

Workshop – „Netzwerksicherheit“

24.10. 2003

Technologiezentrum Salzkammergut
Attnang-Puchheim

- 9.00 Uhr: Begrüßung
Mag. Veronika Deisenhammer, TZA
Thomas Mayrhofer, eSYS
- 9.15 Uhr: Netzwerksicherheit, Bedrohungen – ein Überblick
Thomas Mayrhofer, eSYS
- 10.15 Uhr: Kaffeepause
- 10.30 Uhr: Sicherheitsplanung und –management
Thomas Mayrhofer, eSYS
- 11.30 Uhr: Einführung in Firewalltechnologien
Dipl.-Ing. Rene Mayrhofer, Universität Linz
- 12.30 Uhr: Mittagspause
- 13.30 – 18.00 Uhr (EDV-RAUM)
Firewall – Konfiguration und Schwachstellenanalyse
Thomas Mayrhofer, Dipl.-Ing. Richard Leitner, eSYS



- Gegründet 2002
- Schwerpunkte
 - Netzwerksicherheit
 - Netzwerkplanung und –betreuung
 - Individualsoftwareentwicklung
 - IT-Consulting
 - Firewall – Gibraltar
- Referenzen
 - Lenzing AG
 - Bildungszentrum Lenzing
 - COPYright by Josef Schürz
 - Kirsch – Muchitsch & Partner
 - Ebnerbau Mondsee
 - ...



- Thomas Mayrhofer, Geschäftsführer
 - Selbstständig seit 1997
 - Studium der Wirtschaftsinformatik, Schwerpunkt Wissensmanagement
 - Microsoft Certified Professional
 - 2 Jahre IT-Betreuung Lenzing AG
 - 6 Jahre EDV-Trainer für BZL, RACON, VOEST, ...
 - Zahlreiche Software-Projekte
- Dipl.-Ing. Richard Leitner, Prokurist
 - Selbstständig seit 2001
 - Studium der Informatik, Schwerpunkt Netzwerksicherheit
 - IT-Betreuung Fa. Rosenbauer International
 - Zahlreiche Software-Projekte
- Mag. Andreas Wöckl, Prokurist
 - Selbstständig seit 2000
 - Studium der Wirtschaftsinformatik, Schwerpunkt Software-Engineering
 - Microsoft Certified Professional
 - Zahlreiche Software-Projekte



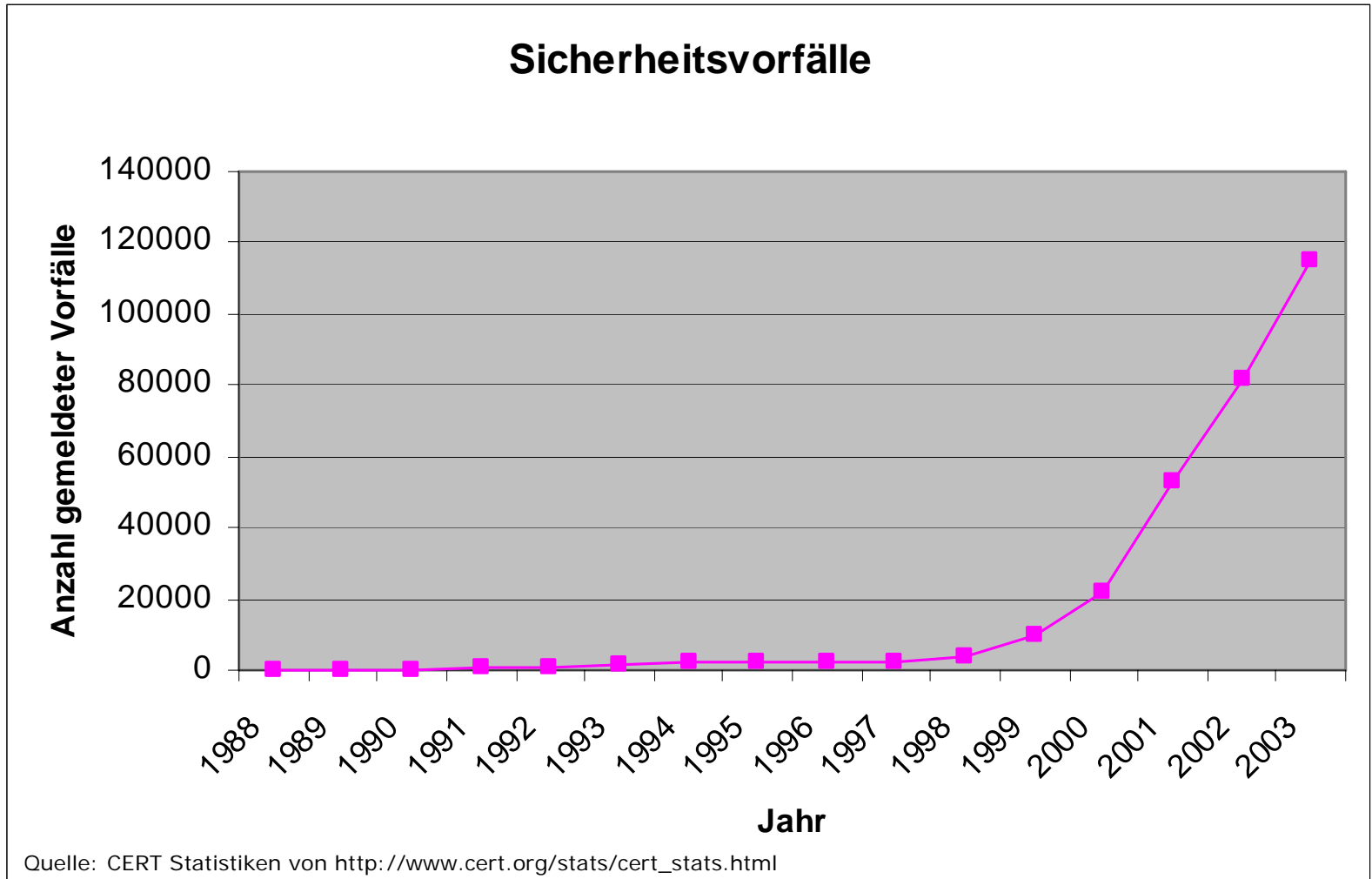
- Dipl.-Ing. Rene Mayrhofer, Network Security Specialist
 - Studium der Informatik
 - Derzeit Assistent am Institut für Praktische Informatik der Johannes Kepler Universität Linz, Dissertationsthema: Context Awareness
 - Seit März 1999: Entwicklung Gibraltar-Firewall
 - Seit 1998: Beschäftigung mit IPv6, Programmierung diverser Netzwerkttools für IPv6
 - Offizieller Entwickler von Debian/GNU Linux: IPSec- und PPTP-Unterstützung in Debian, Logfile-Überprüfung



Netzwerksicherheit – Bedrohungen – ein Überblick

Von Viren, Würmern, Trojanern und Hackern

Thomas Mayrhofer, eSYS Informationssysteme GmbH



- 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

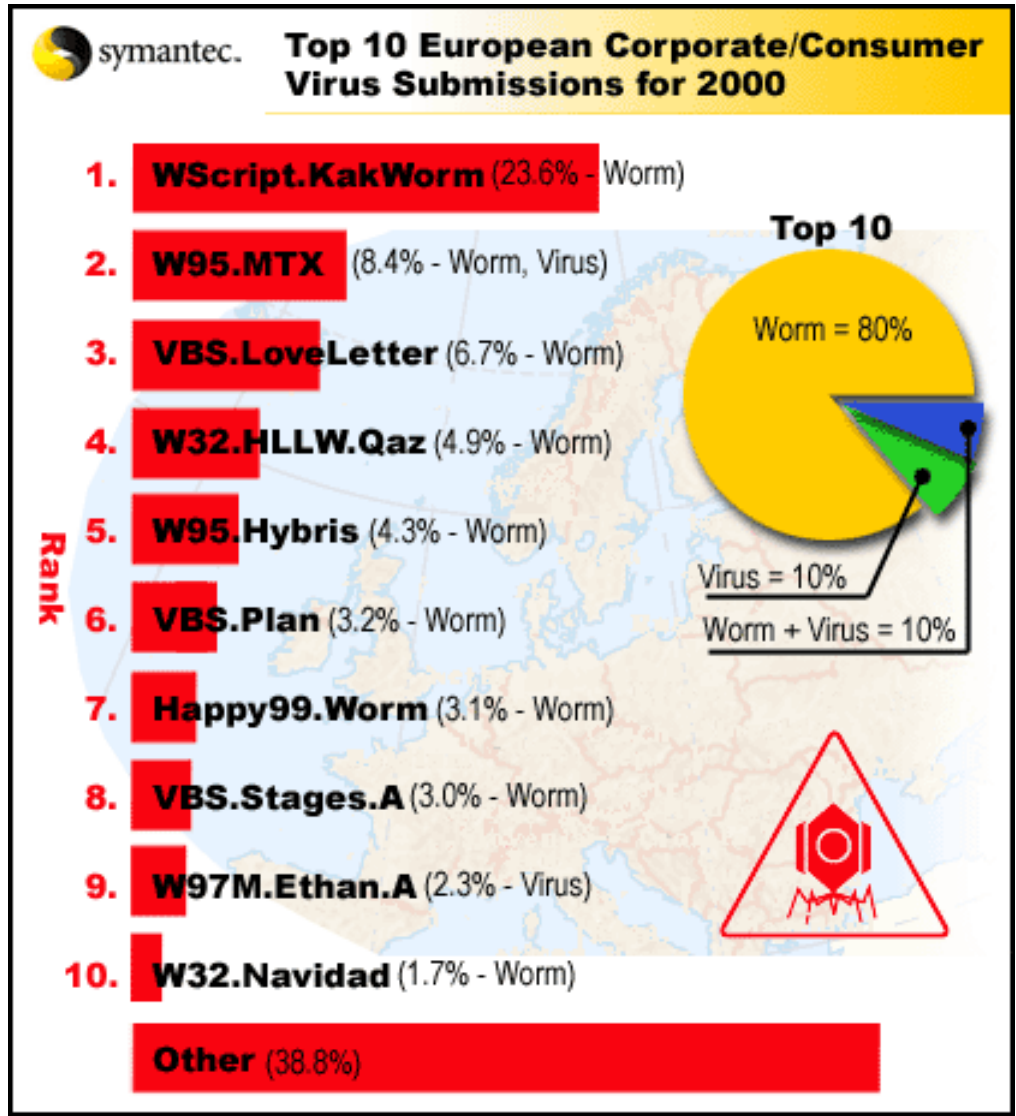


- Schadensprogramm, dass sich von Datei zu Datei auf einem Computer ausbreitet
- Virus repliziert sich selbst
- Virus muss aktiviert werden
- Strategie: den Wirt beherrschen
 - So viele Dateien wie möglich infizieren
 - Funktionen blockieren
 - Übertragung durch Diskette, E-Mail ...
 - Langsame Infektion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



- 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





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



- 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



- „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

Source: Symantec Corporation



- 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



- 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



- 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!!



- Bedrohung durch Hacker im Vergleich zu Viren, Würmer und Trojaner eher gering
- Problem: werden meistens nicht bemerkt
- Nur ein geringer Prozentsatz verursacht Schäden
- Motivation: Herausforderung, Thrill
- Spezialwissen öffentliche 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



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



Sicherheitsplanung und - management

4 Säulen der Netzwerksicherheit
Sicherheitsmanagement
Maßnahmen

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 anormalen 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.



- Aufgabe
 - Erreichung der strategischen Sicherheitsziele
 - Abwenden von realen Schäden an der Informationsinfrastruktur und damit wirtschaftlichem Schaden
 - Vermeiden und Vermindern von Schäden durch Sicherungsmaßnahmen, Überwälzen von Schäden sowie Selbsttragen von Schäden (Restrisiko)
- Erfüllung der Aufgabe
 - Erkennen von Bedrohungen (Bedrohungsanalyse) und von potenziellen Schäden aus den Bedrohungen (Schwachstellenanalyse)
 - Planung und Realisierung von Sicherungsmaßnahmen
 - Risikopotenzial und Schutzpotenzial sollen so aufeinander abgestimmt sein, dass weder ein unkalkulierbares Risiko verbleibt, noch sinnlose Sicherungsmaßnahmen implementiert werden



- Bedrohungen
 - Unzuverlässigkeit der Informationsinfrastruktur
 - deliktische Handlungen
 - Umgebungseinflüsse

 - Verletzung der Integrität
 - Verletzung der Verbindlichkeit
 - Verletzung der Verfügbarkeit
 - Verletzung der Vertraulichkeit
- Risikoklassen
 - A: hohe Eintrittswahrscheinlichkeit, große Schadenshöhe
 - B: niedrige Eintrittswahrscheinlichkeit, große Schadenshöhe
 - C: hohe Eintrittswahrscheinlichkeit, geringe Schadenshöhe
 - D: niedrige Eintrittswahrscheinlichkeit, geringe Schadenshöhe



- Maßnahmen
 - Sicherungsmaßnahmen zum Schutz von Objekten wie Gebäude und Räume
 - Sicherungsmaßnahmen zum Schutz von Hardware wie Netze und PCs
 - Sicherungsmaßnahmen zum Schutz vor Software, insbesondere Anwendungsprogrammen
 - Sicherungsmaßnahmen zum Schutz von Daten (Datenschutz)
- Maßnahmenkategorien
 - Vermeidung eines realen Schadens
 - Verminderung eines realen Schadens
 - Begrenzung des Risikos
 - Begrenzung des wirtschaftlichen Schadens
 - Finanzielle Vorsorge für den Schadensfall



- Beispiel „Netzwerksicherheit“
- Bedrohungen
 - Viren, Würmer, Trojaner, Hacker, interne Angriffe
- Gefährdungen
 - Daten: Löschen, unberechtigte Weitergabe, Veränderung, Beschädigung (Hacker, Trojaner)
 - Software: unberechtigte Benutzung, Veränderung und Beschädigung (Viren, Würmer, Hacker)
 - Hardware: unberechtigte Benutzung (Viren, Würmer, Trojaner, Hacker)
- Maßnahmen
 - unternehmensweite Sicherheitsstrategie
 - Zugriffsrechte
 - Virenschutz
 - Firewall – Policy
 - Intrusion Detection
 - Vulnerability - Scanning

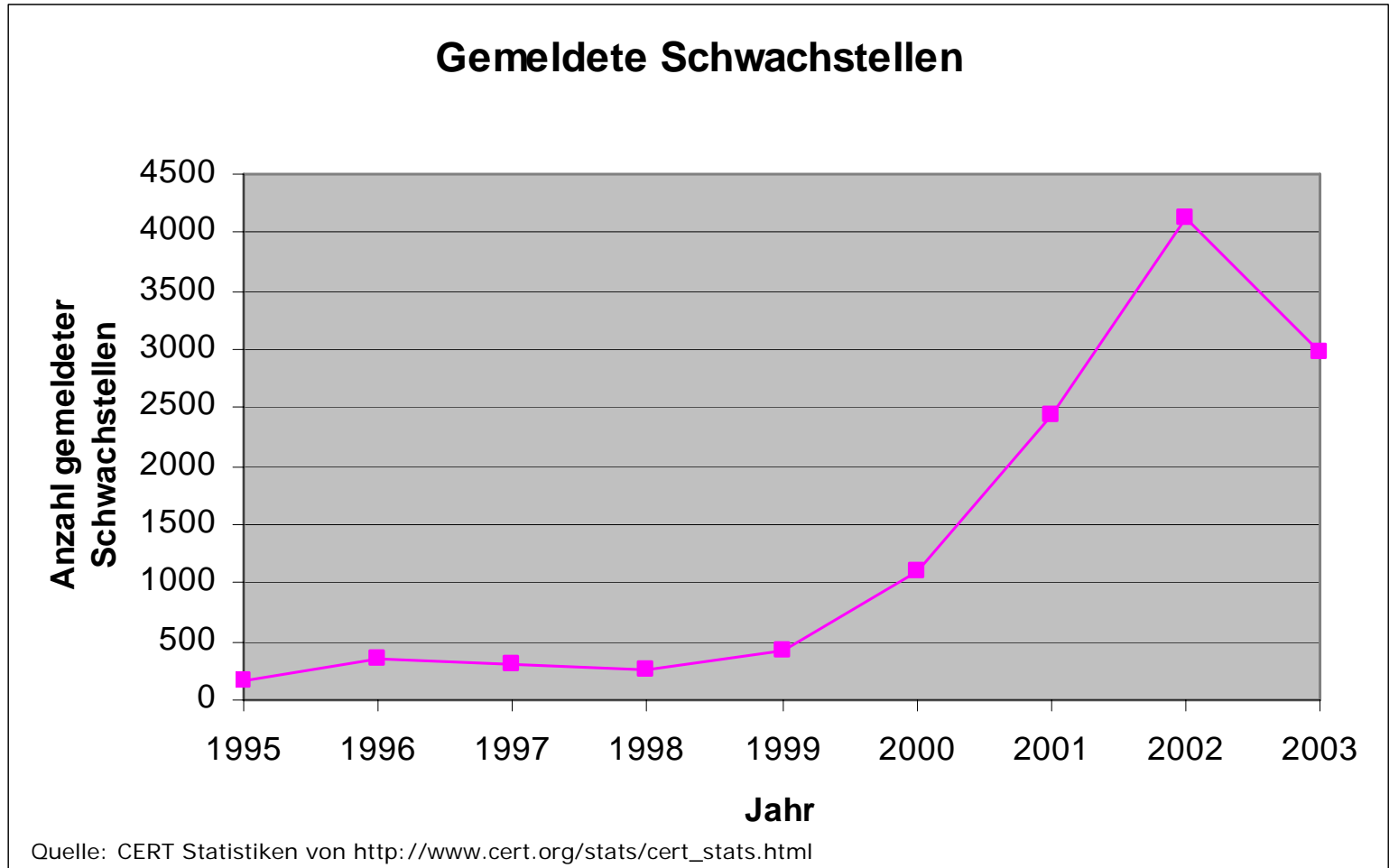


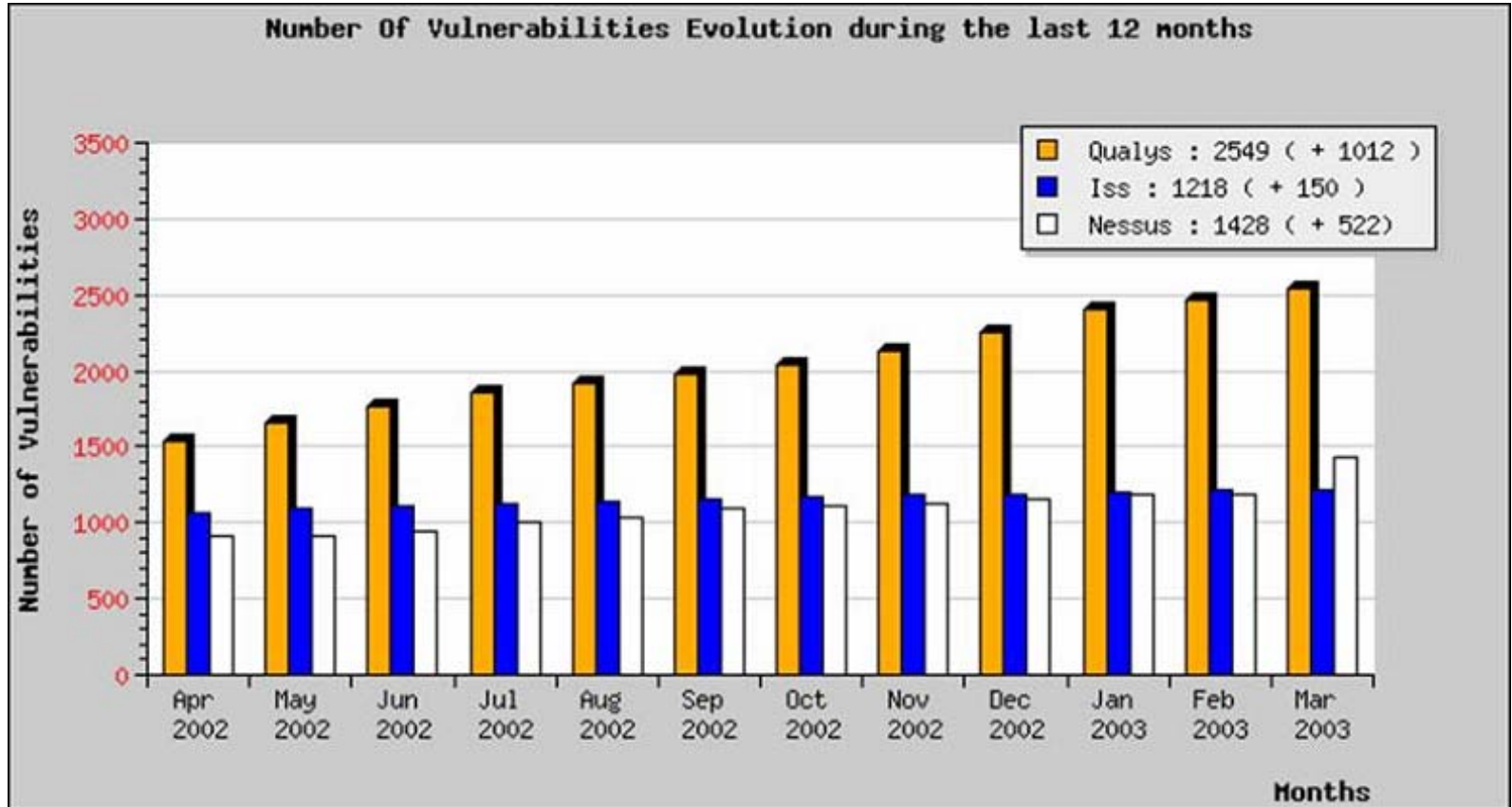
- Teil der unternehmensweiten IuK-Strategie sein
- Inhalte
 - Klassifikation der Bedrohungen und Gefährdungen
 - mögliche Schäden und Schadenshöhe
 - Maßnahmen zur Vermeidung von Schäden
 - Firewall, Intrusion-Detection, Vulnerability-Scanning, Virenschutz, Datensicherung, Zugriffskontrolle, bauliche Maßnahmen
 - Backup-Strategien
 - Wiederherstellungsstrategie im Schadensfall
 - laufende Kontrolle der Sicherungsmaßnahmen
 - permanente Verbesserung der Sicherheitsmaßnahmen
 - Reaktion auf aktuelle Bedrohungen
 - Sicherheitsverantwortlicher



- 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 Virenscannern







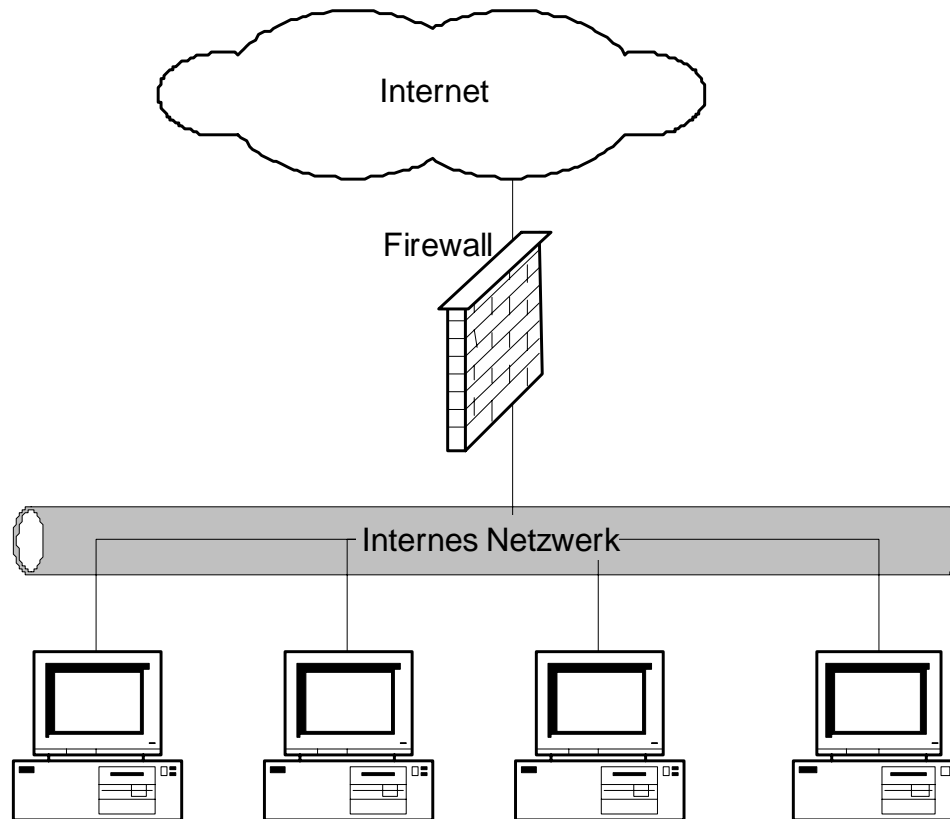
Quelle: Qualys Inc. (www.qualys.com)



Einführung in Firewall-Technologien

Firewalls
Paketfilterung
Proxy
NAT
VPN

- überwacht den Übergang zwischen privatem und öffentlichen Bereich eines Netzwerks



- 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 gegen Angriffe von innen
- bietet keinen vollständigen Virenschutz
- kann sich nicht selbst einrichten

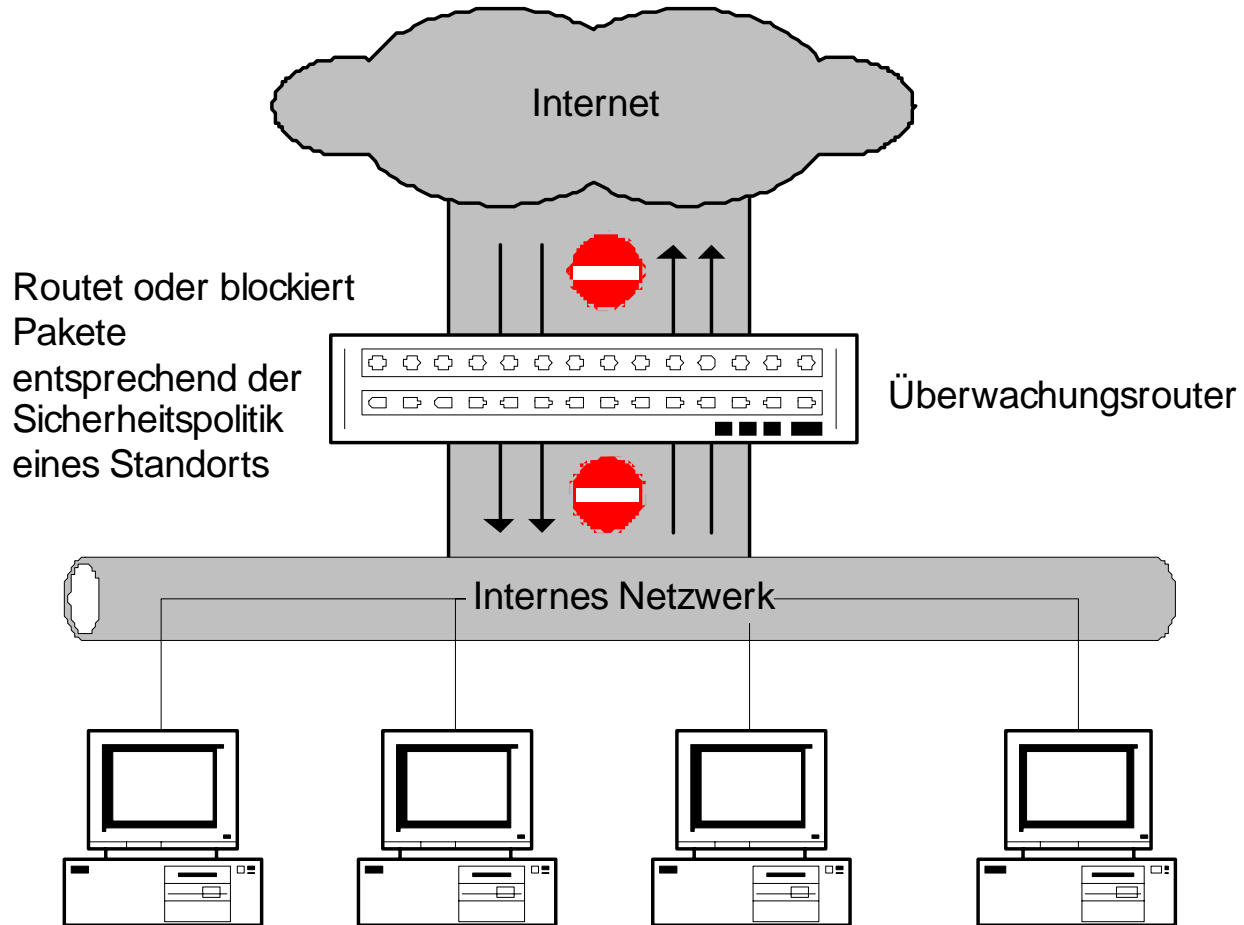


- Paketfilterung
- Proxy-Dienste
- NAT (Network – Adress – Translation)
- VPN (Virtuelle Private Netzwerke)
- IPSec



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 arbeiten auf Ebenen 3 und 4 des ISO/OSI Schichtenmodells
- routet Pakete zwischen internen und externen Hosts
- arbeiten selektiv
- Erlauben und Blockieren von Paketen

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



- 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

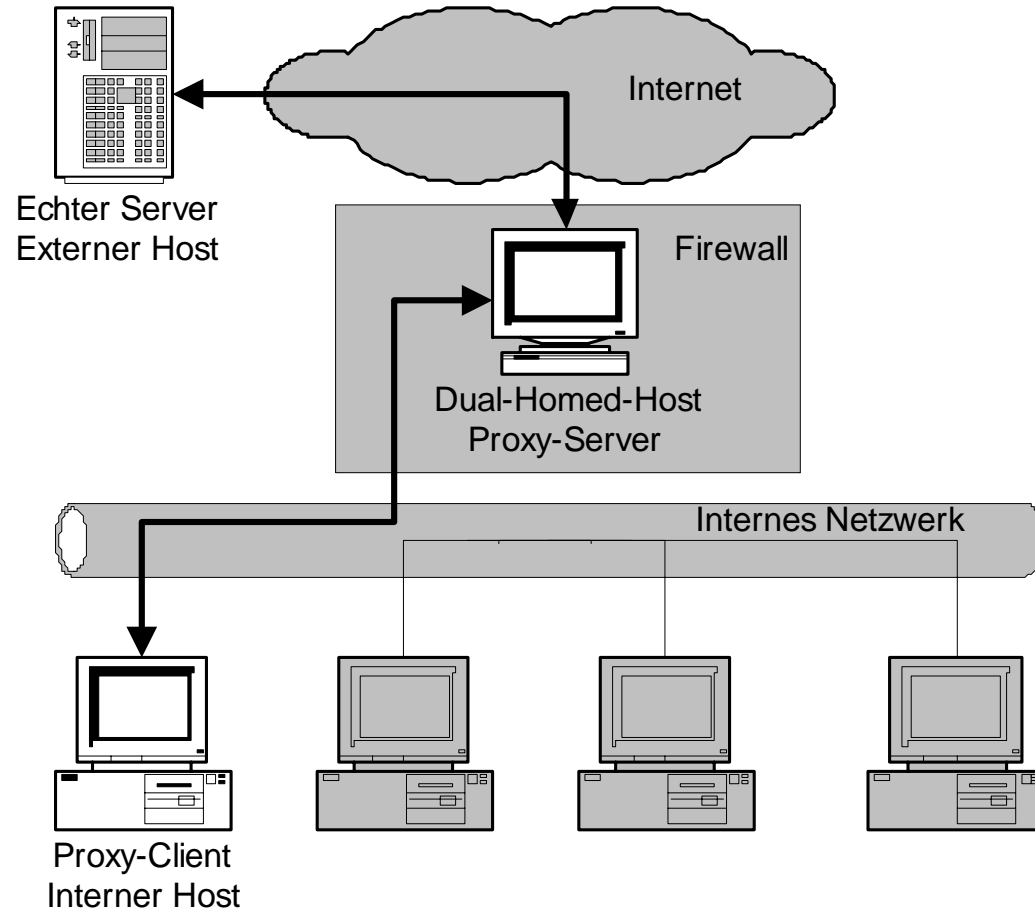


- bekannte Daten
 - Schnittstelle, an der das Paket empfangen wurde.
 - Schnittstelle, an die das Paket weitergeleitet werden soll.
 - ob das Paket eine Antwort auf ein anderes Paket war (**stateful**)
 - wie viele andere Pakete zuvor zu oder von dem gleichen Host übertragen wurden (**stateful**).
 - 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).



- 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





- 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)

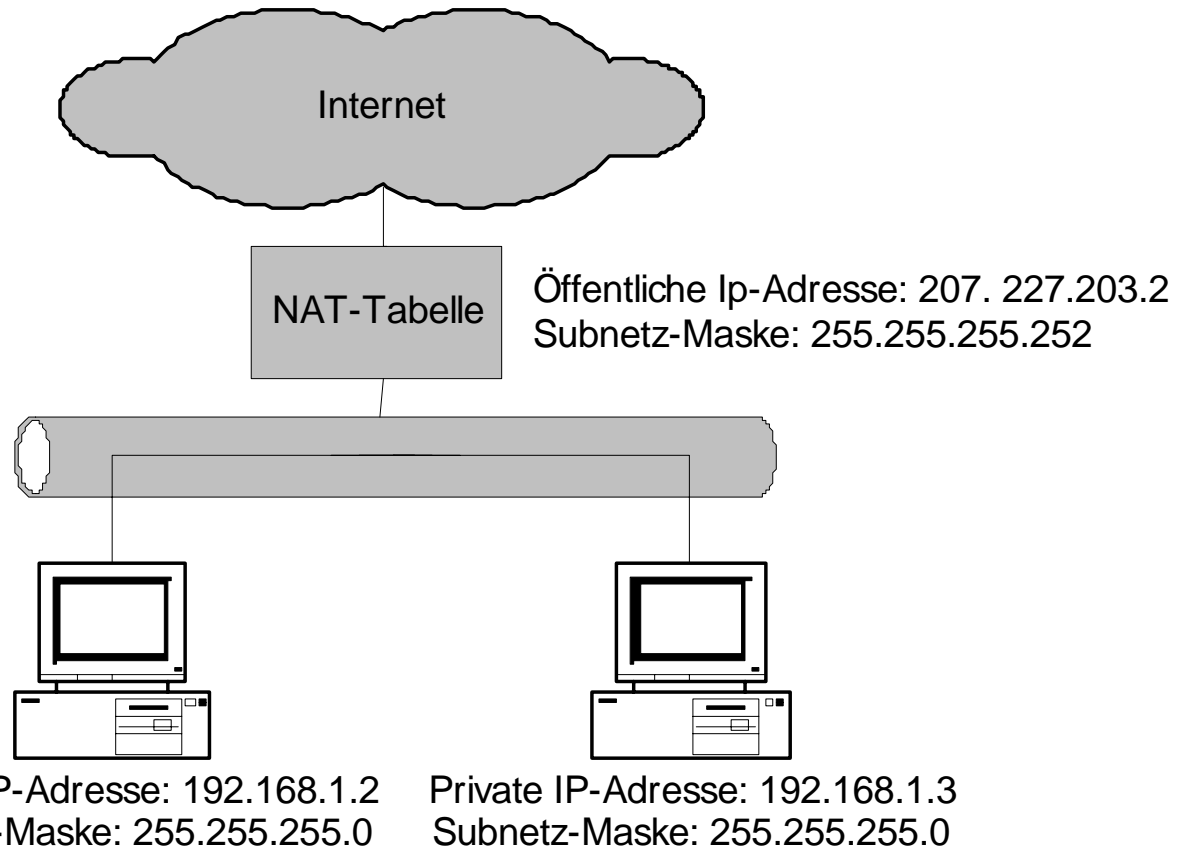


- Veränderung von Netzwerkadressen
- Router verändert Pakete
 - nach außen: Quelladresse wird verändert
 - nach innen: Zieladresse wird verändert
- Häufigste Anwendung: Masquerading / Maskierung:
 - Problem: Durch IPv4-Adressknappheit wird von Providern oft nur eine einzige IP-Adresse zur Verfügung gestellt, 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.



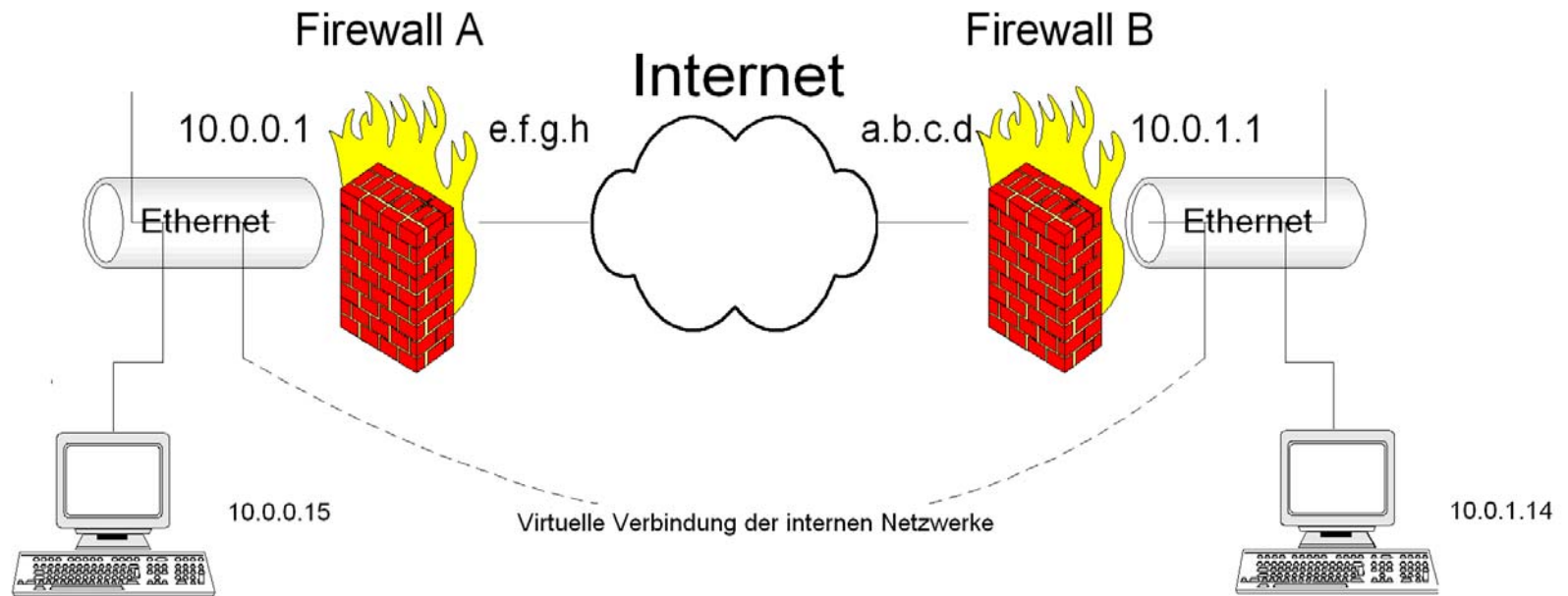
- Vorteile
 - NAT unterstützt die Kontrolle der Firewall über nach außen gerichtete Verbindungen
 - eingehender Verkehr kann eingeschränkt werden
 - interne Konfiguration des Netzwerks wird verborgen
- Nachteile
 - ev. Problem mit eingebetteten IP-Adressen
 - Verschlüsselung und Authentifizierung erschwert
 - 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



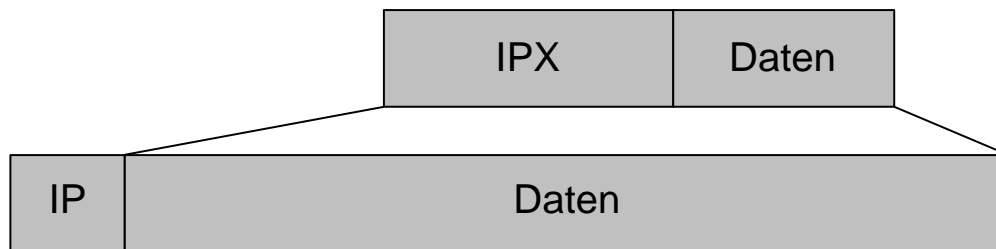
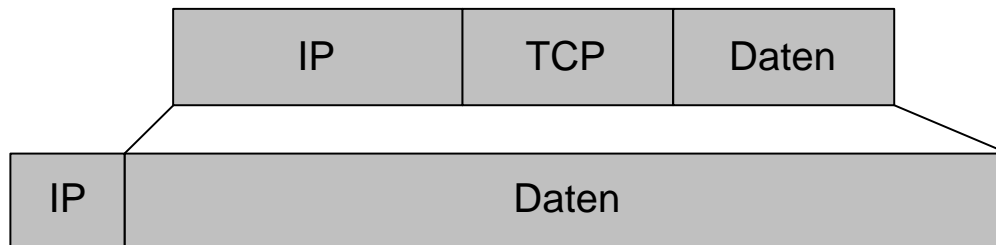


- öffentliches Netz wird privat genutzt
- Verschlüsselung
- Integrität wird geschützt
- Authentizität wird sichergestellt
- Daten werden gekapselt
- Methoden
 - End-zu-End Verschlüsselung
 - Tunnel
- Zeitpunkt der Ver- bzw. Entschlüsselung
 - Behandlung durch den Paketfilter





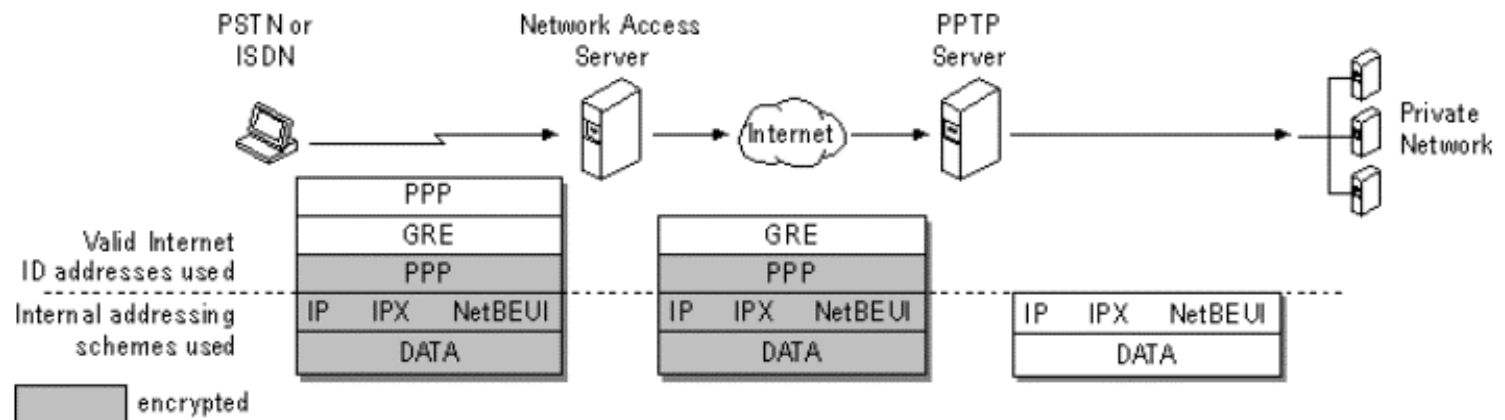
- Meist im Tunnel-Modus betrieben: Rechner hinter den jeweiligen Gateways können transparent miteinander kommunizieren, obwohl die Gateways keine direkte Verbindung haben
- Methode: „Verpacken“ der Pakete, die zwischen den internen Rechnern ausgetauscht werden sollen in IPv4-Pakete



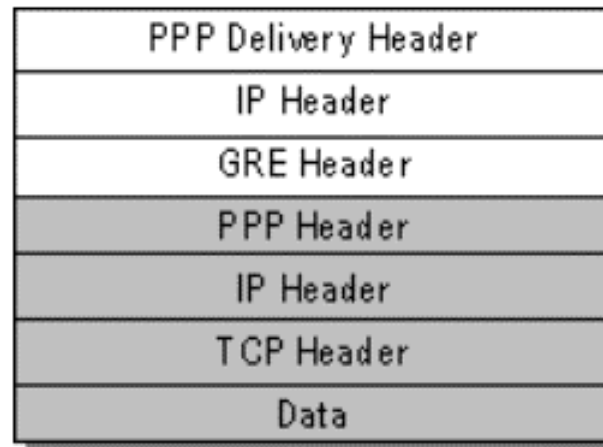
- Verschiedene Implementierungen von Tunneling (Beispiele):
 - GRE (unverschlüsselt)
 - IPv6-in-IPv4 (unverschlüsselt, Übergangsmaßnahme zu IPv6)
 - PPP-over-Ethernet
 - PPP-over-ATM
 - L2TP
 - PPTP
 - IPSec
 - VTun
 - CIPE
 - Tinc
 -



- 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



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



- UNSICHER !

- 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 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“



- 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



- 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



- 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
 - BITS und BITW – Implementierungen
 - VPNs
 - IPSec kapselt IP Pakete mit IPSec Headern



Transport Mode IPSec	Tunnel Mode IPSec
Application	Application
TCP, UDP oder anders IP Protokol	TCP, UDP oder anders IP Protokol
IPSec Security Layer	Inner IP-Address (the ultimate destination of the packet beyond the firewall or gateway)
IP Address	IP Security Layer
Data Layer	Outer IP-Address (gateway or firewall for example)
Physical Layer (hardware)	Data Layer
	Physical Layer (hardware)



- 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 → Einrichtung neuer Zugänge ohne Umkonfiguration des IPSec-Gateways
- Aber: oft problematisch bei verschiedenen Implementierungen



	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

