Vorstellung

Holger Rank
Project Manager HP Services

Hewlett-Packard GmbH
Kieler Straße 147
22769 Hamburg
Tel: 0172 4505057
Email: Holger.Rank@hp.com

Agenda

- Vorstellung HP NSG + Security Services
- Themeneinführung Security
- BSI Security-Konzept Aufbau
- Security Lösungen und Komponenten
  - Network Security
  - Firewall inkl. Content/Virus
  - Access / VPN
  - Intrusion Detection
  - Security Standard 802.1X
  - Desktop / Device Security
- Security Gesamtbild

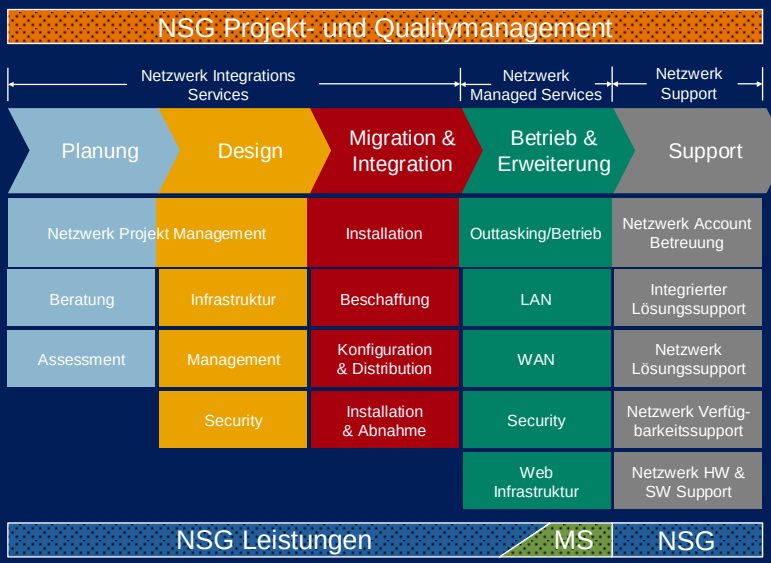
HP Services
Network Solution Group
(NSG)

Vorstellung

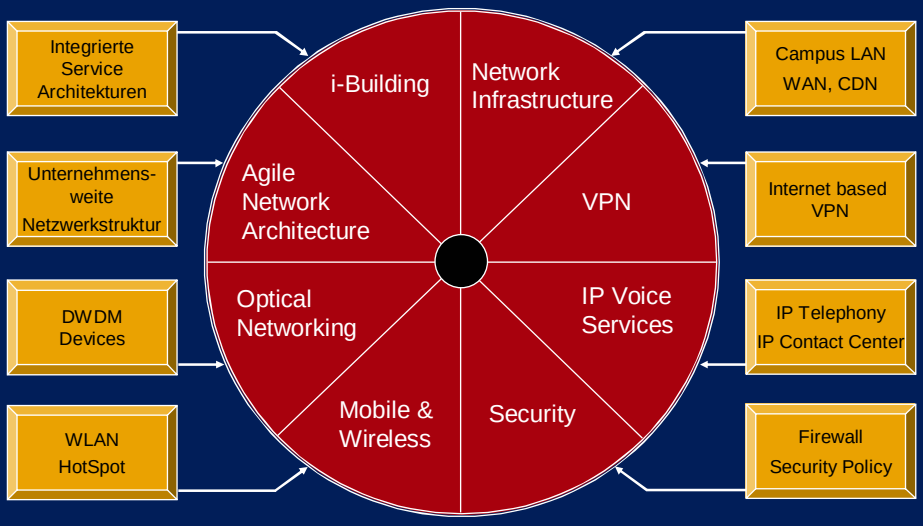
Network Solutions Group Deutschland

- Mitarbeiter an 10 Standorten in Deutschland
  - Business Management und Development
  - Sales und Sales Development
  - Technical Consultants
  - Projektmanager
  - Service Consultants
- Cisco Spezialisierung HP Deutschland
  - Wireless LAN
  - Voice Access
  - IP Telephony
  - VPN und Security
  - Content Networks
  - Network Management
- Zertifizierungen HP Deutschland
  - 14 CCIE‘s
  - 8 CCDP‘s
  - 14 CCNP‘s
  - 3 CCDA‘s
  - 4 CCNA‘s

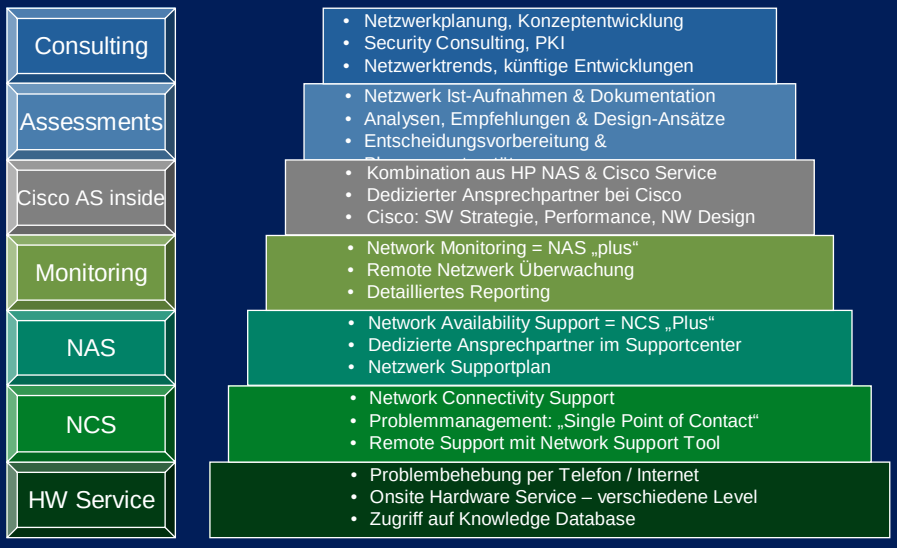
Netzwerk Lifecycle



NSG Fokusthemen



Überblick HP Netzwerk Services



HP Security Themen

- Security Checks / Basis Sicherheitschecks
- Security Konzepte
- Security Reviews
- Network Security
- Application/System Security
- Firewall Security
- Virus und Content Security
- VPN / Session Encryption
- Email Security / PKI

Themeneinführung Security

Themeneinführung Security
Security-Konzept Aufbau
BSI Security-Konzept
Security Lösungen und Komponenten
Network Security
Firewall
Access / VPN
Intrusion Detection
Security Standard 802.1X
Desktop / Device Security
Security Gesamtbild

Themeneinführung Security

Warum brauchen wir Security Lösungen?

- Die Firmen müssen die **Vertraulichkeit**, **Integrität** sowie die **Verfügbarkeit** der IT-Systeme und Daten sicherstellen
- Ein Imageschaden wäre für die meisten Firmen existenzbedrohlich
- Datenschutzauflagen der Regierung und Länder

Themeneinführung Security

Was sind die Gefahren die uns bedrohen?

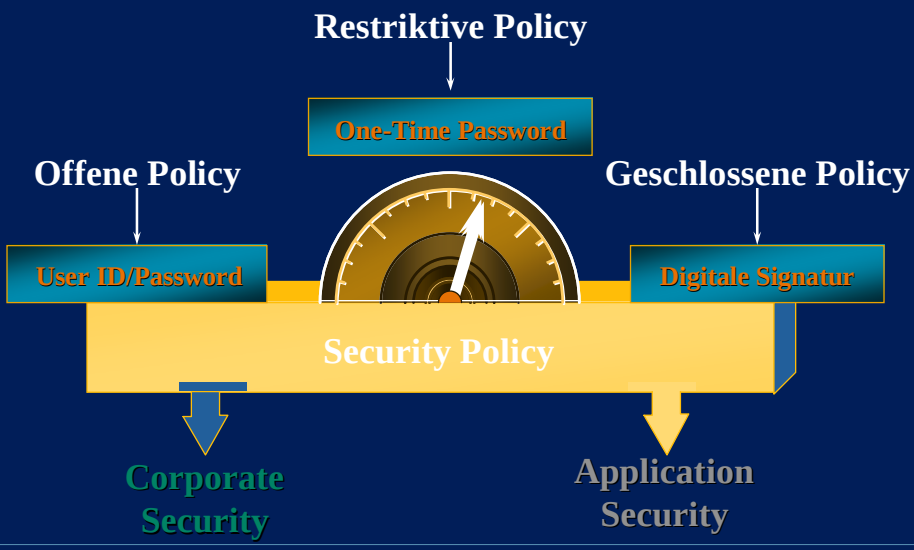
- Keine sicherheitssensiblen Mitarbeiter
  - kein Sicherheitsbewusstsein - wichtige Daten liegen frei zugänglich
  - Informationen werden unbeabsichtigt nach außen getragen
  - die offene Tür des Büros
  - Fremde Personen im Gebäude
  - Notizen über Passwörter
  - Schwache Passwortverfahren - alle verwenden das gleiche Passwort

Themeneinführung Security

Was sind die Gefahren die uns bedrohen?

- Der gezielte Angriff von **innen** auf Firmendaten
  - 60-80% der Angriffe kommen von innen!
  - Beispiel: bewusstes platzieren von Fehlern z.B. in der Datenbank
- gezielte Angriff von außen auf Firmendaten
  - „Das neue Produkt“
  - Konkurrenz - Konkurrenten ausschalten
  - Bei Schulen Angriffe der Schüler/Studenten auf die Zensurdatenbank, Klausuren usw.

Themeneinführung Security



Themeneinführung Security

Wie sieht die Lösung aus?

Themeneinführung Security

Was fehlt… ?

ein *Sicherheitskonzept*

Security-Konzept Aufbau

Themeneinführung Security

Der Inhalt eines Security Konzeptes

1. Ist-Aufnahme aller IT-Systeme
2. Schutzbedarfsfeststellung
3. Bedrohungsanalyse
4. Anforderungskatalog
5. Einteilen in Sicherheitsbereiche
6. Mögliche Sicherheitsmaßnahmen
7. Empfohlenen Sicherheitsmaßnahmen
8. Stufenkonzept


BSI Security-Konzept Vorgehensmodell
Themeneinführung Security
Security-Konzept Aufbau
BSI Security-Konzept
Security Lösungen und Komponenten
Network Security
Firewall
Access / VPN
Intrusion Detection
Security Standard 802.1X
Desktop / Device Security
Security Gesamtbild


Ist-Situation
Schutzbedarfsfeststellung
Bedrohungsanalyse
Anforderungskatalog
Einteilen in Sicherheitsbereiche
Mögliche Sicherheitsmaßnahmen
Empfohlene Sicherheitsmaßnahmen
Stufenplan

Ist-Situation

- Netzwerkstrukturen
- Betriebssysteme
- Anwendungen
- Dateninhalte
- Kommunikationsverhalten
- Schutzanforderungen
- Wie sieht die Policy heute aus?
- Wie ist das Sicherheitsgefühl?

Schutzbedarfsfeststellung

Erfassung aller IT-Systeme

Nr.	Bezeichnung	Lokation	Vernetzt mit	Status	Benutzer
1	HOST	Haus 7	allen Werken Fernwartung Zulieferer 2,3,4,6,7,8	in Betrieb	alle
2	PC-LAN	in allen Häusern	Fernwartung 1,2,7	in Betrieb	alle
3	...	...	...	...	...

Schutzbedarfsfeststellung

Erfassung der schutzbedürftigen IT-Anwendungen

Nr.	**Bezeichnung**	**Schutzbedürftige IT-Anwendungen (grob absteigend vorsortiert)**
1	HOST	Personalwesen Zeiterfassung Rechnungswesen Beschaffungsmarkt Vertrieb Controlling Materialwirtschaft Anwenderprogramme
2	PC-LAN	MS-Word MS-Excel MS-Powerpoint MS-Access MS-Mail usw.
3	...	...

Schutzbedarfsfeststellung

Feststellung des Schutzbedarfs für jedes IT-System

Nr.	Bezeichnung	Grundwert	mittel	hoch	sehr hoch	Begründung
1	HOST	Vertrau-lichkeit		X		Auf diesem System stehen strategische Informationen wie Geldströme und Warenströme von und zu Kunden/Lieferanten, die für den Wettbewerb einen erheblichen Wert darstellen (deutlich mehr als DM 25.000).
		Integrität			X	Durch eine Manipulation der Materialwirtschaft kann die Logistik so stark beeinflußt werden, daß die Produktion falsch läuft, das notwendige Material fehlt, falsche Lieferzeiten berücksichtigt werden, usw. Dieser Umstand kann zu einem finanziellen Schaden über 5 Millionen DM führen.
		Verfüg-barkeit		X		Verzögerte Bearbeitung von Verwaltungsvorgängen und verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen sind bis zu einem Tag tolerabel. Ein längerer Ausfall des Systems hätte einen Renommeeverlust des Unternehmens zur Folge und würde zu einen finanziellen Schaden deutlich über DM 25.000,--führen.
2	PC-LAN	Vertrau-lichkeit			X	Auf diesen Rechnersystemen wird die Korrespondenz gespeichert. Da hier streng vertrauliche Informationen

Bedrohungsanalyse

Bedrohungen	Bewertung/relevant
Höhere Gewalt - G 1.1 Personalausfall - G 1.2 Ausfall des IT-Systems - G 1.4 Feuer - G 1.5 Wasser - G 1.8 Staub, Verschmutzung	Wird als geringe Bedrohung angesehen. Bei Ausfall des Systemadministrators ist eine Vertretung sichergestellt. Ein Ausfall des IT-Systems wird durch ein vorhandenes Ersatzssystem aufgefangen. Die entsprechenden Räume sind gegen evtl. auftretende Schäden gesichert.
Menschliche Fehlhandlungen - G 3.2 Fahrlässige Zerstörung von Gerät oder Daten - G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen - G 3.5 Unbeabsichtigte Leitungsbeschädigung - G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal - G 3.8 Fehlerhafte Nutzung des IT-Systems - G 3.9 Fehlerhafte Administration des IT-Systems	Aufgrund der Ausbildung und ständigen Information des zuständigen Technik-Personals wird eine geringe Bedrohung gesehen. Der Zutritt und Aufenthalt Außenstehender zu den schutzbedürftigen Räumen erfolgt nur in Anwesenheit der Zutrittsberechtigten

Anforderungskatalog

- Der Anforderungskatalog ist geprägt durch die Anforderungen der Sicherheitspolitik (Policy) und des Datenschutzes
- Basis für den Anforderungskatalog ist das Abschlussdokument der Schutzbedarfsfeststellung
- Ziel des Anforderungskataloges ist die genaue Beschreibung der Anforderungen eines oder einer Gruppe von IT-Systemen an das Sicherheitskonzept

Anforderungskatalog

Die einzusetzenden Sicherheitskriterien

- Verlust der Vertraulichkeit
  - Daten werden bekannt
- Verlust der Integrität
  - Daten werden verändert und verfälscht
- Verlust der Verfügbarkeit
  - Systemstillstand

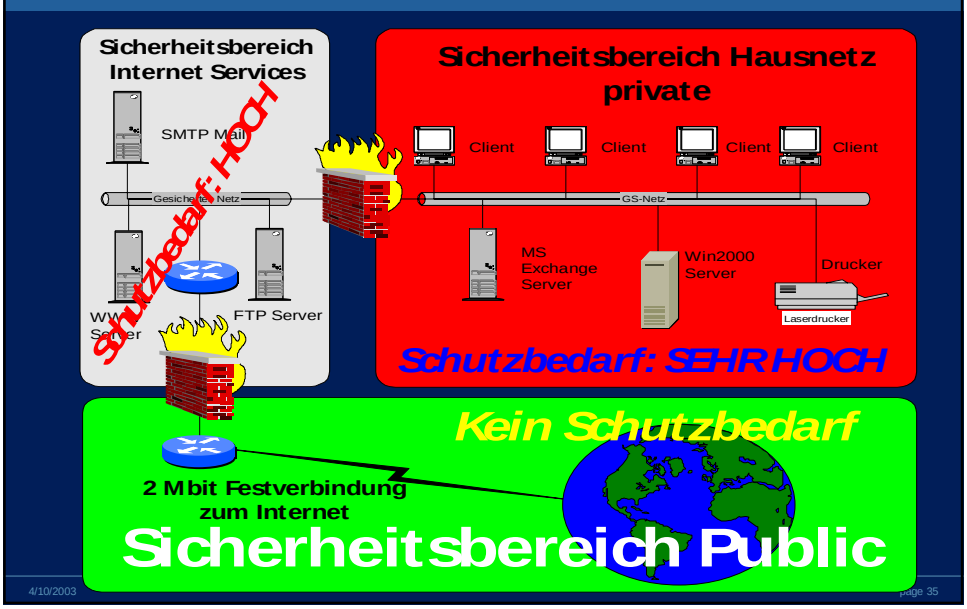
Ist-Situation
Schutzbedarfsfeststellung
Bedrohungsanalyse
Anforderungskatalog
Einteilen in
Sicherheitsbereiche
Mögliche Sicherheitsmaßnahmen
Empfohlene Sicherheitsmaßnahmen
Stufenplan

Sicherheitsbereiche

Zweck von Sicherheitsbereichen:

- Schaffung einer klaren Sicherheitstopologie und IT-Infrastruktur
- Einbringen von Kontrollstrukturen beim Übergang von einem zum anderen Sicherheitsbereich
- Zusammenfassen von IT-Systemen mit gleichem Schutzbedarf
- Bildung klarer Kommunikationsflüsse
- Definition der anzuwendenden Sicherheitsmaßnahmen wie z.B. Verschlüsselung
- Kosteneinsparungen

Sicherheitsbereiche



- Ist-Situation
- Schutzbedarfsfeststellung
- Bedrohungsanalyse
- Anforderungskatalog
- Einteilen in Sicherheitsbereiche
- Mögliche Sicherheitsmaßnahmen
- Empfohlene Sicherheitsmaßnahmen
- Stufenplan

Mögliche Sicherheitsmaßnahmen

- Hier werden alle möglichen Grundschutz-Sicherheitsmaßnahmen für ein IT-System benannt
- Als Basis dient das BSI Grundschutzhandbuch (BSI GSHB)
- Die BSI GSHB Maßnahmen werden unterteilt in
  - Infrastruktur
  - Organisation
  - Personal
  - Hard- / Software
  - Kommunikation
  - Notfallvorsorge
- Tiefergehende Maßnahmen als die des BSI-GSHB

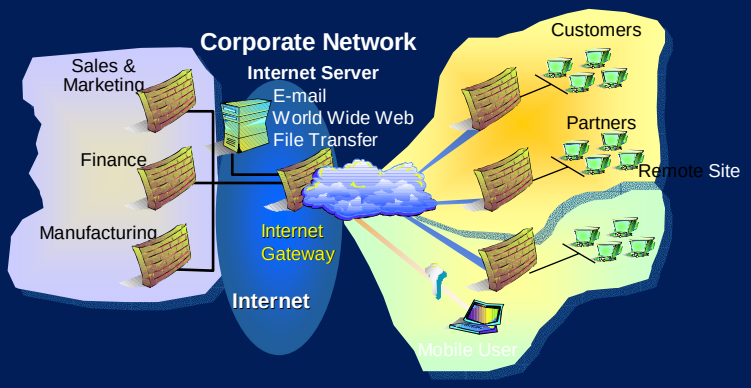
Mögliche Sicherheitsmaßnahmen

Beispiel für ein Sicherheitsbereich

Mögliche Sicherheitsmaßnahmen

Beispiel für eine Maßnahme

Extranet VPN



Empfohlene Sicherheitsmaßnahmen

Beispiele...

- Einsatz von VPNs mit Verschlüsselung
- Bildung verschiedener Sicherheitsbereiche wie z.B. DMZ (Demilitarisierte Zone)
- Einsatz von Firewalls inkl. Proxies für
  - Content Checking
  - Virusscanning
  - Mail und Traffic Entkopplung
- Intrusion Detection Systeme

Stufenplan

Der Stufenplan definiert die zeitliche Vorgehensweise unterteilt in:

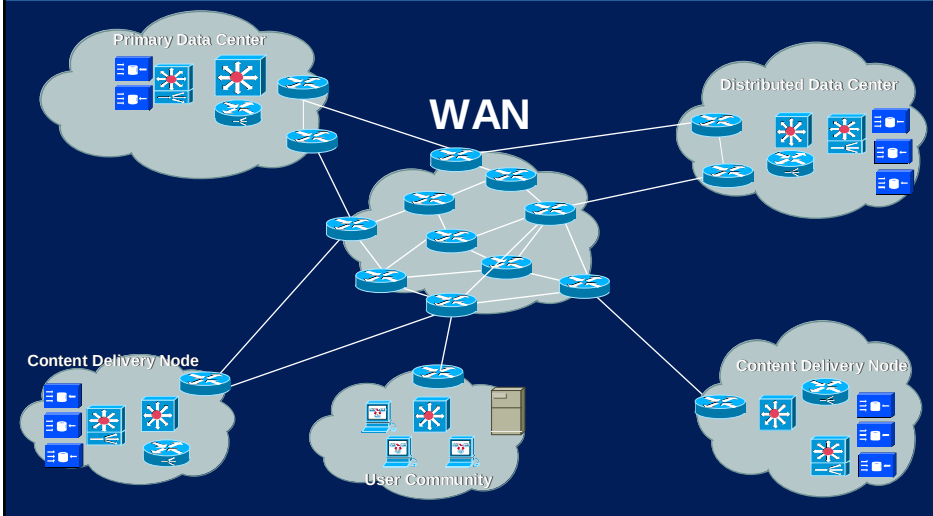
- kurzfristige Umsetzung
- mittelfristige Umsetzung
- langfristige Umsetzung

Security Lösungen und Komponenten

Network Security

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- **Network Security**
- Firewall
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

Network Security



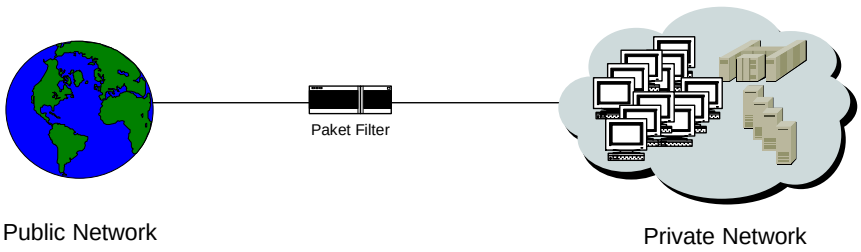
Firewall

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- **Firewall**
- Access / VPN
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

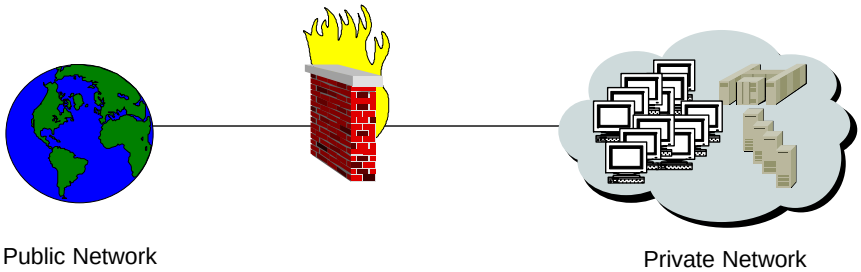
Überblick Firewall

- Paket Filter (Router, Switches)
- Stateful Inspection Firewall
- Application Gateway Firewall
- Kombination aus allen
- Verschiedene technische FW-Konzepte
- Firewall Lösungen für spezielle Erfordernisse

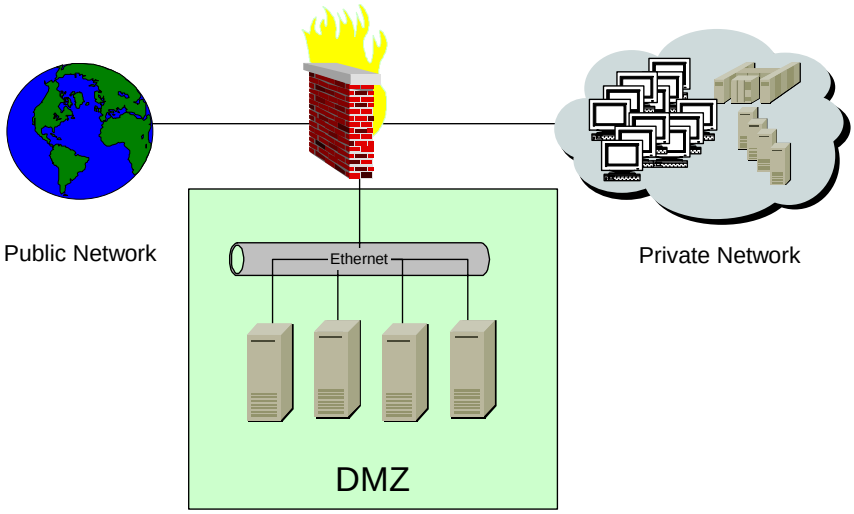
Paketfilter



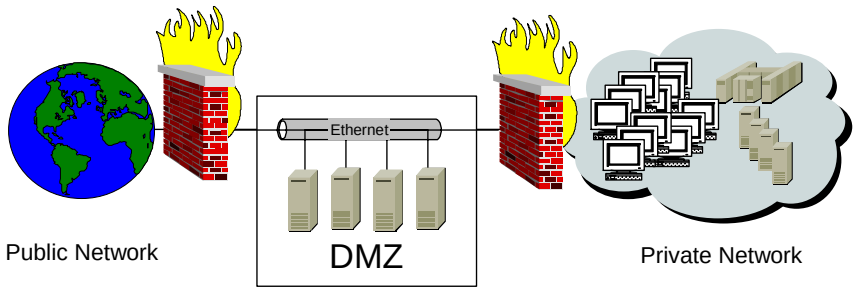
Firewall Typ 1 - Standard



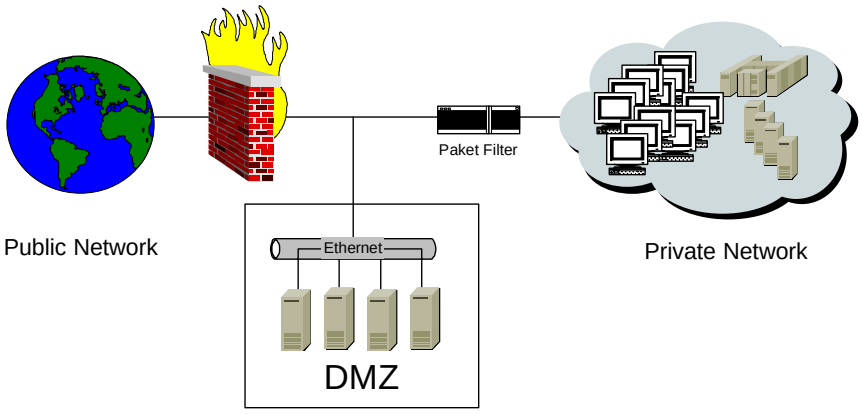
Firewall Typ 2 – Standard DMZ



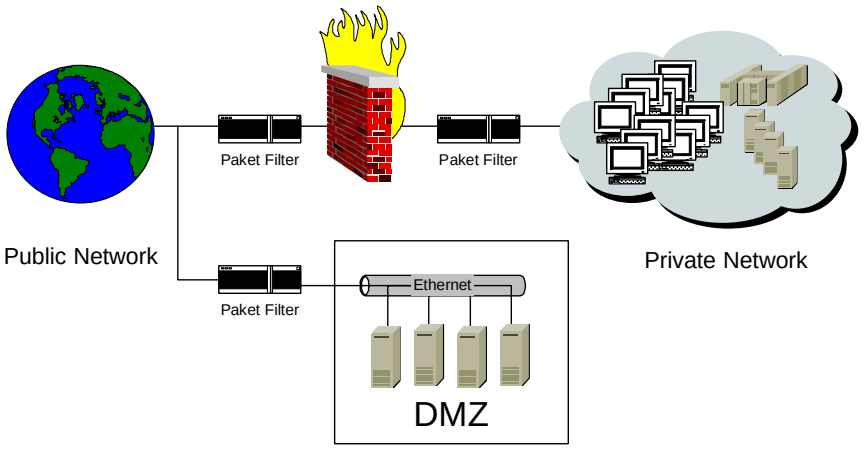
Firewall Typ 3 – 2x FW



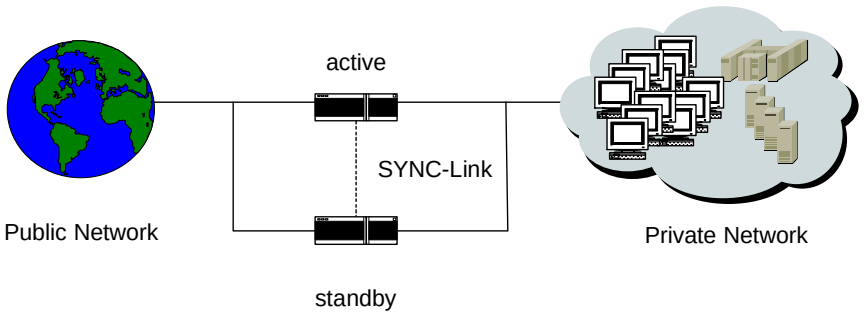
Firewall Typ 4 – FW + PF



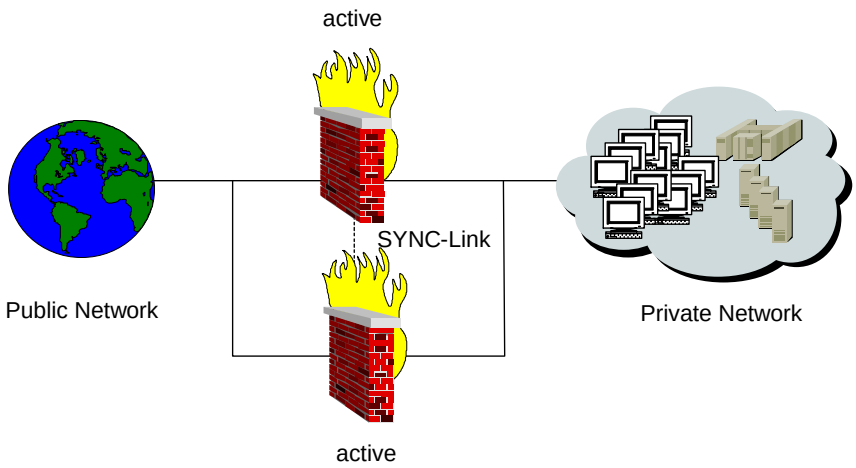
Firewall Typ 5 – Kryptokom (Utimaco)



Firewall Redundanz – Einfach (Appliance)



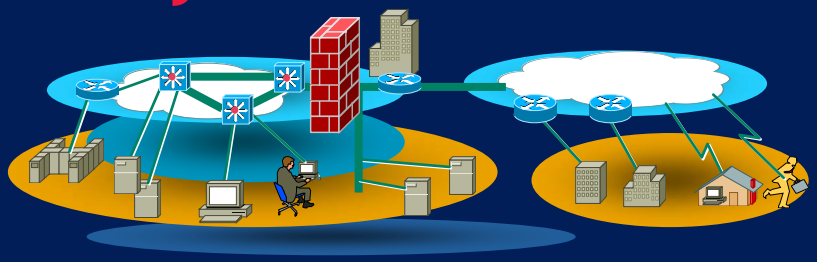
Firewall Redundanz – Software



Sicherheitsverständnis …

Sicherheit = Firewall

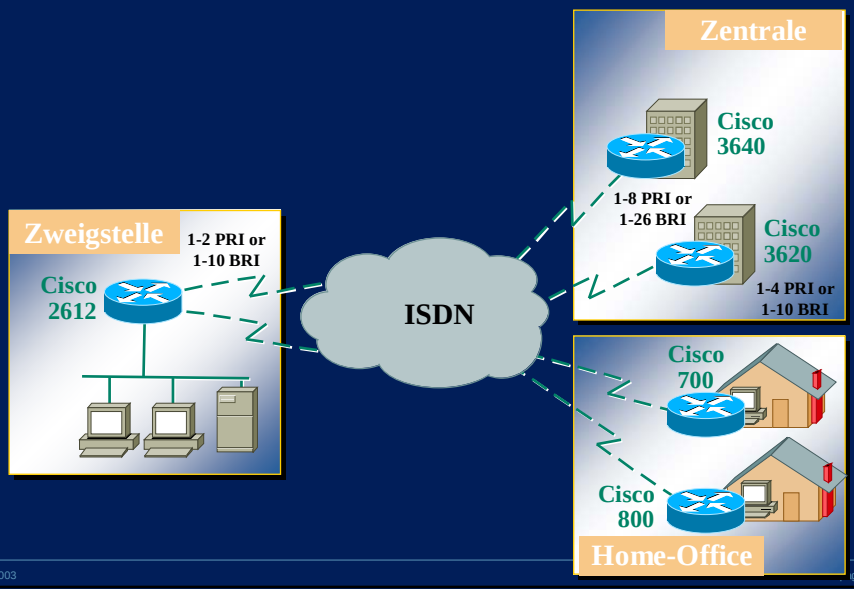
… ist nicht genug !!!



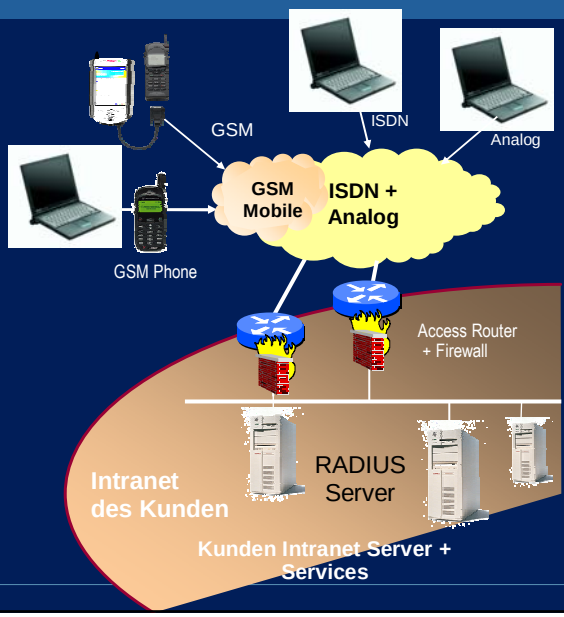
Access / VPN

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- **Access / VPN**
- Intrusion Detection
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

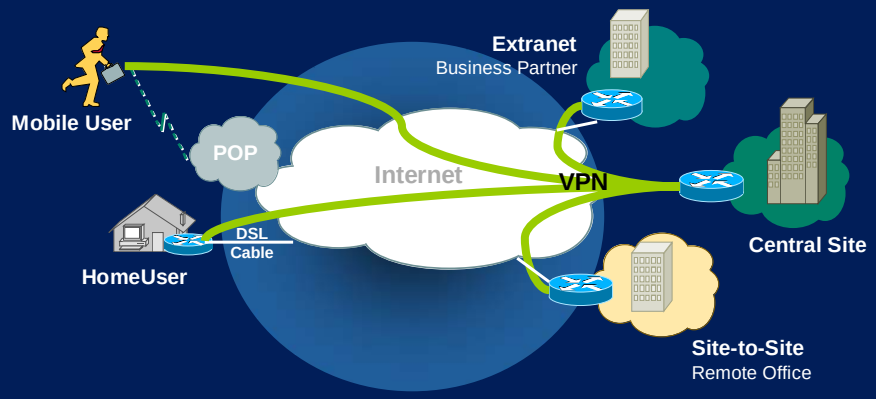
ISDN Dial-In Konzentration



ISDN, GSM, Analog Access



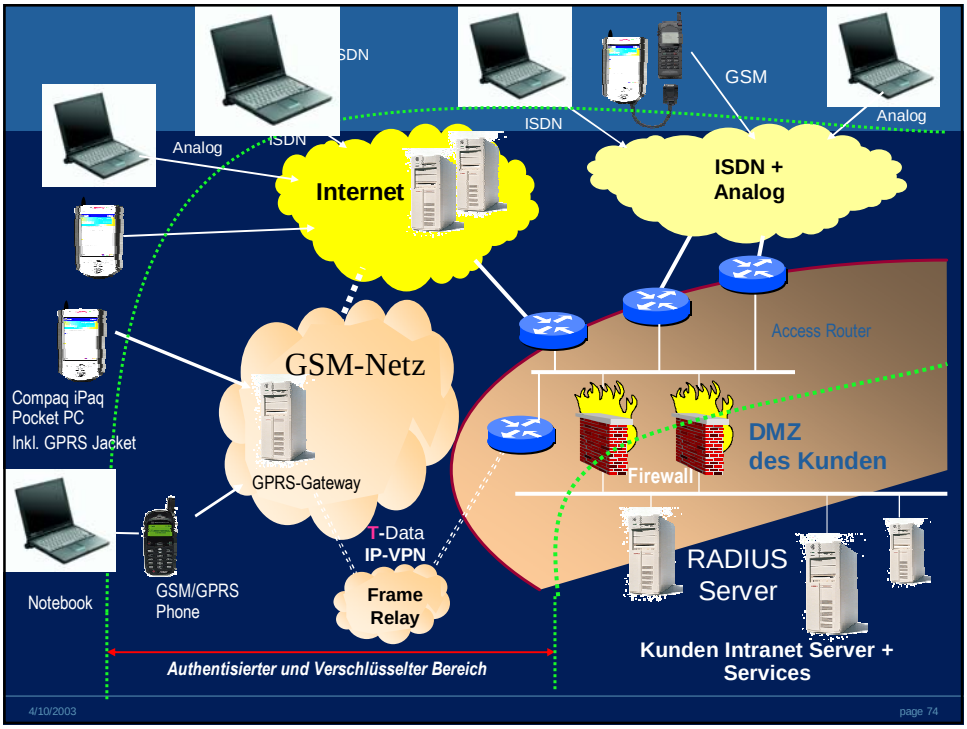
VPN



Und nun....

alles zusammen:

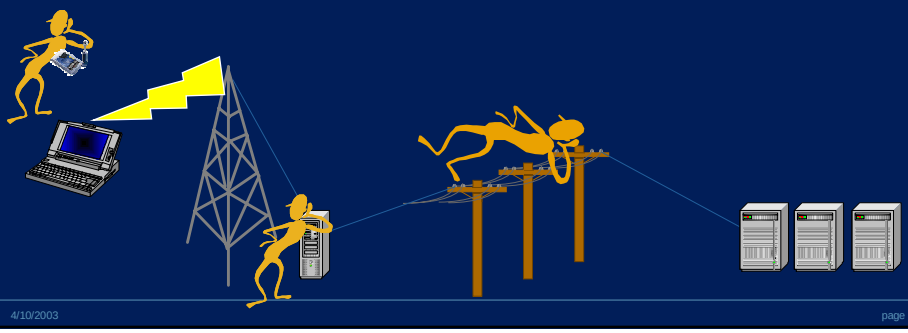
ISDN, Analog, GSM, GPRS, Wireless LAN und VPN


ISDN
ISDN
GSM
Analog
Analog
ISDN
Internet
ISDN +
Analog
Access Router
GSM-Netz
Compaq iPaq
Pocket PC
Inkl. GPRS Jacket
GPRS-Gateway
DMZ
des Kunden
Firewall
T-Data
IP-VPN
Frame
Relay
RADIUS
Server
Notebook
GSM/GPRS
Phone
Authentisierter und Verschlüsselter Bereich
Kunden Intranet Server +
Services
4/10/2003
page 74


invent
VPN Überblick

Virtual Private Networks

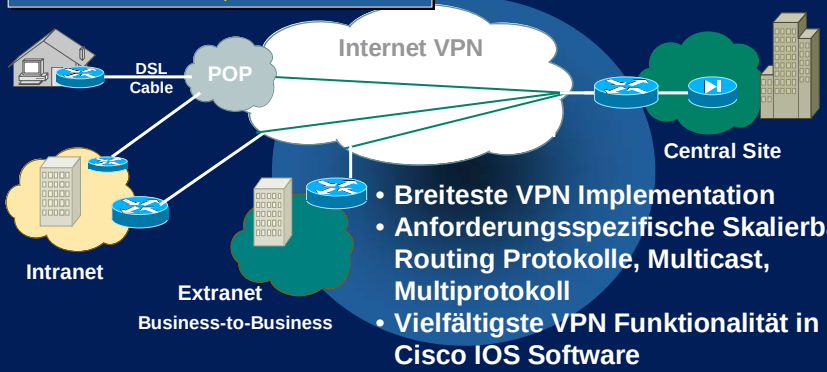
- Use encryption to secure data across an untru network
- Provides confidentiality and integrity
- Extend our private network to mobile users



Cisco Site-to-Site VPNs

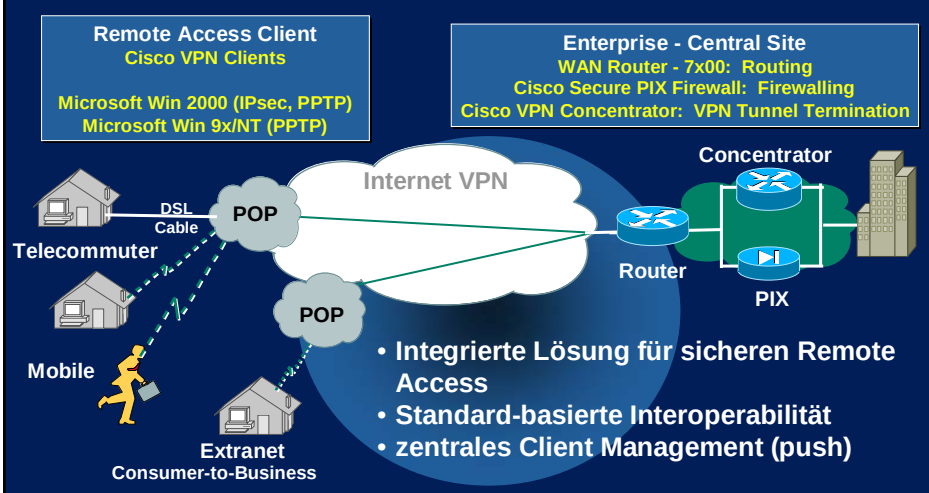
Access CPE - Remote Site
Cisco VPN-Optimized Routers -
800, 1700, 2600, 3600, 7100
Cisco Broadband Access Platforms -
1400 Cable Modem, uBR DSL Modem

Enterprise - Central Site
Cisco VPN Routers - 7x00: Routing + VPN
Cisco Secure PIX Firewall: Firewalling

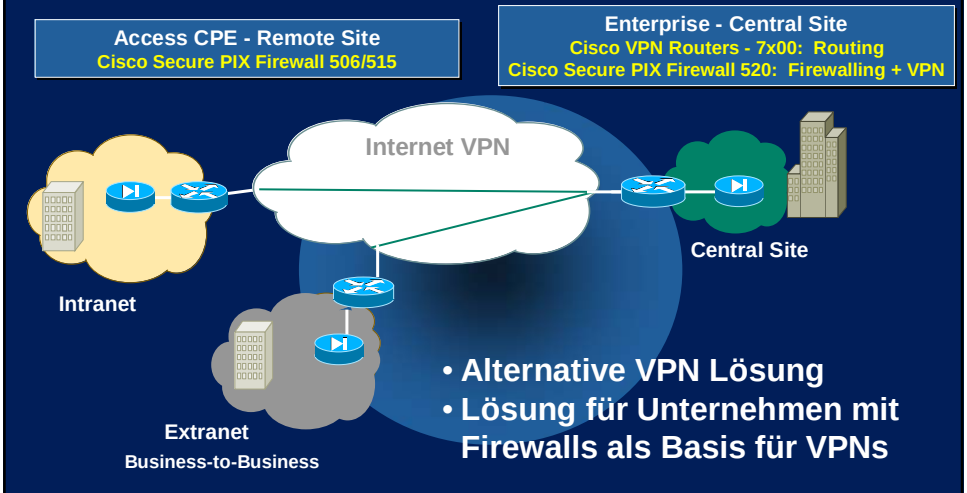


- **Breiteste VPN Implementation**
- **Anforderungsspezifische Skalierbarkeit, Routing Protokolle, Multicast, Multiprotokoll**
- **Vielfältigste VPN Funktionalität in der Cisco IOS Software**
- **QoS Funktionalitäten**

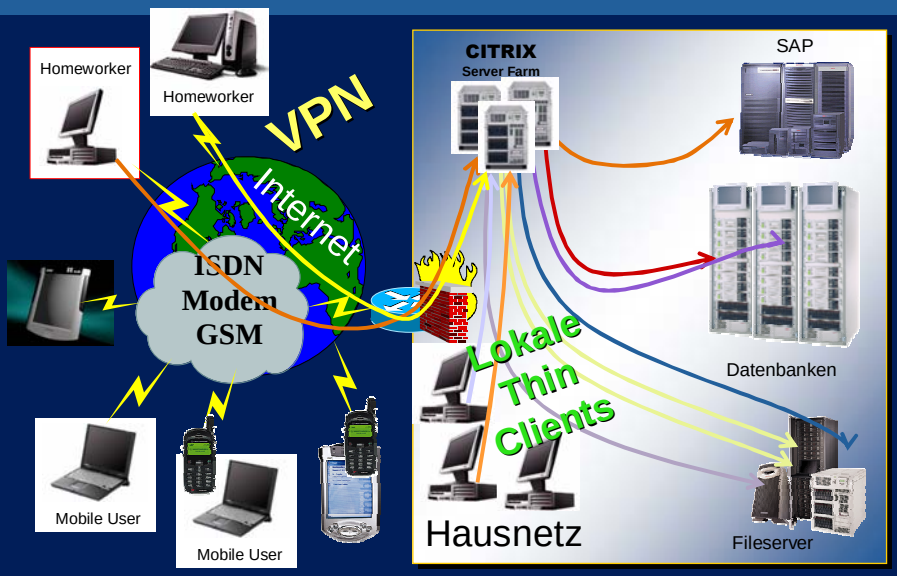
Remote Access VPNs: Cisco VPN 3000 Concentrator



Cisco Firewall-Based VPN



Citrix VPN Lösung



4/10/2003 page 80

Intrusion Detection

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- Access / VPN
- **Intrusion Detection**
- Security Standard 802.1X
- Desktop / Device Security
- Security Gesamtbild

Was ist Intrusion Detection ?

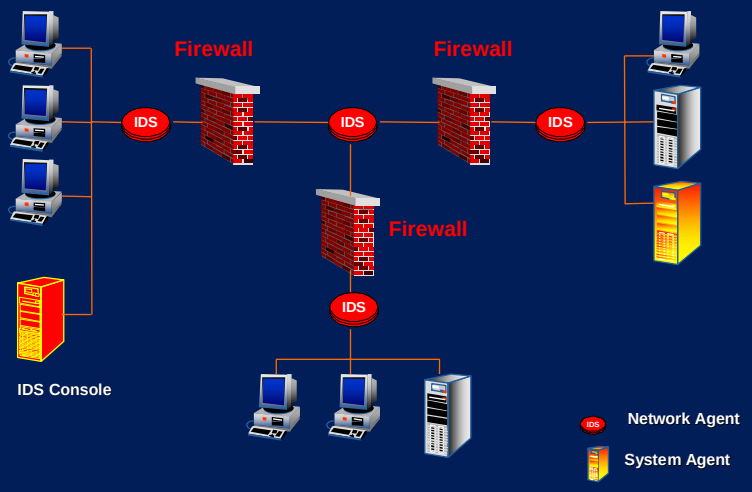
Erkennung von

- Angriffsversuchen
- Einbrüchen
- Schadensumfang
- Viren
- Zielgenaue Analyse

IDS - Baustein zur Verteidigung

- Hostsensoren
- Netzsensoren
- Zentraler Log und Management Server
- Alarming
- Correlation

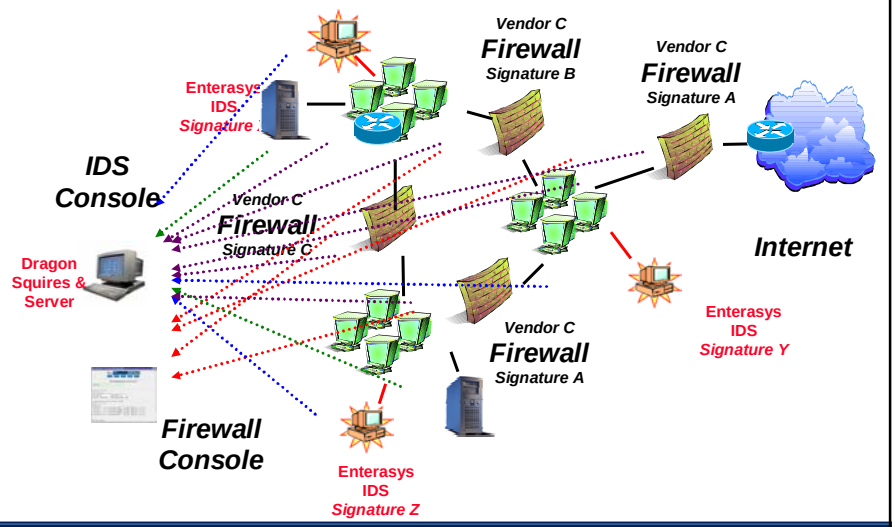
Übersicht: Intrusion Detection



IDS Management

- Zentrales Management für alle IDS Sensoren
- Zentrale Auswertung von Log-Files (auch 3rd Party)
- Alarmfunktionen (Email, Pager, SNMP usw.)
- Angriffsreporting
- Automatischer Soft- und Regelupdate Download vom Hersteller
- Automatische Soft- und Regelupdates für alle IDS Sensoren

Intrusion Detection Firewall, Router, Host log files...



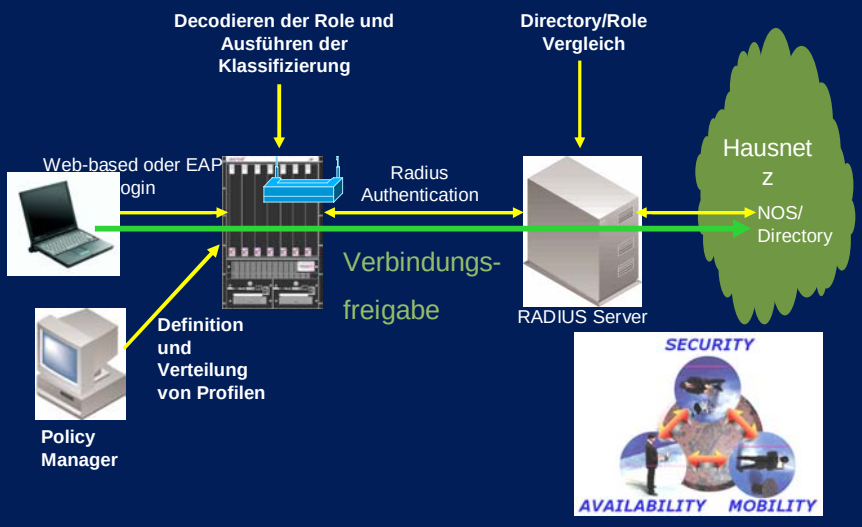
Security Standard 802.1X

- Themeneinführung Security
- Security-Konzept Aufbau
- BSI Security-Konzept
- Security Lösungen und Komponenten
- Network Security
- Firewall
- Access / VPN
- Intrusion Detection
- **Security Standard 802.1X**
- Desktop / Device Security
- Security Gesamtbild

IEEE 802.1x

- **Standard verabschiedet Juni 2001**
- **Port based Network Access Control**
- **Definiert**
  - Authentication Framework
  - Mechanismen zur Zugangskontrolle
  - Verschiedene Level zur Zugangskontrolle
  - Verhalten der Ports innnerhalb dieser Level (transmission, reception of frames)
  - Protokolle zur Kommunikation zwischen Authenticator und Authentication Server
- **Ermöglicht interoperable Benutzer-Identifikation, zentralisierte Authentisierung, Key Management**
  - Nutzt existierende Standards: EAP, RADIUS, MD5
  - Compatibel mit existierende Roaming Technologien, ermöglicht Nutzung in Hotel und öffentlichen Plätzen
- **Unterstützt wird Ethernet, Token Ring und IEEE 802.11(Wireless)**

IEEE 802.1x Funktionsweise



Desktop / Device Security

Desktop Security

- Normales Username / Password Verfahren reicht nicht
- Einfaches aber sicheres Verfahren notwendig
- Rechtevergabe auf Basis der Policy (LDAP/AD)
- Bereitstellung von Applications nach Userpolicy
- Besitztum und Wissen als „Passwort“ (Smartcard + PIN)
- Einsatz von biometrischen Verfahren (Fingerprint, Iris Scan usw.)
- Single SignOn

Desktop Security Devices

- Alle IT-Systeme!
  - Server
  - PC‘s
  - Terminals
  - PDA
  - Notebooks
  - Unix Systeme
  - Other System (VMS usw.)

Mögliche Verfahren

- One Time Password - SecureID Token
- SmartCard
- Fingerprint Reader (Builtin, Mouse, PCMCIA)
- Iris Scan (Festinstallation / Zugangsschutz)
- Spracheingabe
- Handy SMS Verfahren
- USB Dongles
- Sonstige Dongles (Serial usw.)

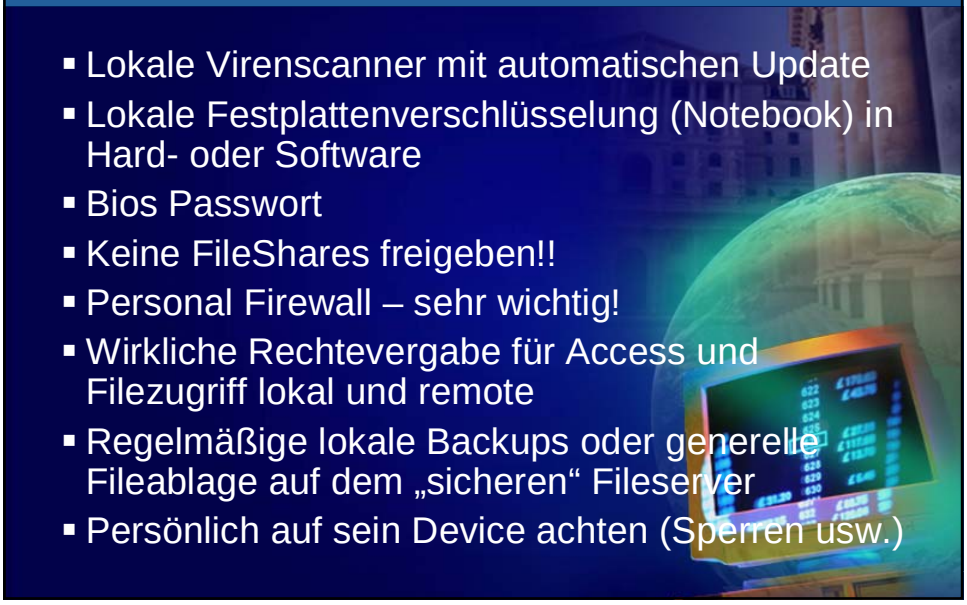
Zielsetzung: So einfach und komfortable wie möglich für den User!!!

Einsatzgebiete

- Natürlich Benutzeranmeldung am System
- Remote Access
- VPN / Firewall Anmeldung
- Lokale und Remote Datenverschlüsselung
- Email Verschlüsselung und Signatur
- HBCI HomeBanking
- Zugangssysteme z.b. RZ
- PDA
- Öffentliche Terminals z.B. in Schalterhalle d. Bank

4/10/2003

Desktop Security – weitere Maßnahmen

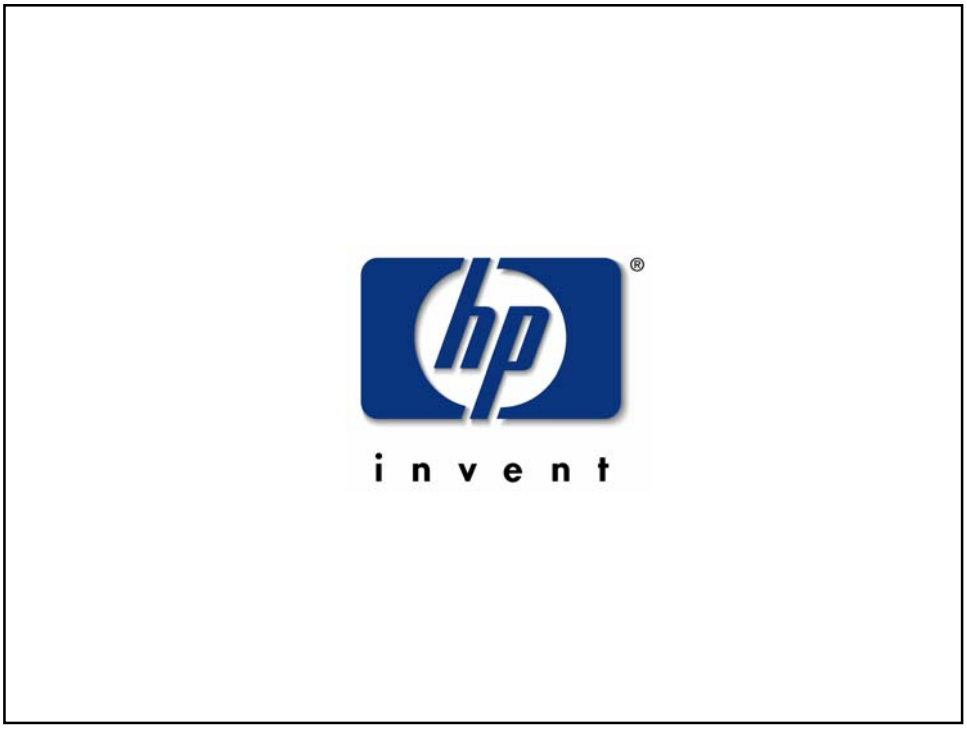


- Lokale Virenscanner mit automatischen Update
- Lokale Festplattenverschlüsselung (Notebook) in Hard- oder Software
- Bios Passwort
- Keine FileShares freigeben!!
- Personal Firewall – sehr wichtig!
- Wirkliche Rechtevergabe für Access und Filezugriff lokal und remote
- Regelmäßige lokale Backups oder generelle Fileablage auf dem „sicheren“ Fileserver
- Persönlich auf sein Device achten (Sperren usw.)

Security Gesamtbild

Gesamtbild

- Security betrifft alle Bereiche einer Infrastruktur
- Security ist keine Einzellösung! (nicht nur Firewall)
- Security beinhaltet organisatorische wie technische Maßnahmen
- Security muss Abteilungsübergreifend in den Firmen betrachtet werden
- Einen 100% Schutz gibt es nicht, aber einen recht hohen Schutz!
- Security ist immer ein Kompromiss
- Schaden: 1. Image, 2. Wirtschaftlich!!!


invent