Security

- Verschlüsselung / Firewall/Proxy
- Virenschutz
- IDS/IPS
- Content Security
- Web-Filterung / VPN
- Authentifizierung
- Analyse/Reporting
- Hochverfügbarkeit
- Traffic-/IP-Management
- Social Engineering

Grundsätzliches

Was wird geschützt ?

- Information (Daten, Applikationen)
- Image des Unternehmens bzw. Behörde
- Ressourcen (Kosten, Arbeitszeit)
- Verfügbarkeit (Business, Kommunikation)

Wovor wird geschützt ?

- Unbefugtes Eindringen
- System-Missbrauch
- Missbrauch von Berechtigungen
- Veränderung, Zerstörung und Verlust von Daten
- Mangelnde Verfügbarkeit von Services

Grundsätzliches

Welche Riskiogruppen gibt es ?

- **Menschen** (Mitarbeiter, Gäste, Administratoren, Freiberufler, Putzfrau, Zeitarbeitskräfte)
- **Hardware** (PC‘s, Server, Netzwerk, Router, etc.)
- **Software** (Programme, Betriebs-Systeme, Applikationen, Kommunikationstools, etc.)
- **Daten** (übertragene Daten, lokal gespeicherte Daten, nicht gespeicherte Daten)
- **Zubehör** (USB-Stick, Access-Points, Sicherungsbänder, CD‘s, Dokumentation, Modems)
- **Räume** (Zutritt, physikalischer Zugriff, Papierkörbe, Arbeitsplätze..)

Grundsätzliches

Fragen:

1.) Wer kann auf meine Daten zugreifen ?
2.) Von woher kann zugegriffen werden ?
3.) Wer könnte Interesse an meinen Daten haben ?
4.) Welche Folgen hat es, wenn meine Daten verändert, gestohlen, veröffentlicht werden oder Unberechtigte Zugang haben ?
5.) Was passiert, wenn mein Unternehmenszugang schlecht/ nicht erreichbar ist ?
6.) Welche Kosten entstehen, wenn kein Überblick über den Zugriff auf Daten und die Nutzung des Internets möglich ist ?
7.) Welche rechtlichen Folgen kann die Nutzung des Internets durch meine Mitarbeiter oder aber auch der Missbrauch meiner Daten und Rechner durch Dritte für das Unternehmen haben ?

Grundsätzliches

Was passiert, wenn mein Unternehmenszugang bzw. meine Behörde schlecht/nicht erreichbar ist ?

- Imageverlust
- mangelnde Kommunikation
- Zeitverzögerungen
- Verlust wichtiger Nachrichten und Informationen
- Verlust von Umsatz/Business
- schlechte Reaktionsfähigkeit
- verspätete Informationen
- Verärgerung von Kunden/Bürgern und Partnern/Institutionen
- Motivationsprobleme bei Mitarbeitern

Grundsätzliches

Welche Kosten entstehen, wenn kein Überblick über den Zugriff auf Daten und die Nutzung des Internets möglich ist ?

- erhöhte Kosten des Internet-Zuganges durch Limit-Überschreitung
- erhöhte Kosten durch zusätzlich benötigte Bandbreite
- Effektivitätsverlust durch Surfen während der Arbeitszeit
- keine Möglichkeit der Kostenzuweisung auf User, Abteilungen etc.

Gesetzliche Vorraussetzungen

StGB Strafgesetzbuch :

§184 Verbr. Porno.Schriften
§ 202a Ausspähen v. Daten
§ 303 Sachbeschädigung
§ 303a Datenveränderung
§ 303 b Computersabotage
§ 303 c

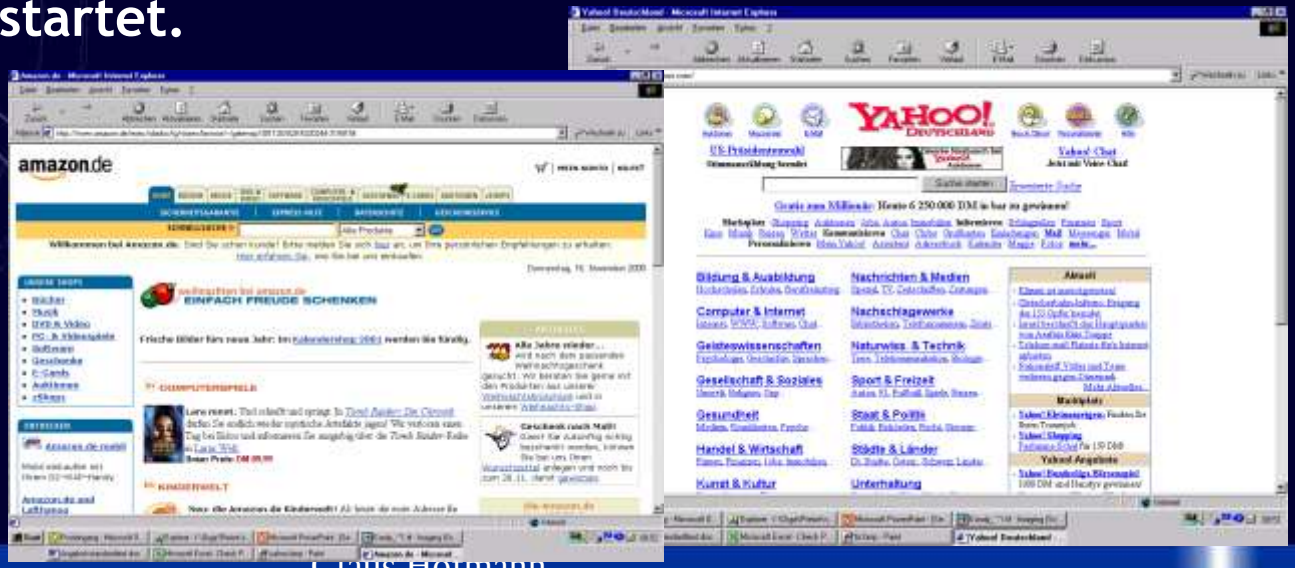
IUKG Multimedia Gesetz

Beispiele

Angriff auf amazon.com, yahoo.com, ebay.com

(Februar 2010)
sog. DDOS (Distributed Denial of Service) Angriffe unter zuhilfenahme von Trojaner-Programmen, die auf einer Vielzahl von gehackten Rechnern installiert wurden

WebServer wurden mit bis zu 100GB an Daten überflutet. Sowohl Verbindungstabellen wurden so gefüllt als auch unzählige Requests auf die WebServer selber und deren Applikationen gestartet.



Beispiele

Bayerischer Rundfunk 2008:

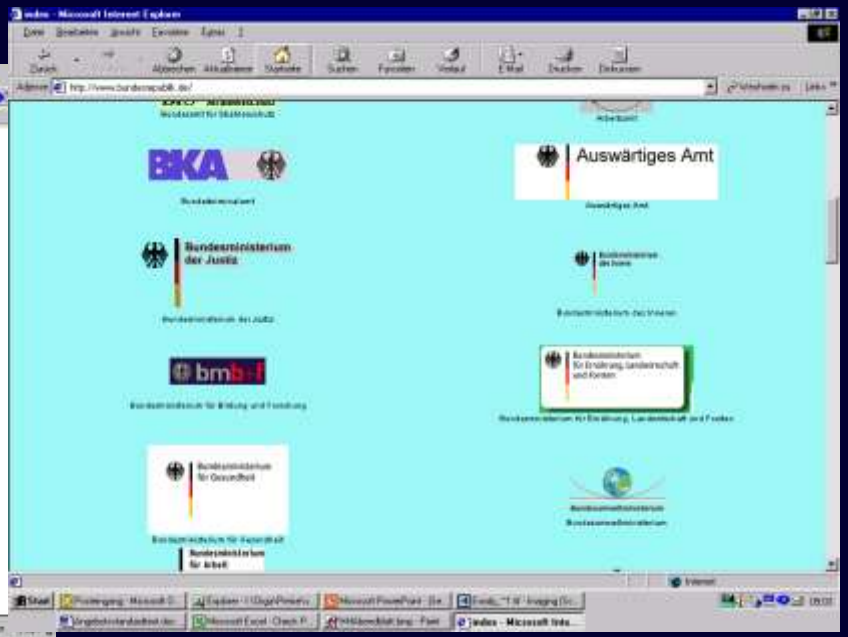
Anhang pornographischer Bilder an e-mails mittels im Hintergrund installiertem „Trojanischen Pferd“
z.B. an CSU, katholische Kirche und Staatskanzlei ...

Beispiele

„I LOVE YOU“

Zerstörung von graphischem Bildmaterial
(Frühjahr 1999 : MELISSA)

Bundesverwaltung, Londoner Unterhaus, Abendblatt Hamburg und weitere unzählige Unternehmen und Internet-user weltweit



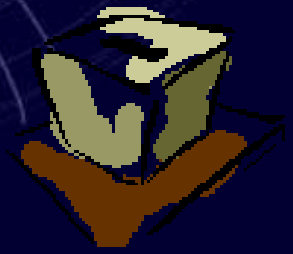
Beispiele

08.11.2000 : Infowar zum US-Wahltag

heise online „News“ :

„Nur wenige Stunden vor Öffnung der Wahllokale in den USA Haben Unbekannte die Website der Republikaner gehackt.

Ein Sprecher der Republikaner bezeichnet den Hack als offensichtlich schmutzigen Trick der Demokraten“



Beispiele

Juni 2010 : Stuxnet

Computerwurm, der zuerst im Iran entdeckt wurde. Speziell zur Überwachung und Steuerung technischer Prozesse der Firma Siemens entwickelt.

IT-Sicherheitsspezialisten gehen davon aus, dass Stuxnet gezielt zur Sabotage iranischer Atomanlagen programmiert wurde. Der Aufwand für den Wurm sei gewaltig und teuer gewesen, zudem richte es nur in bestimmten Anlagen Schaden an, andere würden offenbar ohne Schaden lediglich infiziert.

Frei verfügbare Tools

Stuff-Page - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Vorwärts Abbrechen Aktualisieren Startseite Suchen Favoriten Verlauf E-Mail Drucken Diskussion

Adresse http://www.stuff-page.de/ Wechseln zu Links

Stuff-Page

by Blade & Joseppe

Home Downloads Security Misc Cash 4 Surf Mp 3 Fun Special

0130	Liste gescannter 0130-Server	Unknown
Linux-Tutorial	Erste Schritte unter Linux	FuseFire
Mailbombing	Ein paar Infos über Mailbombing	BSE
Diskettenbombe	Anleitung zum Zerstören von Disketten-Laufwerken	Jolly Roger
FTP	Eine Liste aller gängigen FTP-Befehle	Canaris
ICQ	Anleitung zum unbemerkten Adden eines anderen Users	Unknown
IP	Anleitung zum Herausfinden der IP einer bestimmten Person	DeeP
TCP/IP-Ports	Liste aller gängigen Ports mit Beschreibung	Methos
Mail-Server	Liste von Mail-Servern	Killah Priest
Internet-Zugänge	Mit Hilfe von Trojanern umsonst surfen	Nova-Beast
Telefonleitungen anzapfen	Anleitung zum kostenlosen Telefonieren in Mehrfamilienhäusern	Donald Duck
Telefonkarten	Bastelanleitung zum Erstellen von Endlos-Telefonkarten	Unknown
Testnummern der Telekom	Anleitung wie man seine Leitung überprüfen kann	
Hacking-Tutorial	Umfangreiches Tutorial übers Hacken	Dasro

Wenn ihr Fragen zu den Tutorials habt, fragt bitte die jeweiligen Autoren. Ich habe auch mal wieder Lust, ein Tutorial zu schreiben, allerdings weiss ich noch kein Thema. Vorschläge bitte an Blade!

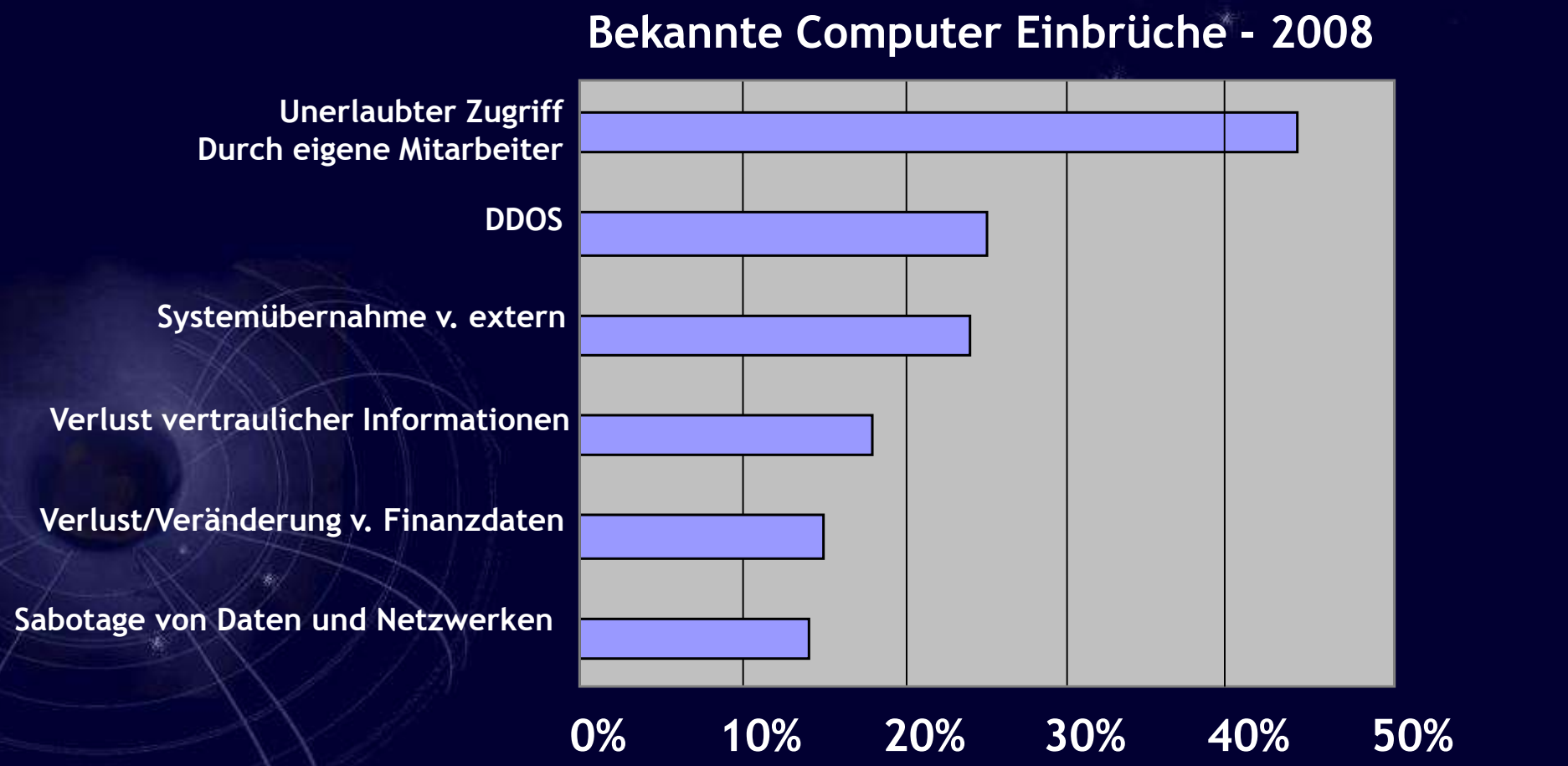
Wir bieten: Preiswürdigkeit, Sicherheit, Service und Spaß!
CYBER PROFIT Anmelden
Primus-Auktion Das große Auktionshaus im Internet!

Internet

Start | Posteingang - Micros... | Explorer - I:\Vertrieb\... | Microsoft PowerPoin... | Exody_~1.tif - Imagin... | Angebotsstandardte... | Microsoft Excel - CPi... | 10:09

sunrise.bmp - Paint | Stuff-Page - Mic... | www.rnc.org - Micro...

Angriffe von intern



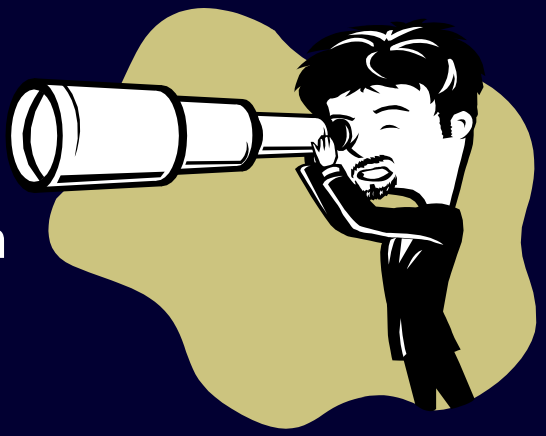
Source: 2008 CSI/FBI
Computer Crime and Security Survey

Angriffe von intern

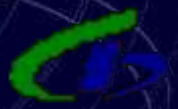
Warum spionieren eigene Mitarbeiter Rechner aus ?

- Neid gegenüber den eigenen Kollegen
- Lukrative Angebote von Adressverkäufern
- Rache am Arbeitgeber oder Vorgesetzten

- Informationsvorsprung erhalten, z.B.
  - Gehälter der Kollegen oder des Vorgesetzten
  - Email traffic des Kollegen („was macht der eigentlich den ganzen Tag ...?)
  - Mobbing
  - Anstehende Kündigungen
  - Anstehende Firmenfusionen etc. ....



VIREN



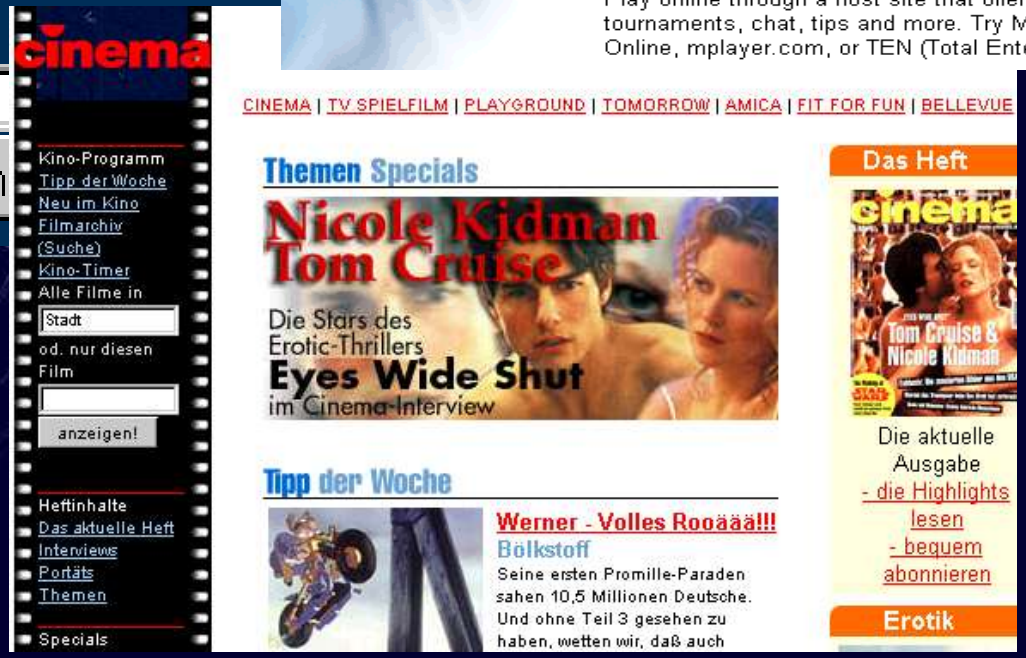
Part.exe

Overheat.exe

VIREN

Sex.com
click here for
SEX.COM's
Sites of the Week
FREE XXX HARDCORE
IN YOUR EMAIL!
Enter E-Mail Here:
Subm

Shopping Cart
Home
Games Catalog
Find Your Fun
Online Games
Tech Support
Membership
Online Games
The excitement is explosive: multiplayer, multimedia gaming on the internet. Play friends. Challenge total strangers. Or test your talents in a tournament. This is the place to find great games for online play.
Games To Play Online
go
See which of our games are designed to play online and all the different ways you can play them. GO...
Game Centers
go
Play online through a host site that offers features like player matching, tournaments, chat, tips and more. Try MSN Gaming Zone, Westwood Online, mplayer.com, or TEN (Total Entertainment Network) GO...


cinema
Kino-Programm
Tipp der Woche
Neu im Kino
Filmarchiv
(Suche)
Kino-Timer
Alle Filme in
Stadt
od. nur diesen
Film
anzeigen!
Heftinhalte
Das aktuelle Heft
Interviews
Porträts
Themen
Specials
CINEMA | TV SPIELFILM | PLAYGROUND | TOMORROW | AMICA | FIT FOR FUN | BELLEVUE
Themen Specials
Nicole Kidman
Tom Cruise
Die Stars des
Erotic-Thrillers
Eyes Wide Shut
im Cinema-Interview
Tipp der Woche
Werner - Volles Rooäää!!!
Bölkstoff
Seine ersten Promille-Paraden sahen 10,5 Millionen Deutsche. Und ohne Teil 3 gesehen zu haben, wetten wir, daß auch
Das Heft
Die aktuelle Ausgabe
- die Highlights lesen
- bequem abonnieren
Erotik

VIREN

Welche Arten von Viren gibt es ?

Bootsektor-Viren

Überträger: Diskette
Opfer: PC‘s mit FD-Laufwerk und DOS/Windows Betriebssystem
Charakteristik: Befällt den Master Boot Record auf der Festplatte
Schaden: gross, da Master Boot Record zerstört oder manipuliert
Gefährdung: Mittel; wenig verbreitet und Schutz durch BIOS Einstellung
Aktuell: Eine neue Variante der Idee stellen VMBRs dar, die beim Rechnerstart eine VM starten Und das vorhandene Betriebssystem in diese hinein laden.

Makroviren

Überträger: Excel, Word Dateien mit Makros
Opfer: PC‘s, Server, LAN‘s durch verstärkten Einsatz von Office-Versionen mit Makro-Funktionalität
Charakteristik: in .doc oder .xls versteckt, infiziert die Dokumentenvorlage (z.B. normal.dot bei Word) und verbreitet sich von da aus weiter
Schaden: enorm gross, da sehr zerstörerisch
Gefährdung: enorm gross, da sehr einfach zu kopieren,zu verändern und zu verbreiten ; zusätzlich Mutationen

VIREN

Welche Arten von Viren gibt es ?

Würmer

Überträger: in E-mail Attachment als ausführbare Datei .exe / .com / .vbs
Opfer: PC‘s, Server, LAN‘s
Charakteristik: Verbreitet sich nach einmaligem Aktivieren selbständig in o.d. Dateien weiter (z.B. „I Love You“ – in .vbs Bilddateien).
Versendet Daten per e-mail selbständig aus dem Adressbuch.
Schaden: extrem gross, da sehr zerstörerisch
Gefährdung: extrem gross, da sich selbst verbreitet

Trojanische Pferde

Überträger: In kleinen Programmen versteckt (z.B. in Bildschirmschonern oder .exe email attachements)
Opfer : PC´s, Server, LAN´s
Charakteristik : Plaziert sich im Hintergrund, ermöglicht das Ausspionieren sämtlicher lokaler Daten oder sogar die Fernsteuerung des Rechners über das Internet. Versendet im Hintergrund beliebig Daten an beliebige Empfänger auf Befehl von aussen.
Ermöglicht komplette externe Kontrolle des Rechners.
Schaden : extrem gross, da sehr zerstörerisch oder kompromittierend
Gefährdung : extrem gross, da der Virus im Hintergrund aktiv ist

VIREN

Welche Arten von Viren gibt es ?

Hoaxes

Überträger: E-mails
Opfer: Empfänger von mails
Charakteristik: Die mail selbst ist der „Virus“
Schaden: gering, aber peinlich und Kosten (evtl. rechtliche Konseq.)
Gefährdung: gross, da jeder verschicken kann und Effektivität senkt
Beispiel: Win a holiday, Good Times

Cookies

- werden von Web-Page Anbietern auf den Rechner des Anwenders abgelegt
- können vom selben Server oder von beliebigem Server wieder ausgelesen werden
- dienen zum Anlegen von Benutzerprofilen im Web
- Datenschutz-rechtlich sehr bedenklich !
- können über Browser deaktiviert werden

Gefahrenquellen

Welche Gefahrenquellen gibt es ?

Bedenkliche/Unerwünschte Web-Inhalte :

Security-Beauftragter von Twentieth Century Fox in USA gab in Interview an, dass die dortigen Mitarbeiter so stark die Möglichkeit nutzen, Radio über das Internet zu hören, dass die verfügbare Bandbreite merklich eingeschränkt wird.

Aussage: „Es käme uns billiger, wenn wir jedem Mitarbeiter ein eigenes Radio zur Verfügung stellten, als weiterhin die exzessive Nutzung des Zuganges für RealAudio Dateien zu akzeptieren...“

Quelle: Elron Software

Gefahrenquellen

Welche Gefahrenquellen gibt es ?

Anwender-Fehler/Programmfehler :

- versehentliches Löschen von Dateien
- unbeabsichtigtes Versenden interner Informationen
- unabsichtliches Versenden von Falschinformationen
- unwissentliches Einschleppen/Aktivieren von Viren
- Verändern von Sicherheitseinstellungen des Browsers
- offensichtlich hinterlegtes Passwort
- wählen trivialer Passwörter
- Hereinfallen auf social engineering
- Aufspielen nicht lizensierter Software auf Firmen-PC
- laufender Rechner über Nacht/Wochenende

Gefahrenquellen

Welche Gefahrenquellen gibt es ?

Anwender-Fehler/Programmfehler

- Schwachstellen in der Software
- Veraltete Software-Versionen sind an der Tagesordnung

- zu geringe Sicherheitseinstellungen in Browsern bieten Angriffspunkte (standard: ActiveX, JavaScript aktiviert)

- überforderte oder schlecht geschulte System-Administratoren
- fehlende Schulungen für User und System-Verantwortliche
- fehlerhafte Konfigurationen (Firewall, Virenscanner etc.)

-Datenvernichtung durch Stromausfall, Brand, Blitzschlag, Plattencrash, Wasserschaden, etc.

Anforderungen an die Security

Diese Gefahren bedeuten neue Anforderungen an die Technologie:

- Zugangskontrolle/Access Control
- VPN/Verschlüsselung
- Virenschutz/ActiveX / Java Scanning
- URL-Blocking, Spam-Filterung, News-Filterung
- Angriffserkennung und Schwachstellen-Analyse
- Kostenzuweisung/ Reporting / Traffic-Analyse
- Hochverfügbarkeit
- Load Balancing/Redundanz
- Authentisierung

Security Policy

Administration/Überwachung
Vorraussetzung : SECURITY POLICY

! Keine Sicherheit ist vollkommen, 100prozentig

! Security muss dynamisch überwacht und angepasst werden

- ✓ **Zentrales Management** ist essentiell, da sonst zu viele Sicherheitslücken und Ausnahmen entstehen
- ✓ Security-Regeln und -Technik müssen ständig auf Aktualität geprüft werden
- ✓ Ungewöhnliche Vorgänge müssen **nachvollzogen** werden
- ✓ **User** müssen angelegt/gelöscht werden
- ✓ **Software-Updates** müssen unternehmensweit verteilt werden
- ✓ Verstösse müssen **festgestellt** werden
- ✓ Security-Technologie sollte **von extern getestet** werden (Penetration Test)
- ✓ Notfallkonzept

Security Policy

Administration/Überwachung bedeutet :

- ✓ Analyse der log files
- ✓ Regelmässiges Backup
- ✓ Abmahnung von Angreifern
- ✓ ggf. Sicherung der Log-Dateien zur Beweissicherung
- ✓ ggf. Nachverfolgung
- ✓ Einspielen von Sicherungskonfigurationen/Backups
- ✓ Wiederherstellen der Verfügbarkeit nach einem Angriff
- ✓ Virensuche und Isolation (Quarantäne Verzeichnis)
- ✓ Sandbox-System / Forensic nach Angriff
- ✓ Honeypot Systeme zur Prüfung bzw. bewussten Ablenkung

VPN – Wofür ?

- Datenübertragung im Klartext ist überall lesbar
- Vertrauliche Daten können unterwegs eingesehen werden
- zu kurze Schlüssel können leicht geknackt werden

Südkoreanisches Schnellzugprojekt 1993

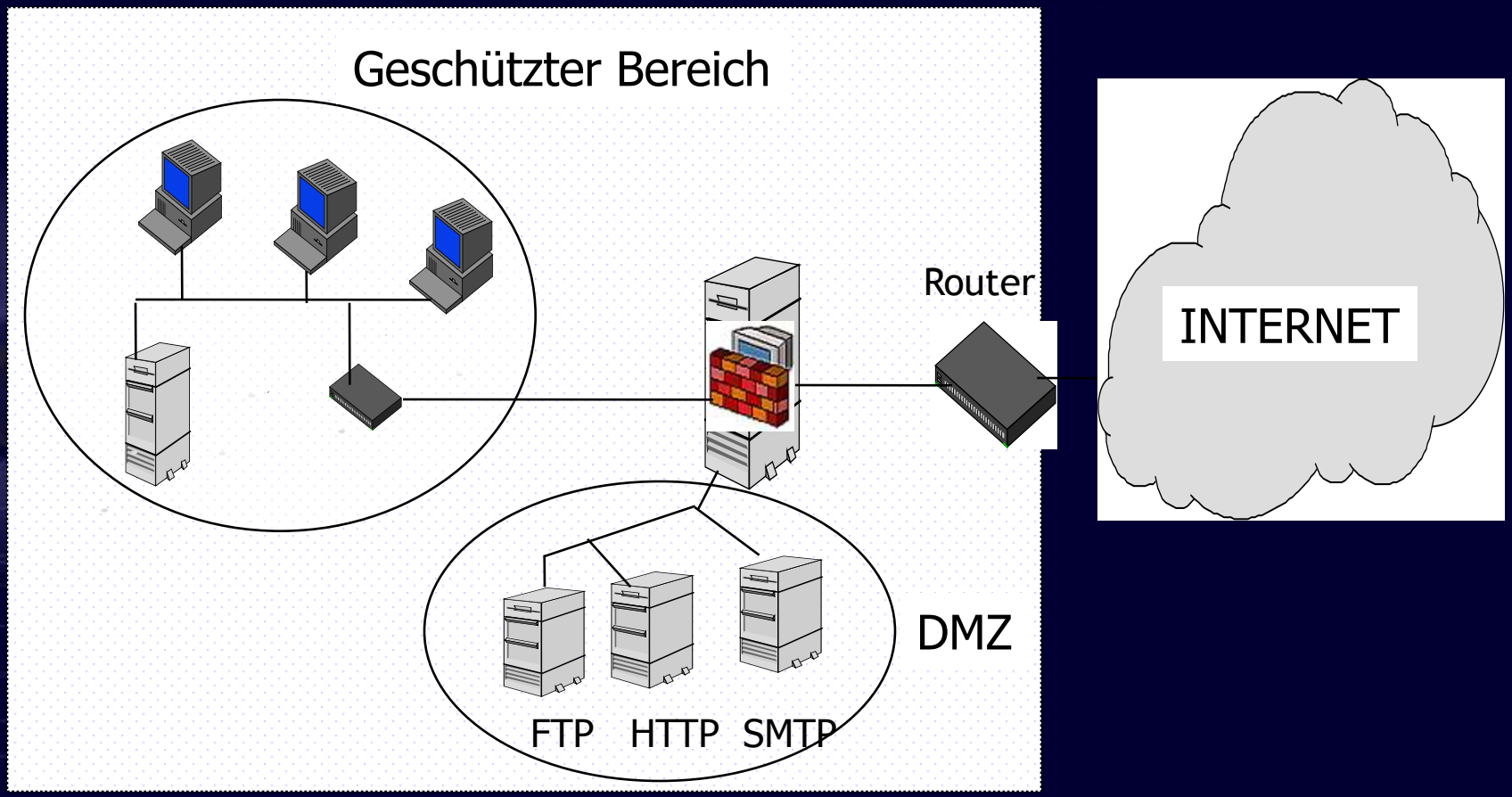
SIEMENS (D) ./. GEC Alsthom (F/GB)

Kommunikationsleitungen (Seoul-Erlangen)
vom DGSE (franz. Geheimdienst) abgehört

--> kurzfristige “Nachbesserungen” des Angebots:
Der Vier-Milliarden-Aufrag für SIEMENS platzt

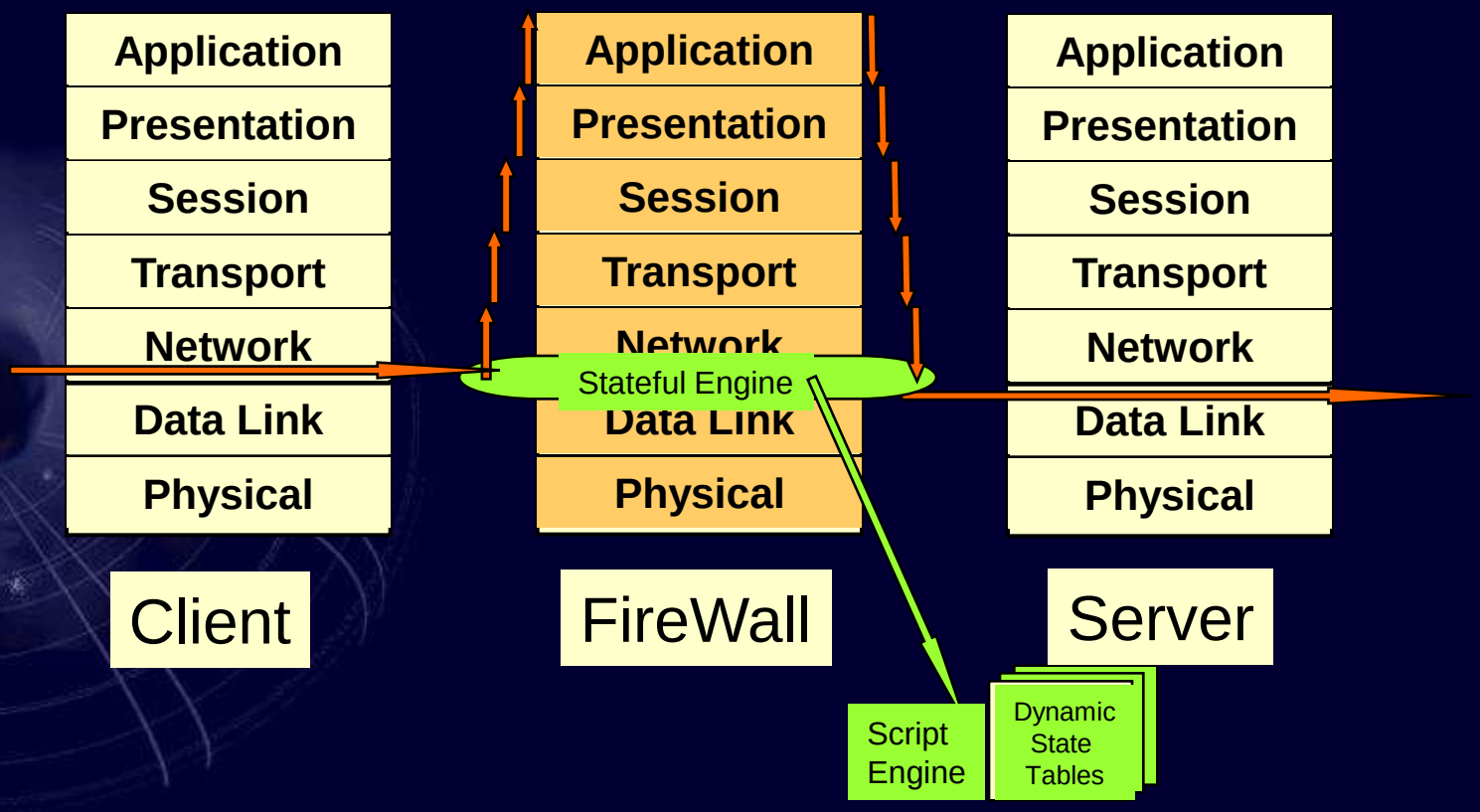
(Quelle: Sicherheit&Management 6/97)

Firewall- und Proxy Lösungen

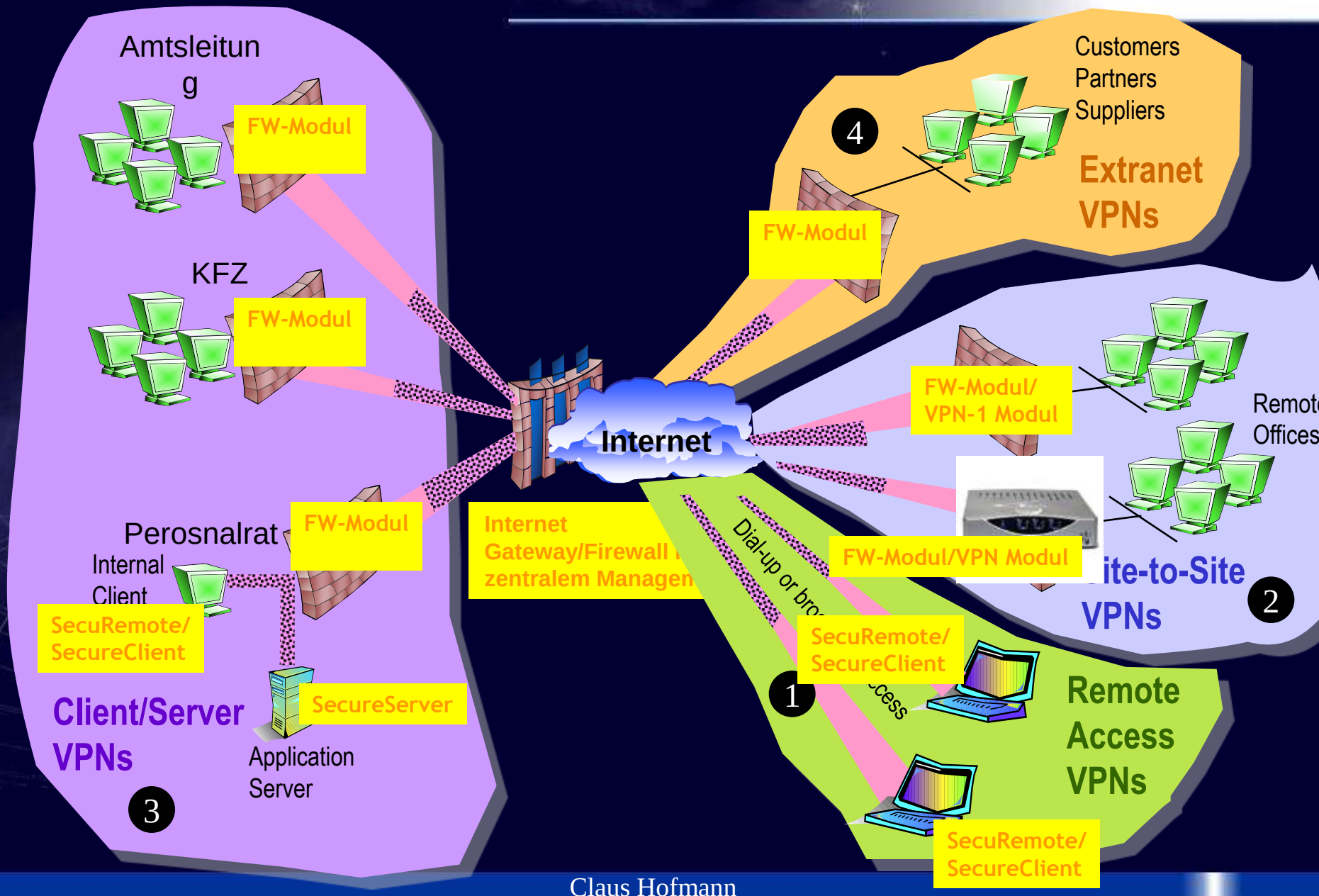


Firewall- und Proxy Lösungen

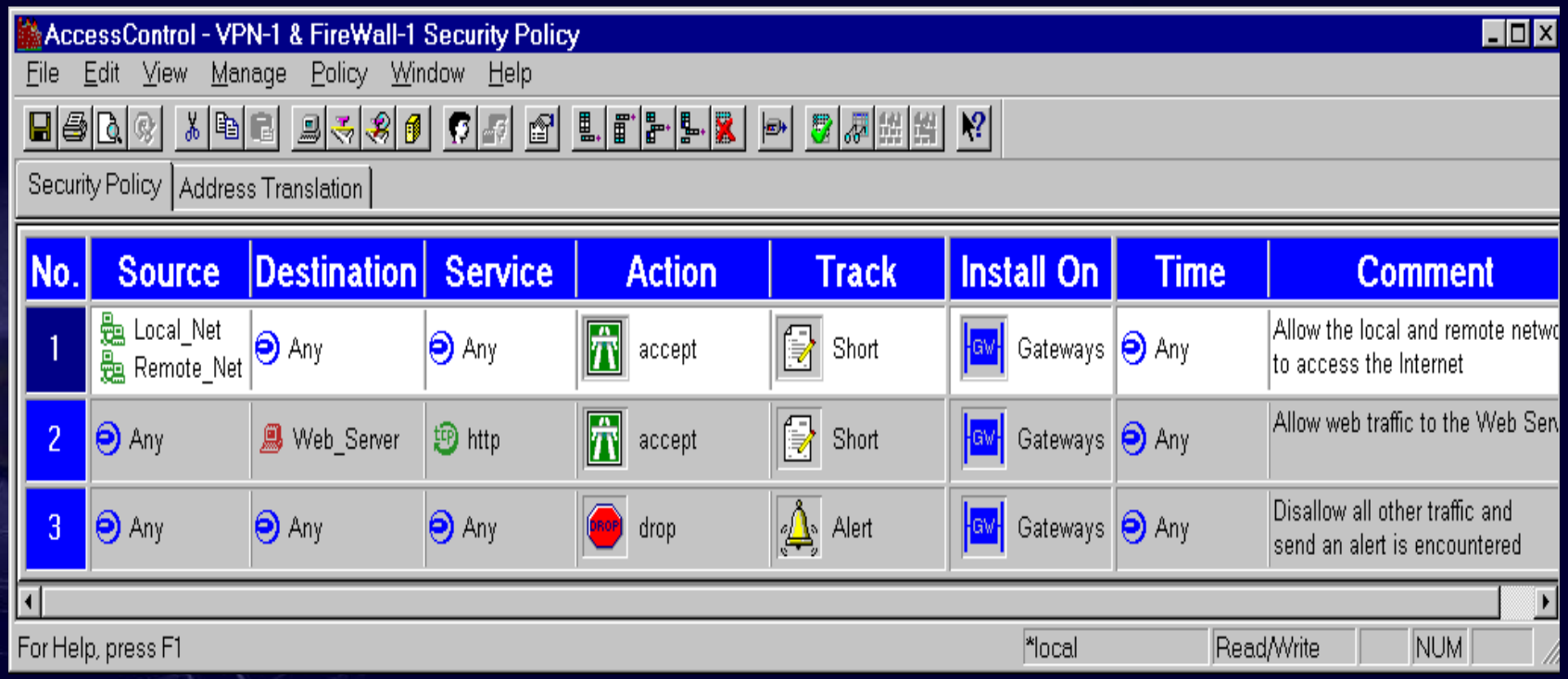
Stateful Inspection / Stateful Multilayer Inspection (SMLI)



Firewall- und Proxy Lösungen



Firewall- und Proxy Lösungen



Virenschutz

Grundsätzliches:

- Virenschutz muss unternehmensweit für alle Eindringungspunkte gewährleistet sein
- muss User-transparent sein
- muss zentral managebar sein
- muss up-to-date sein

Hochverfügbarkeit - Load-Balancing

Grundsätzliches

! Kein System ist 100 %ig verfügbar und ausfallsicher

! FireWall ist „single-point-of-failure“

- ✓Entgangenes Business (z.B. Online-Shop oder -banking), Verlust von Kunden
- ✓Imageverlust
- ✓Verlust an Informationen und Effektivität

Hochverfügbarkeit - Load-Balancing

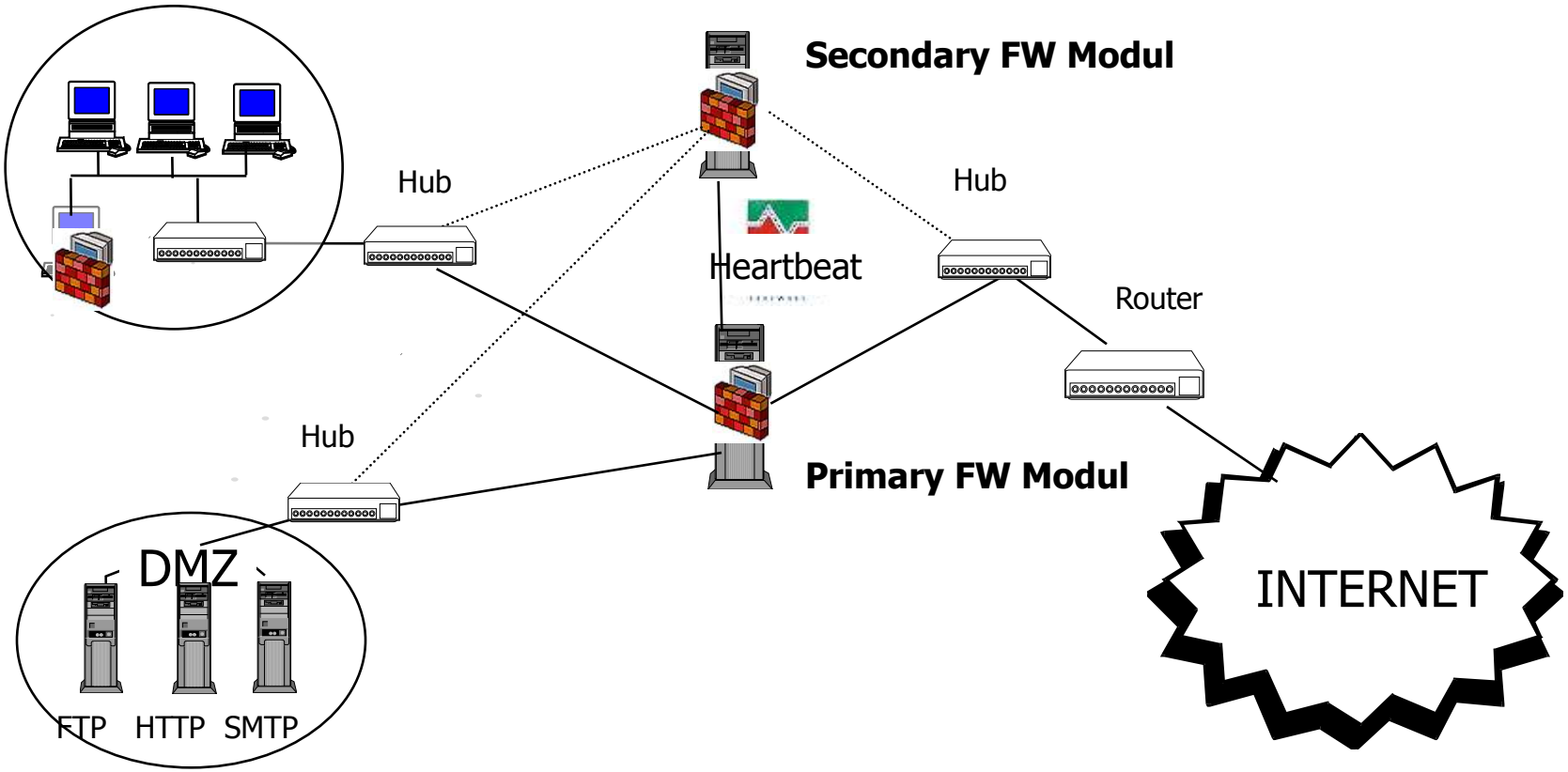
Die Anforderungen :

- Internet Sicherheit und Zugang ohne Ausfallzeiten
- Wartung der FireWall-Systeme ohne Ausfallzeiten
- Übernahme ALLER etablierten Verbindungen
- Verteilung des Traffics auf mehrere Zugangs-Firewalls
- Erweiterungsmöglichkeit (Cluster)

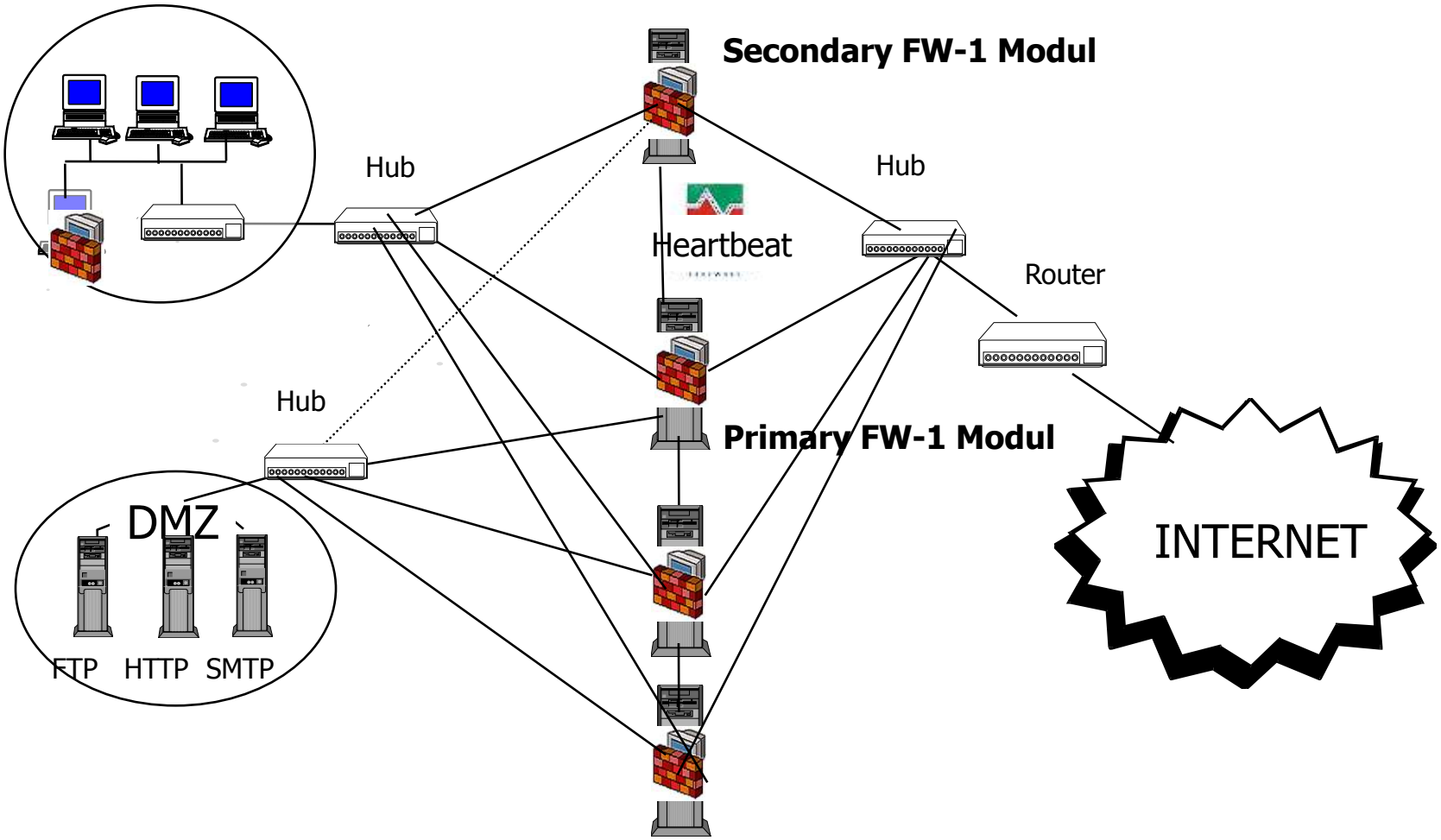
Hochverfügbarkeit - Load-Balancing

- Checkpoint
- Astaro
- GenuGate
- Cisco Pix/ASA
- Microsoft ISA Server
- Defendo
- IPTables
- Sonicwall
- Watchguard
- RedHat Firewall Services

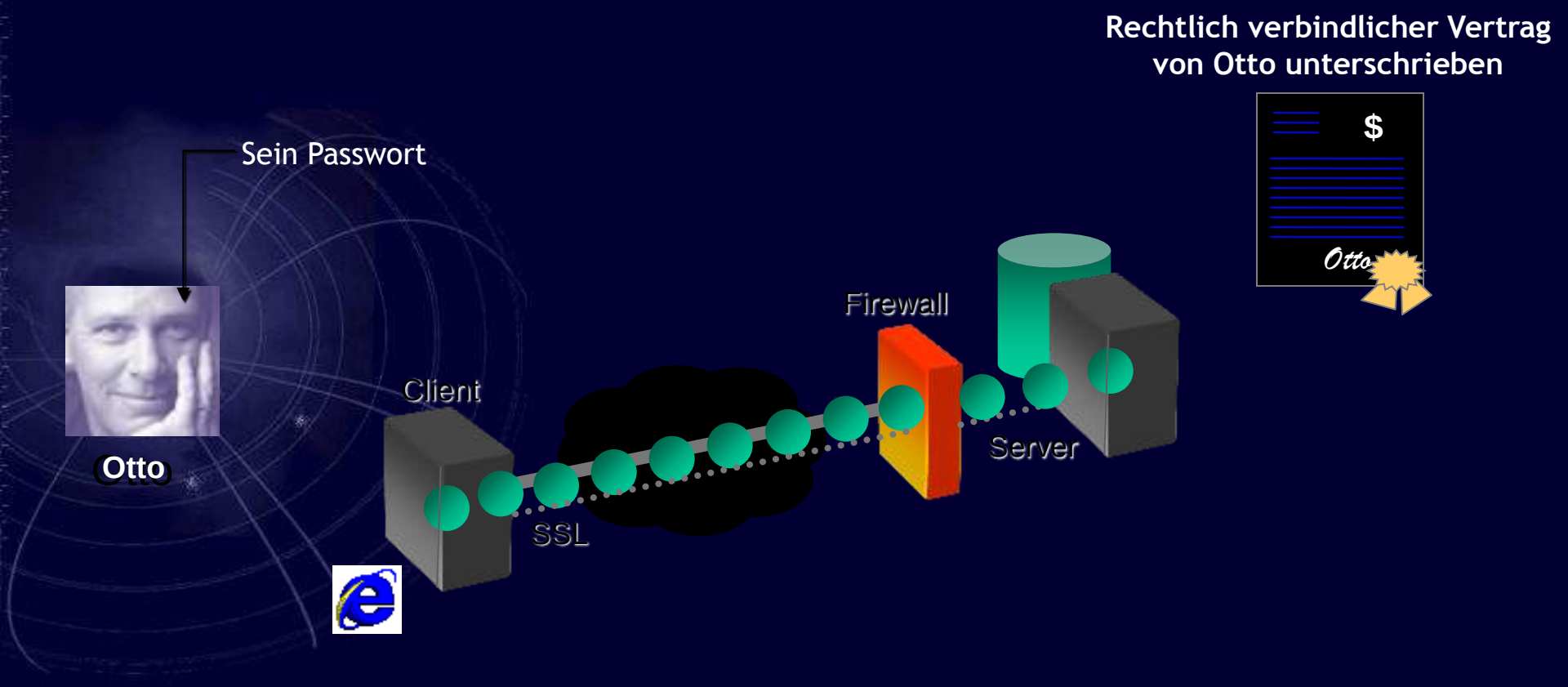
Hochverfügbarkeit - Load-Balancing



Hochverfügbarkeit - Load-Balancing



Authentifizierung – Warum ?



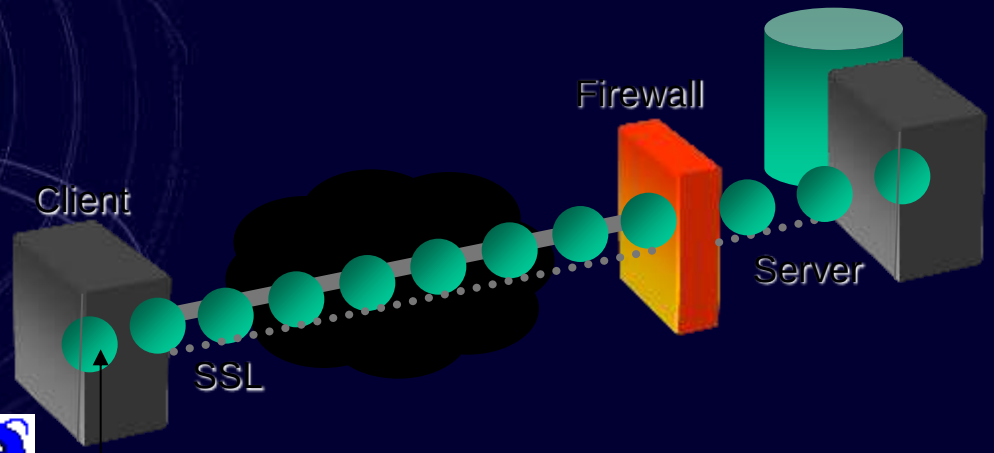
Authentifizierung – Warum ?

Rechtlich verbindlicher Vertrag von Otto unterschrieben

Ottos passwort

Ottos echte Unterschrift

Michael Otto



Authentifizierung

Otto

Wissen → 1. Persönliche Identifikationsnummer (PIN)

Besitz → 2.

Authentifizierung

- Möglichkeiten / Technologien

- statische Passwörter
- dynamische (one-time) Passwörter
- Digitale Signaturen/Zertifikate
- Token
- SmartCard
- Biometrische Verfahren

Datei-Schlüssel

Passwort-1

Passwort-2

Passwort-3

Crypto-Zertifikat

Signatur-Zertifikat

Challenge/Response

Web-Filterung

Warum Web Filterung ?

- **soll keine Mitarbeiter-”Überwachung” sein**
- **soll für User transparent sein**
- **soll Gefahren abdecken**
- **soll Auswertungsmöglichkeiten/Analyse bieten**
- **soll individuell anpassbar sein**
- **Schutz Minderjähriger (Auszubildende) vor gefährlichen Inhalten/Web Seiten**
- **Kostenkontrolle**
- **Schonung von Resourcen (Bandbreite)**

Web-Filterung

Verschiedene Filterlösungen am Markt (Surfcontrol, Websense, Astaro, Ironport, usw.)

- **mit/ohne Virenscanner**
- verschiedene Kategorien wie Gewalt, Glücksspiel etc.
- SSO Lösungen (LDAP, AD, Radius, usw.)
- Die Anzahl der URLs steigt täglich
- URL´s können manuell durch Admin erweitert werden
- Web-basiertes Reporting mit anpassbaren Reports
- Stündliches autom. Update der Kategorielisten oder über Nacht
- Nachvollziehen der HTTP, FTP, Telnet und sonstiger Internetprotokolle nach Nutzer, Gruppe oder Unternehmen

Probleme :

- Geringe Akzeptanz der Mitarbeiter
- False Positive

Verschlüsselung

- **Verschlüsselung lokaler Festplatten/Partitionen (Sektoren)**
  - True Crypt (OpenSource)
  - Steganos Security Suite
  - Utimaco, usw.
  - Verschlüsselung auf Betriebssystemebene
  - Verschlüsselung auf Hardwareebene (BIOS, CryptoCard, USB-Stick)

- **Verschlüsselung via Netzwerk**
  - SSH Tunnel (openssh, usw.)
  - VPN Tunnel (IPSec, Gre, usw.)

Intrusion Detection – Warum überhaupt ?

Mögliche Systemschwächen :

- Konfigurations- und Implementierungsfehler
- Designfehler in Diensten und Anwendungen (z.B. alte Version d. Browsers)
- Fehlverhalten der Benutzer (schwaches Passwort)
- Weil ca. 70 % der Angriffe auf Rechner und Systeme von intern gestartet werden und nicht von extern !!!

Folgen :

- Angreifer erhält Informationen über das anzugreifende Ziel (Erste Angriffe dienen oftmals nur zur Vorbereitung weiterer Angriffe)
- Zugriff auf Netz- und Rechnerresourcen
- Verlust der Verfügbarkeit (Dateien, Internet-Zugang mittels Denial-of-Service)
- Datenvertrauchichkeitsverlust (Verfälschen/Auslesen der Daten während dem Transport oder auf Rechnern)
- Datenechtheitsverlust (Fälschen des Absenders einer e-mail = email spoofing)

Intrusion Detection - Allgemeines

Intrusion-Erkennungs-Systeme besteht aus 2 wesentlichen Komponenten :

Komponente zur Datensammlung

Sinnvolle Quellen sind z.B.

- Von Teilen des Betriebssystems überwachte Komponenenten wie Dateisysteme
- Netzdienste (wer hat sich von aussen angemeldet)
- Log file der Firewalls
- Netzverkehrsdurchsatz (Quell- und Zieladresse) des Datenpaketes etc.

Komponente zur Datenanalyse und Ergebnisdarstellung

Mißbrauchserkennung

Anomalieerkennung

Intrusion Detection - Allgemeines

Missbrauchserkennung :

Ziel : Bekannte Angriffe mittels Signaturen zu identifizieren
Vorraussetzungen :

- Es muss bekannt sein, worauf dieser Angriff basiert (z.B. IP-Paket mit falscher Größenangabe)
- Es muß eine Signatur für diesen Angriff vorliegen
- Die Signatur muß für das ID-System zugänglich gespeichert werden.

Anomalieerkennung :

Ziel : Das System vor noch unbekannten Angriffen zu schützen
Vorraussetzungen :

- Statistische Ansätze (Das System bestimmt „Normalwerte“)
- Logische Ansätze (Zusätzlich zum „Normalverhalten“ werden zeitliche Abläufe berücksichtigt)

Intrusion Detection - Angriffsbeispiele

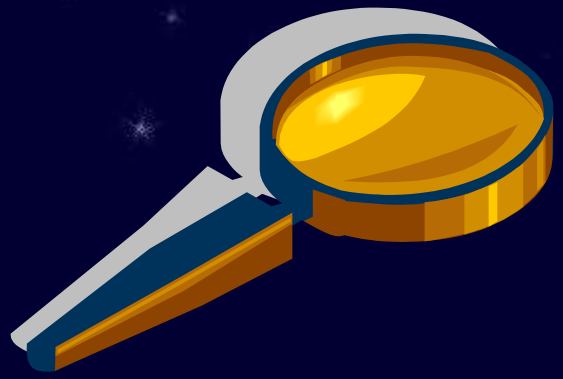
IP Spoofing
Hierbei bringt der Angreifer im IP-Header eine falsche Quelladresse unter. Dies entspricht dem Versenden eines Briefs mit falschem Absender.

Flooding
Hierbei wird das „Opfer“ mit Daten überflutet (z.B. mails)
Ursache für die Wirksamkeit des Angriffs sind meistens Konfigurationsfehler oder auch Schwächen im Selbstschutz der Systemkomponenten

Lauschangriff
Paßwörter, die im Klartext über das Netz versendet werden (email, telnet), können leich
Abgehört werden.

Aktiver Port-Scan
Ein TCP Port Scan ermöglicht es, festzustellen, welche TCP-basierten Dienste ein Zielrechner anbietet

Penetration Test



Penetration Test

- Umfassender “Hack-Test” von aussen und ggf. innen auf ein Unternehmensnetz
- Report-Erstellung mit Schwachstellen-Analyse und Vorschläge für Behebung der Angriffspunkte
- Dienstleistung nur für Partner in deren Auftrag
- Nutzung verschiedenster kommerzieller und frei verfügbarer Tools
- Unabhängige Prüfung z.B. von Firewall-Installation