/>			TCP			flood-protect	<input type="checkbox"/> <input type="button" value="i"/> <input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/> <input type="button" value="del"/>
3.	<input checked="" type="checkbox"/>			ICMP			flood-protect	<input type="checkbox"/> <input type="button" value="i"/> <input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/> <input type="button" value="del"/>
4.	<input checked="" type="checkbox"/>						LOG	<input type="checkbox"/> <input type="button" value="i"/> <input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/> <input type="button" value="del"/>
5.	<input checked="" type="checkbox"/>						DROP	<input type="checkbox"/> <input type="button" value="i"/> <input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/> <input type="button" value="del"/>

Gibraltar 2.0-test2, 2004 by eSYS Informationssysteme GmbH

System

- Live CD Technology: bootet und läuft vollständig von CD ROM
- Keine Festplatteninstallation notwendig
- Speziell gehärteter Linux Kernel
- Sprachen: Deutsch, Englisch, *Finnisch*
- Fernkonfiguration mittels Webinterface oder remote login
- Einfaches Konfigurationsmanagement
- Automatische Live Updates
- Minimale Hardwareanforderungen

Netzwerkunterstützung

- Ethernet 10/100/1000 MBit/s: statisch oder DHCP, virtuelle IP Adressen
- ADSL Ethernet Modems: PPP over Ethernet, PPTP
- ADSL USB Modems: PPP over ATM
- Modem Dial In: Seriell, USB
- Unbegrenzte Anzahl von Netzwerkschnittstellen

Stateful Packet Inspection

- Protokollunterstützung: ICMP, TCP, UDP, GRE, ESP, AH, IPv4-over-IPv6
- Flexibler Paketfilter: Schnittstelle, MAC-Adresse, IP-Adresse, Service, Port,...
- NAT: Network Address Translation
- PAT: Port Address Translation
- Freie Definition von Aliases und Gruppen: Adressen und Ports
- DoS/Flood-Protection: vordefiniert, erweiterbar
- Randomized IP Sequencing
- Gezielte TTL Manipulation
- Protokoll Pass Through: PPTP, FTP, H.323, IRC

VPN (Virtuelle Private Netzwerke)

- IPsec Gateway
- PPTP Server: MPPE 128 Bit Encryption
- Network-to-Network VPN (IPsec)
- Network-to-Client VPN: Kompatibel mit MS Windows 2000/XP (IPsec, PPTP)
- Unbeschränkte Anzahl von VPN Tunnels
- Authentifizierung mit PSK (Private Shared Key) und X.509 Zertifikaten
- Verschlüsselung: 3DES, Blowfish, Serpent, Twofish, CAST, AES
- Authentifizierung PPTP: CHAP, MS-CHAPv1, MS-CHAPv2
- NAT traversal
- Perfect Forward Secrecy (PFS)

Deep Inspection Firewall

- Secure SMTP Relay: eingehend, ausgehend, Attachment Blocking, Block Lists, Viren- und Spamschutz **postfix (+TLS+IPv6+SASL++)**
- Transparenter HTTP Proxy: keine Clientkonfiguration notwendig, Spamschutz **squid (+erweiterte Filter-Patches)**
- User Authentifizierung: Benutzerliste, Active Directory Integration, LDAP
- Content Caching
- Content Scanning: Antivirus, Cookies, JavaScript, Active X
- URL Filter
- FTP Proxy: transparent ausgehend, eingehend **SuSE ftp-proxy**
- Transparenter POP3 Proxy: Antivirus, Spamschutz, und Schutz vor gefährlichen Attachments **p3scan**

Zusatzdienste

- DHCP Server `dhcpcd 3`
- Secure DNS Resolve `djbdns`
- SSL Wrapper für beliebige TCP Dienste `sslwrap`
- Portscan Detection `psad`
- Anti Spam Filter: `spamassassin` über `amavisd-new`
regelbasiert, Bayes, RBL, Razor und DCC, SPF
- ClamAV Virens scanner
- Kaspersky Virens scanner

Vorteil gegenüber Hardware-Lösungen (Watchguard, Sonicwall, Cisco, Zyxel,...)

- Preis
- Skalierbarkeit
- Flexibilität
- Erweiterbarkeit
- Sicherheit durch Open Source
- Sicherheit durch Live-CD-Technology

Vorteile gegenüber Softwarepaketen (Astaro, Checkpoint, Smoothwall,...)

- Preis
- Einfache Installation
- Sicherheit durch Live-CD-Technology
- Keine Festplatte notwendig
- Höhere Ausfallsicherheit

Facts

- Gibraltar ist nicht dauerhaft angreifbar: durch physisch schreibgeschütztes System ist es nicht möglich, sogenannten „malicious code“ dauerhaft zu plazieren
- Gibraltar ist ausgereift: seit dem Jahr 2000 wird Gibraltar weltweit von Linux-Experten verwendet, getestet und weiterentwickelt. Gibraltar verwendet tausendfach getestete Komponenten, deren Quellcode frei verfügbar ist.
- Gibraltar reduziert das Spam-Aufkommen um ca. 95%: durch die Kombination mehrerer Anti-Spam-Maßnahmen (RBL-Listen, Inhaltsanalyse, Bayes-Filter, Razor, DCC, SPF, ...) kann Gibraltar wirksam Spam-Mails erkennen und darauf reagieren.
- Gibraltar ist skalierbar und flexibel: je nach Anforderung kann geeignete Hardware verwendet und auch erweitert werden. Gibraltar unterstützt Load-Balancing und Fail-Over.

Gibraltar – Referenzen

- Universität Washington
- Universität Linz
- Fachhochschule Kufstein
- Technikum Wien
- Doubrava
- COPYright by Josef Schürz
- Kirsch – Muchitsch und Partner
- Finadvice Financial Adivsory GmbH
- Ebnerbau Mondsee
- Prävital
- HGS Unternehmensberatung
- Profactor Steyr
- Datacontact
- CARE Österreich
- ...

Preise und Varianten

	Small Business	Medium	Professional	Enterprise
Anzahl der User	- 10	- 25	- 50	- 100
IpSec Tunnel	1	5	20	open
VPN Clients	1	5	20	Open
Preis	€ 350	€ 690	€ 990	€ 1.790
Update Service/Jahr	€ 80	€ 150	€ 240	€ 370

- Optionale Zusatzdienste
 - Kaspersky Anti-Virus-Engine
 - Betreuung / Wartung

Vortragsinhalt

- Warum Firewalls ?
- Prinzipielle Firewalltechniken und Netzwerktopologien
- Anti-Spam Techniken auf Mail-Gateway/Firewalls
- Gibraltar
- **Praxisbeispiel**
- Tipps & Tricks, Details zu Linux mit read-only Root-Filesystemen

Gibraltar Firewall Praxisbeispiel



*Einrichtung Netzwerk,
Firewall-Regeln, Mail Relay,
VPN*

Vortragsinhalt

- Warum Firewalls ?
- Prinzipielle Firewalltechniken und Netzwerktopologien
- Anti-Spam Techniken auf Mail-Gateway/Firewalls
- Gibraltar
- Praxisbeispiel
- **Tipps & Tricks, Details zu Linux mit read-only Root-Filesystemen**

Tipps & Tricks



Debugging von Firewall-Regeln, Arbeit an Remote Systemen, zentrales Logging, Umgang mit Konfigurationsrevisionen

Debugging von Firewall-Regeln

- Fehlermeldungen im Syslog ?
- Log-Regeln einfügen
- Tcpdump
- „man iptables“ ;-)

Arbeiten mit Remote-Systemen

- Problem: fehlerhafte Firewall-Regeln bzw. Netzwerkkonfiguration verhindern ein Rückgängigmachen
„Aussperren“
- Regel 1: Nachdenken, dann Kommandos ausführen
80%
- Regel 2: Mindestens eine andere Shell offen halten
10%
- Regel 3: Möglichkeit zum lokalen Zugang
5%
- Regel 4: automatisches Speichern der Konfiguration deaktivieren,
„shutdown -r +15“
„shutdown -c“
5%

Zentrales Logging

Vorteile:

- Firewalls benötigen keine lokale Festplatte
- Erhöhte Sicherheit wenn Loghost sicher

Einrichten:

- Zentraler Loghost muss syslog-Dienst anbieten (UDP, Port 514)
„syslogd -r“
(in Debian z.B. in `/etc/init.d/sysklogd: SYSLOGD="-r"`)
auch für Windows NT/2000/XP existiert syslog-Service
- Achtung: Zugriff auf syslog-Service mit Paketfilter beschränken, sonst Risiko einer DoS-Attacke
- Auf jeder Firewall: in `/etc/syslog.conf` statt

```
*.notice;mail.*           -/var/log/syslog
*.=debug;*.=info;mail.none -/var/log/debug
```

weiterleiten auf Loghost:

```
*.notice;mail.*           @loghost.domain.tld
*.=debug;*.=info;mail.none @loghost.domain.tld
```

Umgang mit Konfigurationsrevisionen

- Gesamte Konfiguration in einer Datei abgelegt: `etc.tgz`
- Keine speziellen Berechtigungen, Datei kann mit jedem System einfach kopiert werden
- `save-config` bietet viele Ziele, inklusive Floppy, USB, Email und `scp`
- Sichern über `scp` hilft, Konfigurationsrevisionen zu verwalten
- Auch mehrere Floppy-Disketten oder USB-Medien können verwendet werden
- Einfaches Umbenennen von `etc.tgz` auf Sicherungsmedium verhindert Überschreiben

Gibraltar Internas



*Umgang mit read-only Root-
Filesystemen, Boot-Prozess*

Prinzip mit read-only Root-Filesystem

- Großteil kann read-only sein => ISO9660 ideal geeignet (mit Rockridge Erweiterungen)
- beschreibbar:
 - `/etc` (müsste nicht vollständig beschreibbar sein),
 - `/var`,
 - `/tmp`
- Lösung früher über RAM-Disks, Problem: Größe muss über Kernel-Parameter festgelegt werden
- mit aktuellem Kernel: **tmpfs**
- **zur Speicherersparnis im RAM: symlinks auf statische Inhalte unterhalb `/etc` und `/var`**

Gibraltar Boot-Prozess

- syslinux/isolinux auf Gibraltar Boot-Medien (CD-ROM, USB), entweder direkt in ISO9660 Bootblock oder in VFAT Bootsektor
- auch andere Bootloader möglich (grub, lilo, ...)
- Kernel und initial Ramdisk (initrd) geladen, über Kernelparameter wird als erster Prozess `/linuxrc` von initrd geladen
- `linuxrc` als Shellsript realisiert
- Kommandos in initrd über busybox
- initrd inkludiert alle Kernelmodule, die zum Mounten des Bootmediums gebraucht werden könnten
- linuxrc macht Hardwareerkennung (SCSI), lädt nötige Module und durchsucht angeschlossene Hardware (verschiedene CD-ROM Laufwerke, USB-Bus) nach Bootmedium
- wenn Bootmedium gefunden (über `id.txt` Datei), Umschalten auf wirkliches Root-Filesystem mittels neuem `pivot_root` Mechanismus
- normaler Bootprozess startet (`init` wird über `exec` als Prozess 1 gestartet)

Unterstützung des Bootprozesses

- Paket `mkinitrd-cd` seit 2000, aktuelle Version immer in Debian unstable
- wird auch von anderen Projekten verwendet, bietet allgemeines Booten von CD-ROM und USB Massenspeicher
- Paket `gibraltar-bootsupport` für Umgang mit read-only Filesystem, ebenfalls in Debian unstable

Die Zukunft

Release 2.0

- Integration von Squid mit MS Active Directory
- Postfix 2.1 mit SPF (Policy Filter), Absenderüberprüfung und Pre-Queue-Prüfungen

Release 2.1 (Content/Deep Packet Inspection):

- Verbesserungen am Webinterface, Vereinfachungen, „weniger Klicks“
- Integration von PPTP mit MS Active Directory
- SMTP AUTH über TLS (SMTP-Server von außen für Roadwarrior) mit Integration in MS Active Directory
- Bugfixes ...

Release 2.2 (Availability):

- Hot-Standby System mit automatischer Synchronisierung der Konfiguration
- Password-Expiry für HTTP-Benutzer
- Ändern von Passwörter durch Benutzer selbst (SMTP, PPTP, HTTP)

Die Zukunft (2)

Releases 3.X (IP/Netzwerkebene):

- Kernel 2.6
- Logging, Monitoring, Auswertung, Statistiken, Graphen, ...
- „1-Klick IPSec über WLAN“
- Browser-Authentifizierung für WLAN-Surfen (z.B. NoCat Auth oder das neuere Chillispot)
- Visualisierung / bessere Regeldarstellung im Firewall-Modul
- Traffic Shaping / Quality of Service
- Volume Quotas
- Voller IPv6-Support für alle Dienste, IPv6-in-IPv4 Tunnel, IPv6 Firewall-Regeln, ...
- ...