

Informatik Sicherheit

Folienset „Informatik-Sicherheit“ für



Begriffe

- Sicherheit
- Risiko
- Vertraulichkeit / Verfügbarkeit / Integrität

Was heisst Sicherheit

Sicherheit heisst ***Bewahrung vor Verlust*** (von Leben, Gesundheit, Geld, Sachwerte, ...). Anders definiert kann man Sicherheit auch als ***Gewissheit des korrekten Funktionierens*** definieren.

Was ist ein Risiko

- Eine Kombination aus *Bedrohung* (threat) und *Verletzbarkeit* (Vulnerability).
- Eine Kombination aus *Eintretens- Wahrscheinlichkeit* eines *gefährdenden Ereignisses* und dem daraus resultierenden *Schadenspotential* pro Jahr (Zeiteinheit).
- Gemäss DIN setzt sich das Risiko aus den folgenden beiden Komponenten zusammen:
 - ॐ Das *Schadenausmass* (in sFr.) bei Ereigniseintritt
 - ॐ Die zu erwartende *Häufigkeit* eines *gefährdenden Ereignisses*

Sicherheit gewährleistet

Vertraulichkeit (Confidentiality)

- Einschränkung des Personenkreises auf die Einsichtnahme von Informationen

Verfügbarkeit (Availability)

- Zeitliche und örtliche Bereitstellung von Ressourcen

Integrität

- Richtigkeit / Gültigkeit einer Information



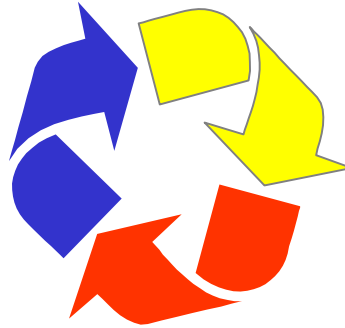
Risk-Management und Sicherheitsstrategie

Allgemeine Gesamtübersicht

Risk Management

Risiko

- Bedrohungen
- Schwachstellen



Verletzbarkeit (Anforderungen)

- gesetzliche und vertragliche Verpflichtungen
- HW/SW Investitionen
- Ordnungsmässigkeit der IT basierten Business-Prozesse

Überprüfung

- Alarmierung / Nachvollziehbarkeit
- Revision / Auditing

Vertraulichkeit
Verfügbarkeit
Integrität

Begriffs-Integration

Vertraulichkeit

Verpflichtungen

DSG
Publikum
Bankengesetz
OR
Geschäfts-
geheimnis

Daten-Pools

Offenlegen

Verfügbarkeit

Investitionen

Server
Workstation
Applikationen
Kommunikation
Datenbanken

appl. Services

Ausfall, Verlust

Integrität

Business-Prozess

Kunden-
Beziehung
Lieferung
Vertrag

Daten-Pools

*Verlust der Ord-
nungsmässigkeit*

Sicherheits-Umsetzung

- **Security Policy**
 - ॐ Commitment der GL
 - ॐ Sicherheits-Gewährleistung
 - ॐ Verantwortungen
- **Weisungen**
 - ॐ verbindlich
- **Richtlinien**
 - ॐ unterstützend
- **Konzepte**
- Umsetzungen in den **Key-Areas**
 - ॐ Physische Sicherheit
 - ॐ Netzwerk Sicherheit
 - ॐ Access Control
 - ॐ Produktions-Sicherheit
 - ॐ Projekt Management
 - ॐ Awareness

Bedrohung und Verletzbarkeit

Bedrohung
durch Risiken
& Kriminalität

Si-Massnahmen

- Physisch
- Netzwerk
- Projekt-Mgmt
- Produktion
- Access Control
- Awareness
- Gesetze
- Organisation

Verwundbarkeit

IT Objekte

- Daten
- Programme
- Server/Netz
- Dokumentation
- Infrastruktur



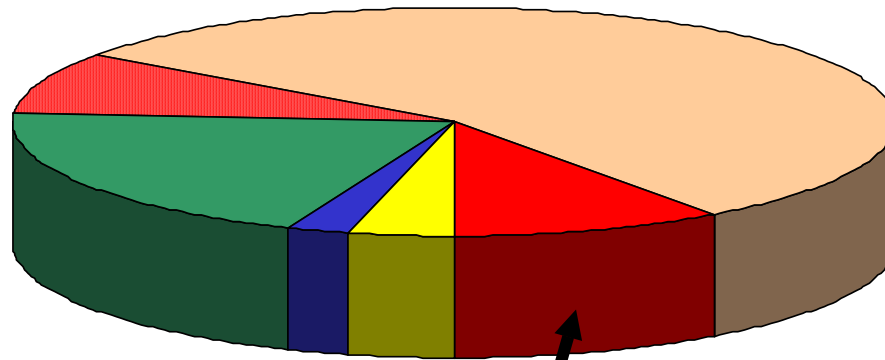
2

Risiko-Beurteilungen

Allgemeine Risiko-Betrachtung

Risiko-Statistik (1)

Allg.
Risiken

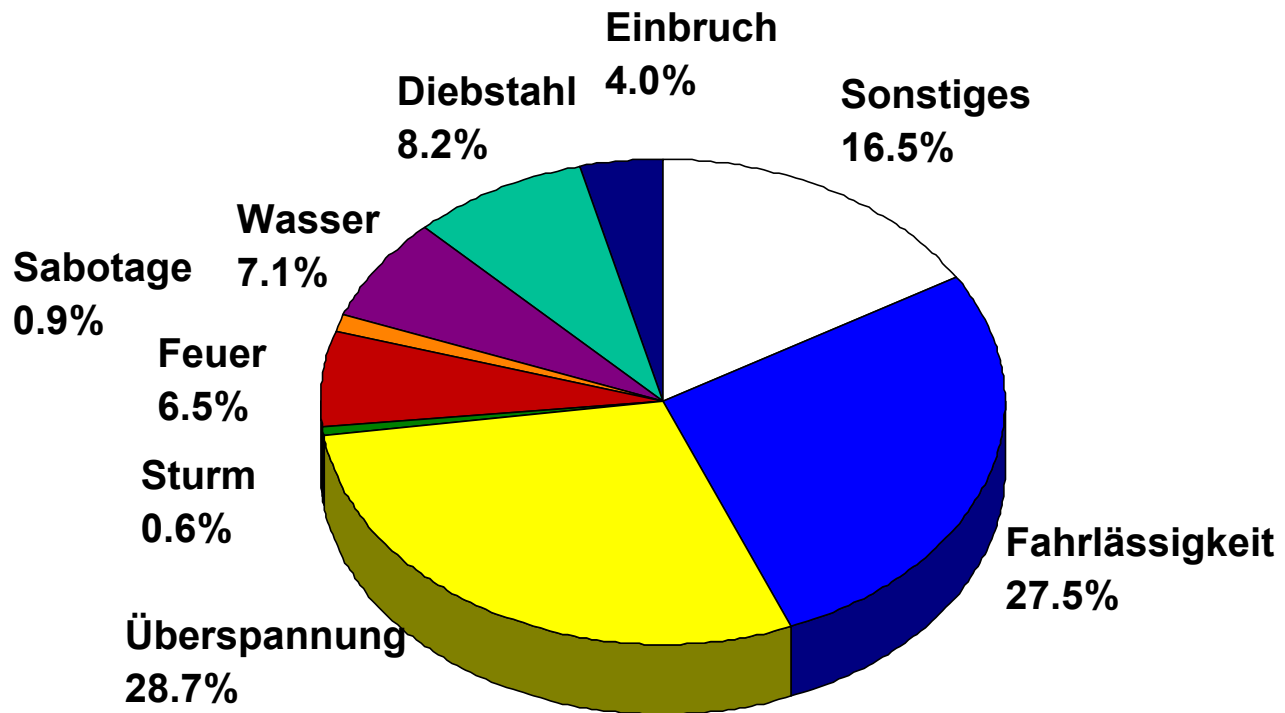


- Viren 4%
- Angriffe von Aussen 2%
- Physische Risiken / Elementarereignisse 20%
- Verärgerte Mitarbeiter 9%
- Menschliche Fehler 55
- Unehrlische Mitarbeiter 10%

Unehrlische MA

Risiko-Statistik (2)

ersicher-
ngs-Optik
on 30'000
chand-
fällen



Bedrohungs-Szenarien

- Risiken

- ॐ Elementar-Ereignisse

- ॐ Technische Vorkommnisse

- ॐ Mensch

- Kriminalität

- ॐ Mensch

- ॐ Firmen-Konkurrenz / Überlebensstrategie

- ॐ Devisen-Beschaffung durch Informations-Angebot

- ॐ Freizeitsportler

- ॐ Geheimdienste / National Security Agency



Allgemeine Sicherheits- Anforderungen

Security Policy

BEKANNT

- Firma mit
 - ☞ Verpflichtungen
 - ☞ Geschäftsprozesse
 - ☞ Informatik-
Investitionen

GESUCHT

- Definition der notwendigen Sicherheits-Levels in bezug auf
 - ☞ Vertraulichkeit
 - ☞ Verfügbarkeit
 - ☞ Integrität

Gesucht: **Bestimmung des IT Sicherheits-Niveaus**

	Vertraulichkeit	Integrität	Verfügbarkeit
Security Policy	Maximal		
	Hoch		
	Mittel		
	Niedrig		
	Firma		

Aussagen gemäss Beispiel

- **Vertraulichkeit (mittel)**

ॐ Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.

- **Integrität (hoch)**

ॐ Die verarbeiteten Informationen müssen korrekt sein, auftretende Fehler müssen erkennbar und vermeidbar sein.

- **Verfügbarkeit (niedrig)**

ॐ Dauernder Ausfall ist zu vermeiden, längere Ausfallzeiten sind jedoch hinnehmbar.

Aufgabenstellung

First Cut in der Projektphase „Vorstudie“

- Auf Projektbasis Beurteilung der Sicherheitsanforderungen bezüglich
 - ॐ Vertraulichkeit
 - ॐ Verfügbarkeit
 - ॐ Integrität
- Einzelarbeit
- Aufwand 20 Min.

A magnifying glass icon with a red handle and a teal lens. The number '4' is written in yellow inside the lens.

4

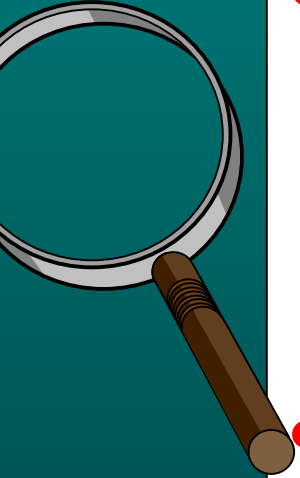
Allgemeine Sicherheits- Massnahmen im Überblick

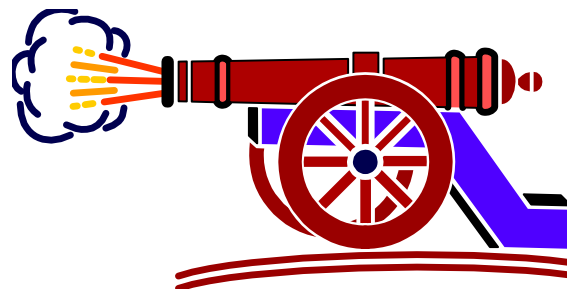
Sicherheitsmatrix mit Gegenüberstellung der Risiken zu den Massnahmen

Risiken	Sicherheitsmassnahmen			Betroffene Ressourcen
	Präventiv	Detectiv	Korrektiv	
	Risiko Analyse Schwachstellen-Analyse Verantwortlichkeitsregelung Access Control Backup / Restore Recovery / Restart Datenverschlüsselung (Strima) Digitale Kennung (MAC, Signature) Berechtigungs-Anträge PC / Notebook Sicherheit Weisungswesen Guidelines Ausweichverfahren (Planung) Daten-Auslagerung Überbrückung / Contingency Netz-Sicherheit (Routine Control) Netz-Sicherheit (Traffic Control) Physische Sicherheit Datenklassifikation Security Awareness and Training	Auditing der Benutzerrechte Auditing der Sicherheitsvorfälle Physische Sicherheit Auditing der SI-Massnahmen Schwachstellen-Analyse Risiko Analyse Plausibilitätsprüfungen Lizenzen- / Virensprüfungen Vollständigkeitsprüfungen Compliance (rechtl. Einhaltung)	Restore Recovery / Restart Ausweichverfahren Wiederanlauf	Daten / Informationen Programme Prozeduren Hardware Betriebssysteme Netzwerk Infrastruktur / Energie
Menschliche Risiken				
- gezielte kriminelle Handlungen auf die DV (Diebstahl, Zerstörung)				
- gezielte kriminelle Handlungen auf die Infrastruktur				
- ungezielte kriminelle Handlungen (Vandalismus)				
- menschliches Versagen, Unterlassungen, Unfälle				
- Streik				
Technische Risiken				
- Ausfälle von Servern, Disks				
- Defekte an Druckern, Tapestationen				
- defekte an der Infrastruktur (Notstrom, Klima)				
Umwelt-Risiken				
- Feuer, Rauch, Löschwasser				
- Erdbeben, Überschwemmung				
- Luftverschmutzung, Chemie-Unfälle				
- Blitz				

präventiv
detection
korrektiv

Aufgabenstellung

- 
- **Gegenüberstellung der Risiken zu den Sicherheitsmassnahmen**
 - ॐ Mit welchen präventiven, detektiven und korrektiven Sicherheits-Massnahmen werden welche Risiken eliminiert / reduziert
 - Erarbeiten der Aufgabenstellung zu Hause



Schwachstellen

Angriffstechniken

Computer-Kriminalität

Gesetzliche Normen

Datenschutz

Risiko-Analyse

Schwachstellen

- **Schwachstellen im Programmdesign**
- **Sicherheitsrisiko Unternehmensorganisation**
- **Sicherheitsrisiko Zugangsberechtigung**
 - **☞ Schwache Authentifikation (Passwörter)**
- **Sicherheitsrisiko Kommunikationsprotokolle**
- **Sicherheitsrisiko Internet-Applikationen**
- **Sicherheitsrisiko Informationsdienste**

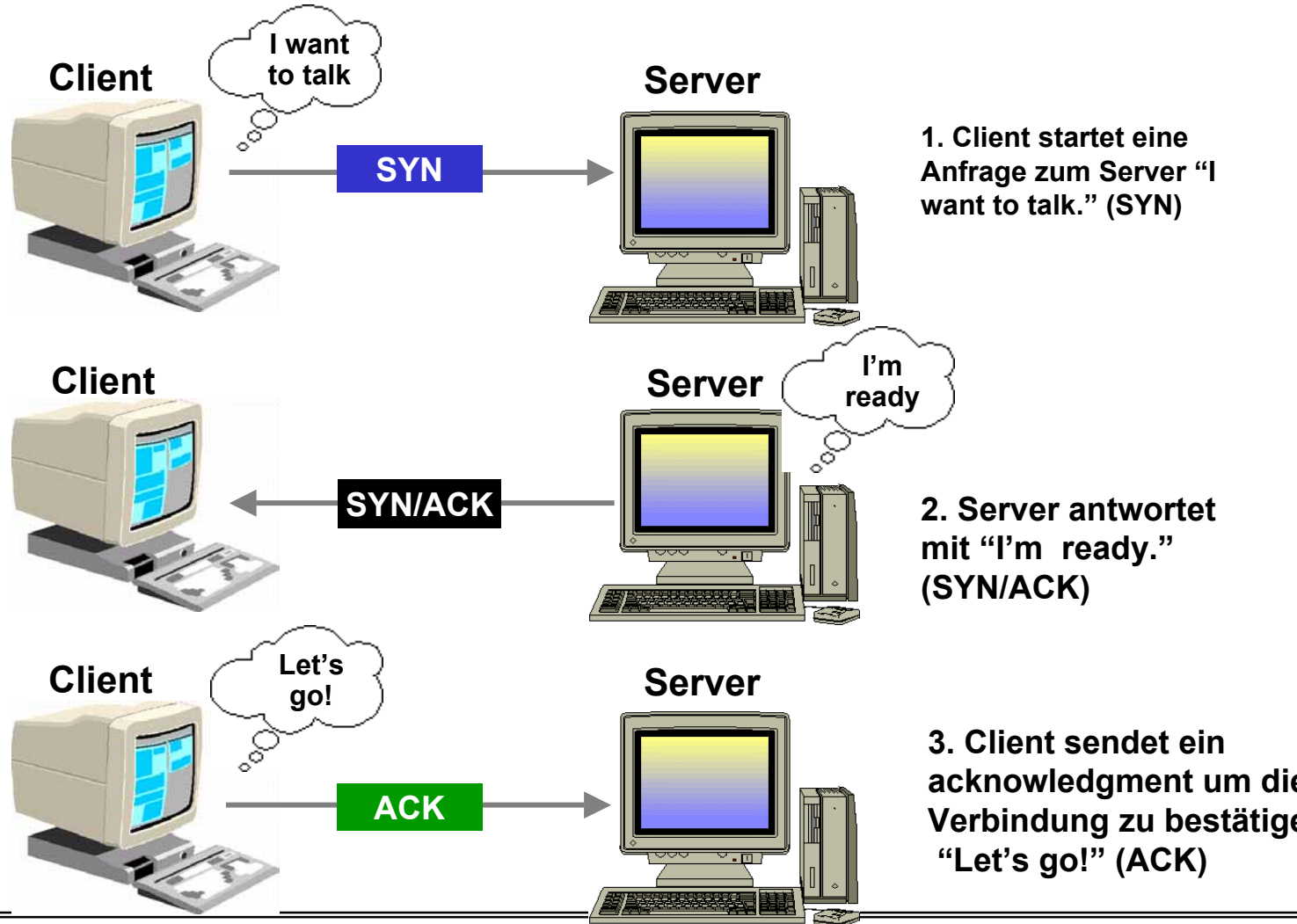
Passwort Knack-Programm „Cracker-Jack“

- Permutationen des User-Accounts “Billy The Kid”. Es gibt 4 Manipulationsebenen:
 - ॐ **Jedes Wort**
“Billy” “the” “Kid”
 - ॐ **Kombinationen von zwei Wörtern**
“BillyThe” “BillyKid” “TheBilly” “TheKid”
 - ॐ **Kombination eines Wortes und bis zu zwei Initialen**
“BillyTK” “BillyKT” “TKBilly” “TbillyK” “Bkid”
 - ॐ **Kombination von Teilstrings aus bis zu drei Wörtern**
“BiThKid” “BillKi” “BilTheKi” “TheBillyK” “BTK”

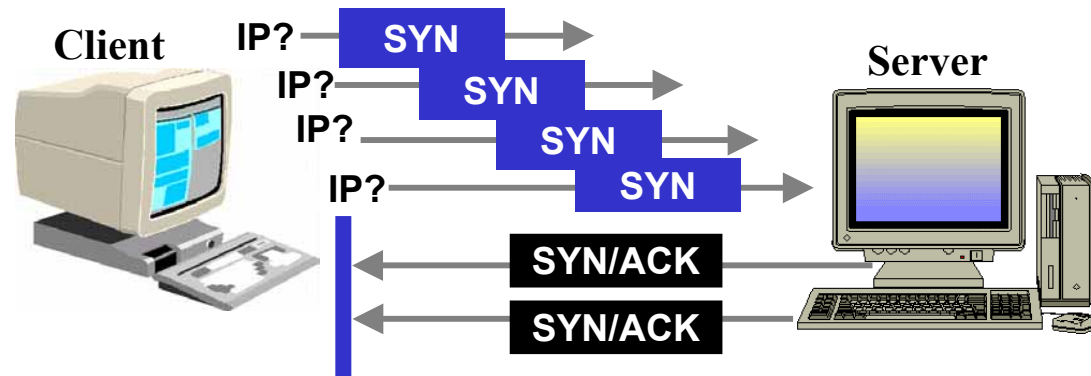
Angriffe auf dem TCP/IP Protokoll

- Das Programm RealSecure der Firma ISS erkennt heute ca. 160 Angriffsvarianten auf dem TCP/IP (www.iss.com). Einige davon sind:
 - Internet Adress Spoofing
 - TCP Sequenznummern Angriff
 - ICMP Angriffe
 - IP Fragment Angriff
 - Internet Routing Angriff
 - Broadcast Stürme
 - UDP Spoofing

SYN Flooding



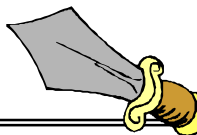
SYN Flooding



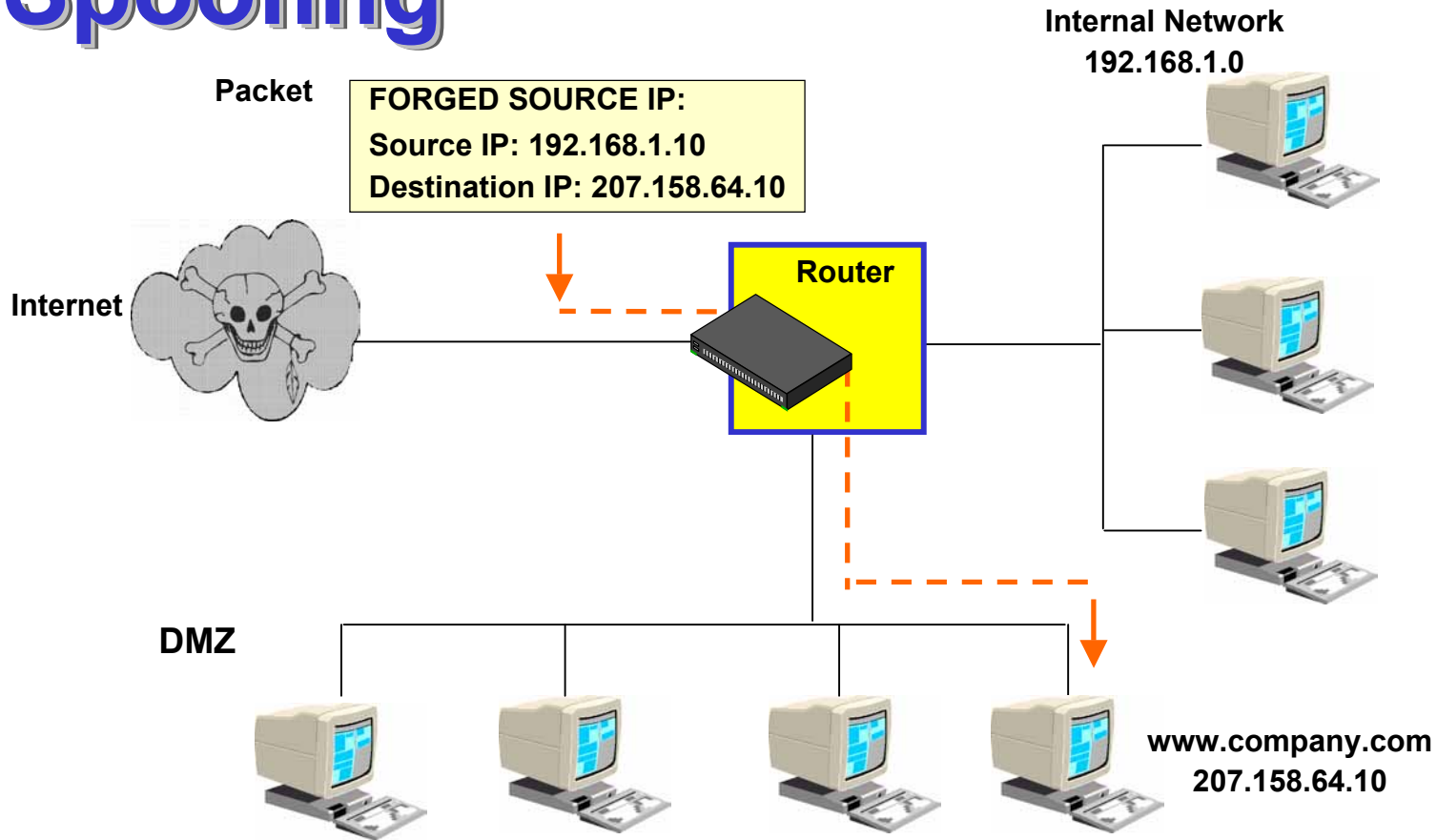
1 Client attackiert den Server durch eine Flut von SYN Paketen mit falscher Absende-Adresse (spoofed IP address)

2 Der Server sendet SYN/ACK Antworten zu einer nicht erreichbaren IP Adresse.

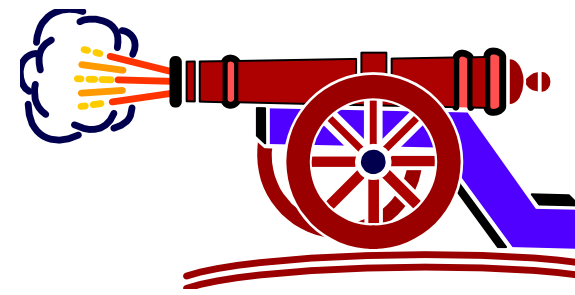
3 Ein ACK wird nie vom Client empfangen.



Spoofting



Der Hacker bringt ein IP Paket durch den Router und ACL, in dem er vortäuscht, das Paket komme von geschützten, inneren Netzwerk.



Computer-Kriminalität / Gesetzliche Normen

Computer-Kriminalität

- Alle Sachverhalte, bei denen die EDV Tatmittel und / oder Tatobjekt ist und die den Verdacht auf eine Straftat begründen.
- **Achtung:** Komputer Kriminalität abgrenzen gegenüber Fahrlässigkeit oder unsachgemäßes Handeln

Computer-Kriminalität

Urkundenfälschung (StGB 251)

- ... eine Urkunde fälscht oder verfälscht, die echte Unterschrift oder das echte Handzeichen eines anderen zur Herstellung einer unechten Urkunde benützt ...
 - Unrichtige Eingabe;
 - Missbräuchliche Veränderung von gespeicherten Daten durch Löschen, Zufügen oder Ändern;
 - Fälschen von unterschriftsanaloge Kennzeichen auf Datenträger und Ausdruck;
 - Unrichtige Programmgestaltung;
 - Eingriffe in den Ablauf der Datenverarbeitung;
 - Veränderung von Karten (Chip-, Code-, Geld- und Wertkarten, die als elektronisches Zahlungsmittel dienen);
 - Manipulation in der Output-Phase.

Computer-Kriminalität

Unbefugte Datenbeschaffung (StGB 143)

- Wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, sich oder einem anderen elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

Computer-Kriminalität

Unbefugtes Eindringen in ein Datenverarbeitungssystem (Hacking) (StGB 143bis)

- Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungs-Einrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

Computer-Kriminalität

Datenbeschädigung (StGB 144bis)

- Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.
- 2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.
- Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

Computer-Kriminalität

Betrügerischer Missbrauch einer Datenverarbeitungsanlage (StGB 147)

- Wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

Computer-Kriminalität

Erschleichen einer Leistung (StGB 150)

- Wer, ohne zu zahlen, eine Leistung erschleicht, von der er weiss, dass sie nur gegen Entgelt erbracht wird, namentlich indem er ein öffentliches Verkehrsmittel benützt, eine Aufführung, Ausstellung oder ähnliche Veranstaltung besucht, eine Leistung, die eine Datenverarbeitungsanlage erbringt oder die ein Automat vermittelt, beansprucht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

Zusammenfassung gesetzlicher Normen

- Datenschutzgesetz (DSG, VDSG)
- Urkundenfälschung (StGB 251)
- Datenspionage (StGB 143)
- unbefugtes Eindringen (StGB 143bis)
- Datenbeschädigung (StGB 144bis)
- betrügerischer Missbrauch der DV-Anlage (StGB 147)
- Erschleichen einer Leistung (StGB 150)

Gesetzliche Pflichten

- Der Gesetzgeber verlangt im Gesetzestext auch die „besondere Sicherung“ der Daten (bspw. StGB 143). Ansonsten wird das Strafmass für den Täter reduziert.
- Unter „besondere Sicherung“ versteht man einen genügenden Schutz gemäss heutigem Verständnis (bspw. gemäss Code of Practice)

Gefahren durch einen Internet Anschluss

Eindringen von nichtautorisierten Personen:

- Einfügen, löschen und verfälschen von Daten
 - ◌ Verlust von vertraulichen Informationen
 - ◌ Störung der Netzverfügbarkeit
- Einschleusen von trojanischen Pferden und Viren

Unternehmen die am Internet angeschlossen sind werden im Durchschnitt 8-mal so häufig angegriffen wie Unternehmen ohne Internet Anschluss.

JSA: Erkannte Testangriffe

38'000 Angriffe untersucht

25'000 erfolgreich (65%)

13'000 abgewehrt (35%)

1'000 bemerkt (3%)

24'000 nicht bemerkt (62%)

267 berichtet (< 1%)

721 nicht berichtet (>2%)

HIP97

- **HIP´97: Hacking in Progress**

 - **ॐ Notizen aus dem Hackerzeltlager**

- **Hacker brauchen Phantasie, um neue Schleichwege in Rechnersysteme zu erkunden. Sie zeigen sie aber auch bei der Gestaltung ihrer Zusammenkünfte: Vier Jahre nach dem legendären `Hacking at the End of the Universe´ (HEU) verwandelten sie vom 8. bis 10. August einen niederländischen Zeltplatz in das vielleicht größte zivile Freiluftnetzwerk aller Zeiten.**

http://www.heise.de/ct/art_ab97/9710066/ oder <http://www.hip97.nl/notice.html>

CCC 1999

Camp Press Review

INTERNATIONAL ARTICLES

Computerworld

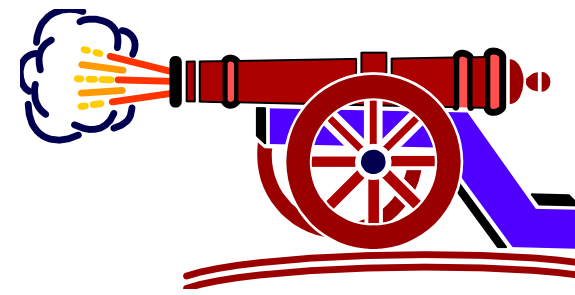
- Reporter's notebook: Hackers on holiday [[pdf archive](#)]
<http://www.computerworld.com/home/news.nsf/all/9908102chaos>
- Hacking your way to an IT career [[pdf archive](#)]
<http://www.computerworld.com/home/news.nsf/all/9908124hackcareers>
- Hackers, IT consultants embrace free security tool [[pdf archive](#)]
<http://www.computerworld.com/home/news.nsf/all/9908124swan>

GERMAN ARTICLES

- Hacken im Sommercamp - Der Chaos Computer Club rief und etwa tausend Hacker und Cypherpunks kamen [[pdf archive](#)]
<http://www.tagesspiegel.de/archiv/1999/08/08/ak-in-ne-10733.html>

Konklusion

- Dauernde Änderung der Bedrohungs-Szenarien durch
 - ॐ Vernetzung
 - ॐ Politischer Wandel
 - ॐ Ethische Vorstellungen
 - ॐ Profitgier
- Vor was schützen wir uns letztlich?



Datenschutz

Datenschutzgesetz (DSG)
Verordnung (VDSG)

Besonders schützenswerte Personendaten

- Religiöse, weltanschauliche, politische und gewerkschaftliche Ansichten oder Tätigkeiten
- Gesundheit, Intimsphäre oder Rassenzugehörigkeit
- Massnahmen der sozialen Hilfe
- administrative oder strafrechtliche Verfolgungen und Sanktionen
- Persönlichkeitsprofil, das eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben

Bearbeiten

Jeglicher Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das

- ॐ Beschaffen
- ॐ Aufbewahren
- ॐ Verwenden
- ॐ Umarbeiten
- ॐ Bekanntgeben (Zugänglichmachen von Personendaten wie
 - Einsicht gewähren
 - Weitergeben
 - Veröffentlichen
- ॐ Archivieren
- ॐ Vernichten

Bearbeitungsgrundsätze der Personendaten

- Rechtmässige Beschaffung der Daten
- Bearbeitung nach Treu und Glauben
- Bearbeitung gemäss Angabe bei der Beschaffung
- Vergewissern nach der Richtigkeit
- Auskunftsrecht und Berichtigung
- Keine Gefährdung im Ausland
- Datenschutz

Datenschutz

- Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7)

Risiken der Daten

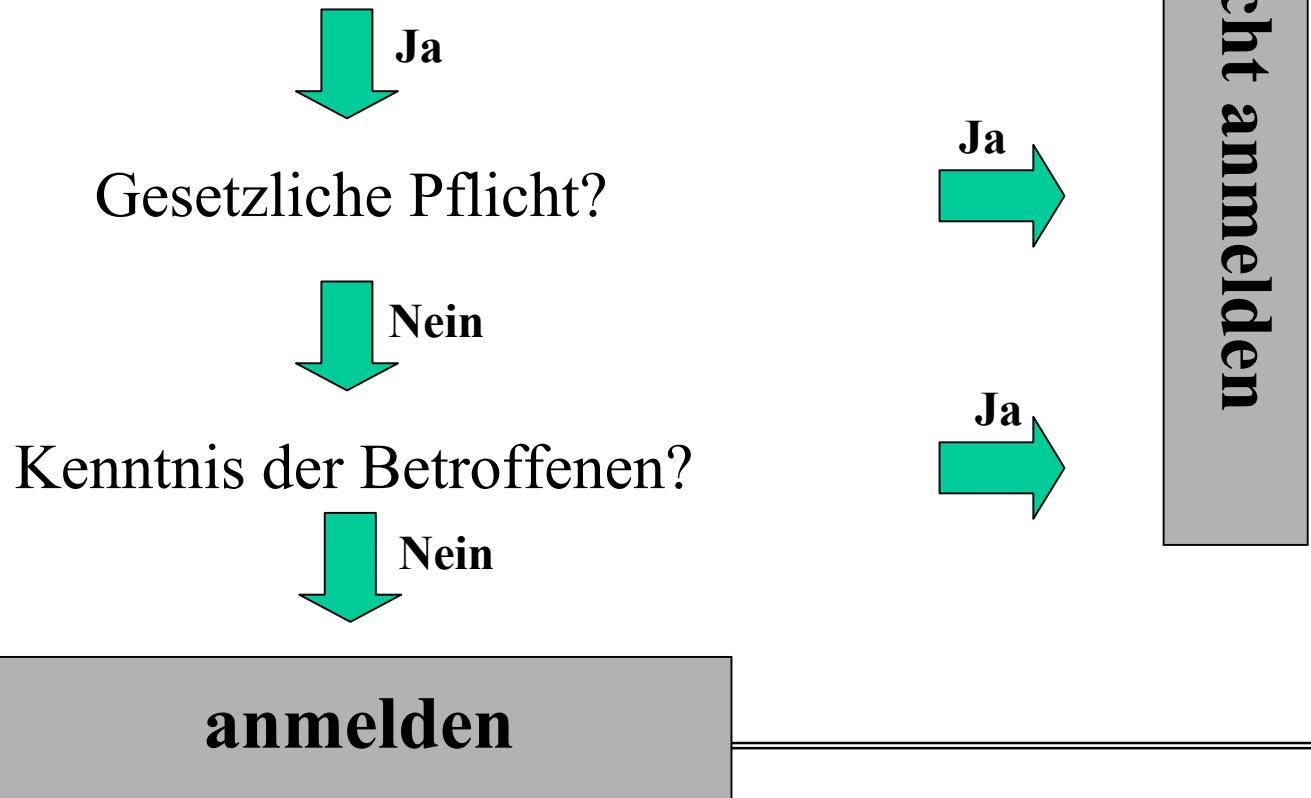
- unbefugte oder zufällige Vernichtung
- zufälliger Verlust
- technischer Fehler
- Fälschung, Diebstahl oder widerrechtliche Verwendung
- unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen

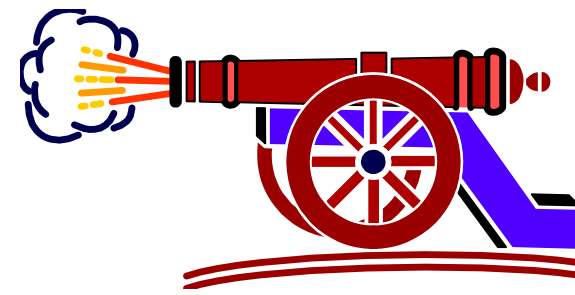
Massnahmen zum Schutze der Personendaten (Art. 8 VDSG)

- **Zugangskontrolle** (physische Sicherheit)
- **Personendatenträgerkontrolle** (Schutz der Datenträger)
- **Transportkontrolle** (Netz-Sicherheit)
- **Bekanntgabekontrolle** (Identifikation des Empfängers)
- **Speicherkontrolle** (Schutz vor Einsicht und Veränderung)
- **Benutzerkontrolle** (Nutzung von DV-Systemen)
- **Zugriffskontrolle** (nur berechtigte Personen haben Zugriff)
- **Eingabekontrolle** (Protokollieren der Einsichtnahme)

Anmelden der Datensammlung

Regelmässige Bearbeitung von besonders schützenswerten Daten oder Personalprofilen oder Bekanntgabe an Dritte





Risiko Analyse

- Systemabgrenzung
- Erfassen der Risiken
- Bewerten der Risiken
 - ॐ Häufigkeit / Wahrscheinlichkeit
 - ॐ Schadenausmass
- Auswerten des Ergebnisses

Systemabgrenzung

- Was gehört zu meinem Betrachtungsfeld
- Welches sind die zu schützenden Objekte
 - ॐ Datenpools (Vertraulichkeit)
 - ॐ Prozesse (Integrität)
 - ॐ HW / SW Investitionen (Verfügbarkeit)
- Welchen Risikobereich beurteile ich
 - ॐ Netz
 - ॐ Backup
 - ॐ

Erfassen der Risiken

- **Welches Risiko wirkt auf welches Objekt wie**
- **Welche Risiken werden durch bestehende Sicherheits-Massnahmen wie stark reduziert bzw. eliminiert**

Bewerten der Risiken

- **Welche Risiken sind**
 - wahrscheinlich / eher wahrscheinlich
 - nicht wahrscheinlich
- **Streichen der „nicht wahrscheinlichen“ Risiken**
- **Welche Situationen machen es möglich, dass die Risiken grössere Schäden verursachen**
- **Streichen der Risiken kleiner Schäden**

Auswerten der Ergebnisse

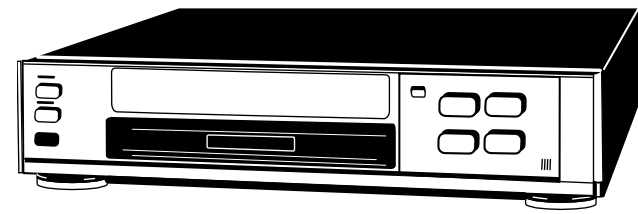
- Zu erwartende Schäden (sFr.)
- Aufwände für die notwendigen Sicherheitsmassnahmen
 - ॐ Kosten
 - ॐ Aufwände
- Gegenüberstellung / Pay Back
 - ॐ lohnt sich (nicht)
 - ॐ Outsourcing

Aufgabenstellung

Risiko-Analyse

- Die Firma GigaToys will einen Internet-Anschluss realisieren. Sie sind beauftragt, eine kleine Risiko-Analyse dieses Anschlusses durchzuführen. Als Resultat stellen Sie die Kosten den möglichen Schäden gegenüber.
- Gruppenarbeit
- Aufwand 20 Min.





Netzwerk Sicherheit

Allgemeine Übersicht

Was ist ein Netzwerk?

Übersicht

- Sammlung von Computer-Systemen innerhalb eines oder mehrerer Gebäude an gleichem Standort
- Verbunden miteinander, um gemeinsam Informationen, Programme, Printer, etc. zu teilen.

Services im LAN

- File Services (Novell)
- Applikations-Services (Unix, NT, MVS)
- Media Services (CD ROM, Printer, FAX)
- Connectivity Services (Router, Gateway, Firewall)

Netzwerk Management

- Monitoring des Verkehrs auf dem LAN (Sniffer)
- Identifikation und Lösung von Kommunikations-Problemen (Alerts)
- Remote Konfiguration von Kommunikations-Systemen
- Zentrale Konfigurations-Datenbank mit Benutzer-Informationen und Software

Übertragungs-Technologie

- Transmission (Layer 2)
 - ॐ Ethernet
 - ॐ Token Ring
 - ॐ FDDI
- Jede Meldung wird an jede Station innerhalb des LAN's gesendet
- Jede Station kann jede Meldung auf dem gleichen LAN-Abschnitt abhören

Warum LAN Security

Personal

**Erfahrung
Awareness
Verantwortungs-Regelung**

Communication

**Modems
Zugriffe zu internen /
externen Services**

PC

**Unsichere PC's
Fehlende Backups
Viren**

Gebäudeschutz

Physischer Zutritt

Technik

**Fehlende Standards
Übertragungs-Verletzungen**

Hauptrisiken auf dem Netzwerk

Vertraulichkeit

- Mitlesen vertraulicher Informationen

Integrität

- Verfälschung einer Meldung
- Wiedereinspielung einer Meldung

Verfügbarkeit

- Ausfall / Instabilität von Netzwerk-Komponenten

Baseline Controls

Baseline controls für die Informatik-Sicherheit sind ein Set von Massnahmen, mit denen man eine mittlere Sicherheit erreicht:

ॐ Unternehmensweite Baseline Controls

- Sicherheits-Verantwortung
- Hardware / Software Standards

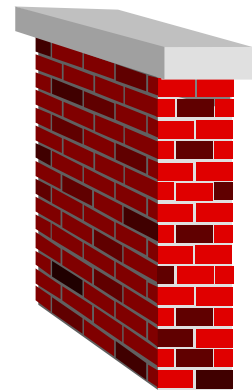
ॐ Baseline-Controls für ein individuelles LAN

Baseline Controls für ein individuelles LAN

- LAN Administration und Betrieb
- Access Control
- Physische Sicherheit
- LAN Konfiguration
- LAN Applikationen
- Business Continuity Planning
- Virus-Protection

Verantwortung für die Baseline Controls

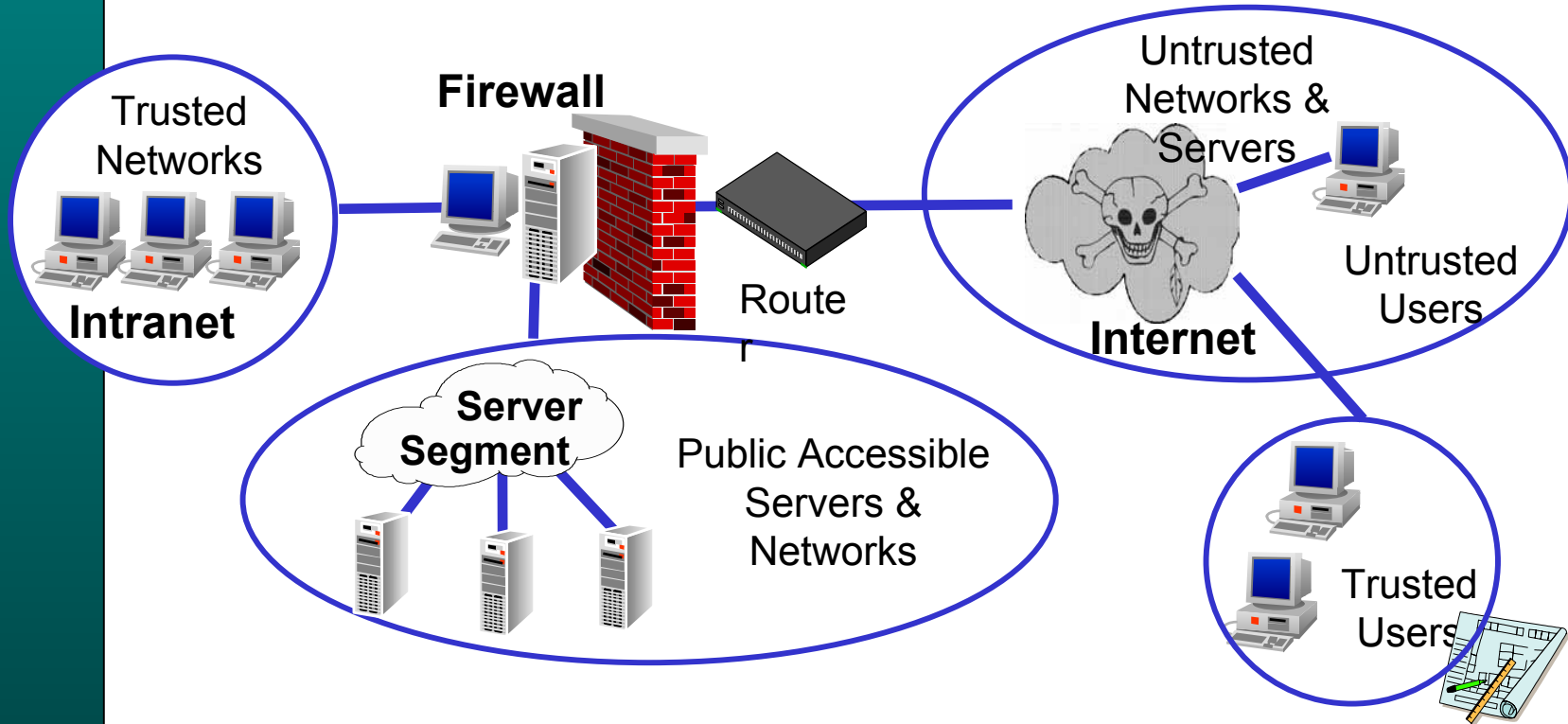
- Zentraler Security Manager
 - ॐ Koordination der Sicherheits-Massnahmen
- LAN Owner
 - ॐ Business-Manager als User
- LAN Administrator
 - ॐ Verantwortlicher für Betrieb, Unterhalt und Sicherheit des LAN's
- LAN Installateur
 - ॐ Verantwortlicher für LAN-Konfiguration, Hardware und Interconnectivity mit anderen LAN's



Netzwerk-Sicherheit

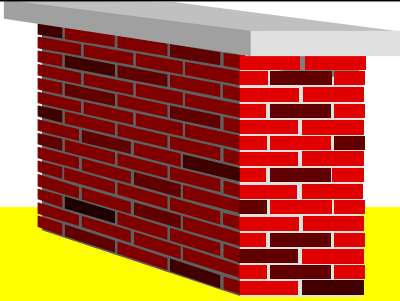
Firewall-Technologie

Übersicht Netzeintritt



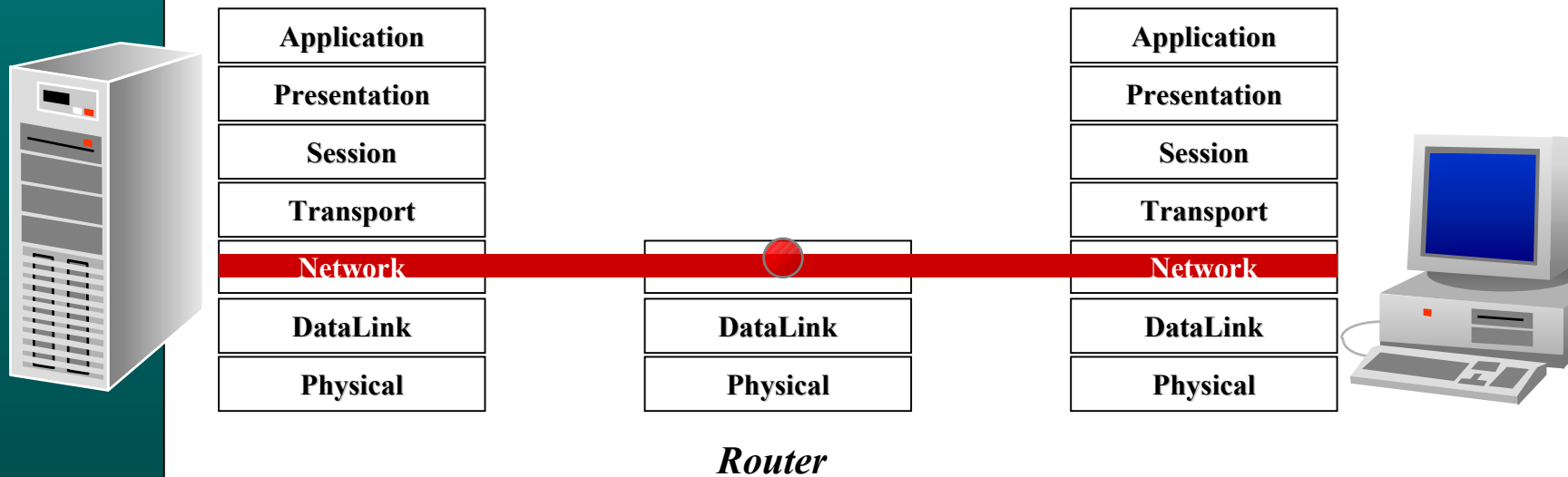
Verbindet interne und externe Netzwerke. Berücksichtigt unterschiedliche Sicherheits-Bedürfnisse durch Regelung der Kommunikation

3 Arten von Firewalls

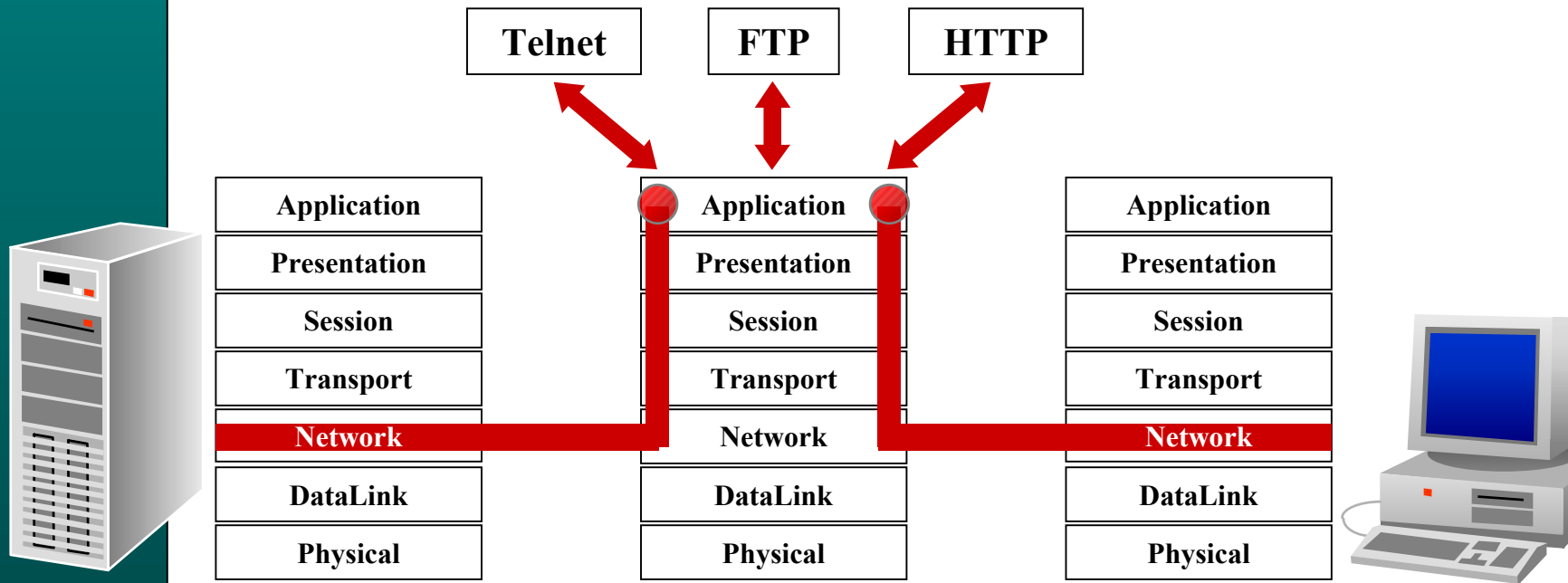
Application	• Application Layer Gateway (Proxy)
Presentation	ॐ Application Level
Session	
Transport	
Network	• Packet Filtering
	ॐ Network Level
	• Stateful Inspection (Circuit Relays)
Data Link	ॐ FireWall-1 / Raptor: Before Network Level
Physical	



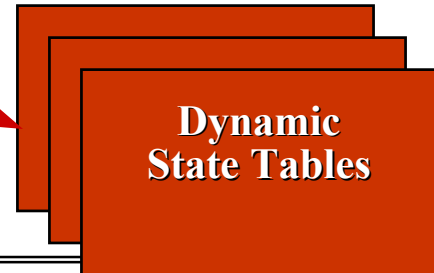
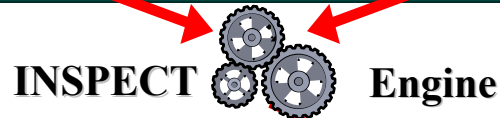
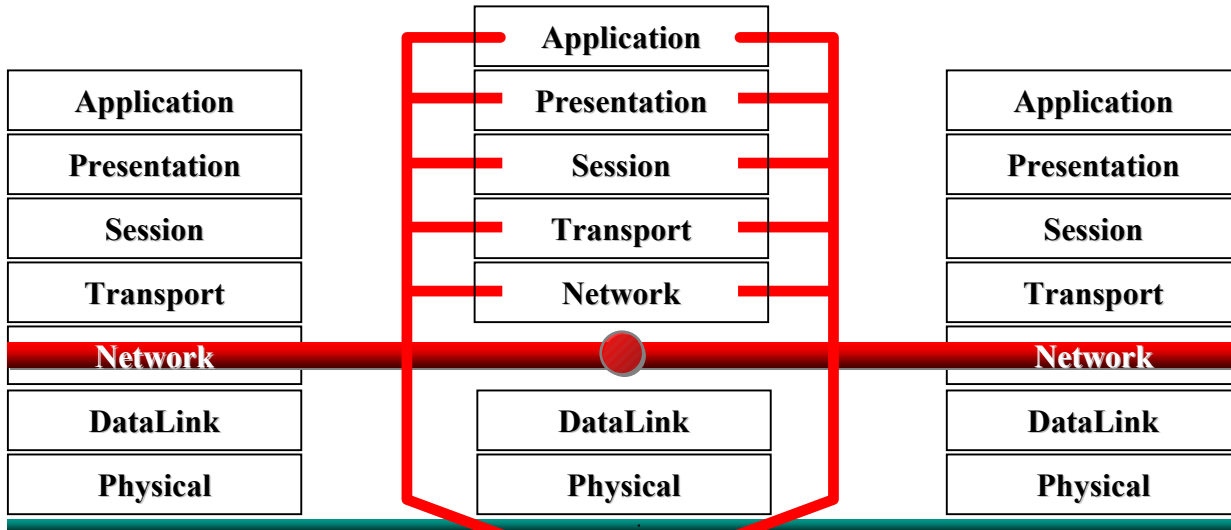
Packet Filtering



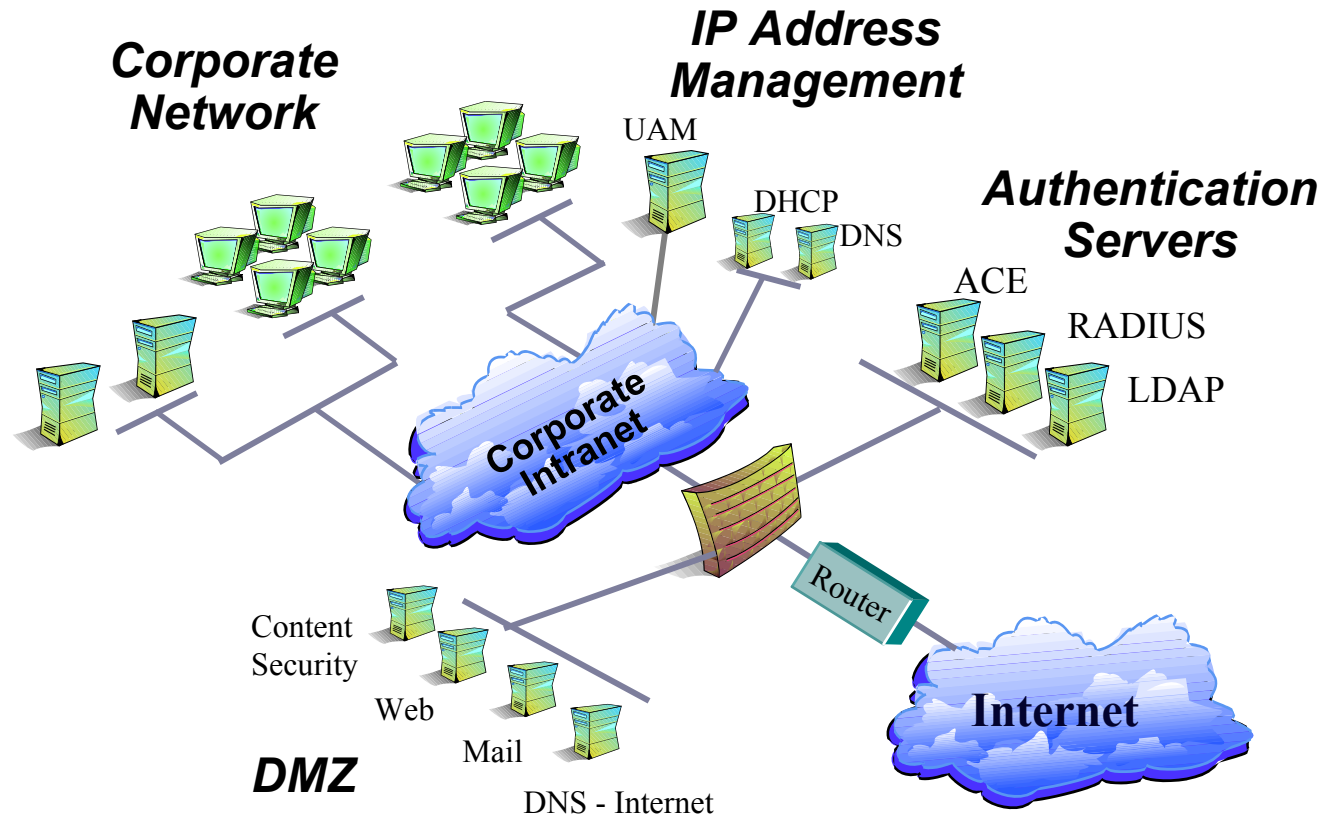
Application Gateway



Circuit Relay



Implementations-Übersicht



Verkehrsregelung

AccessControl - FireWall-1 Security Policy

File Edit View Manage Policy Window Help

Security Policy | Address Translation

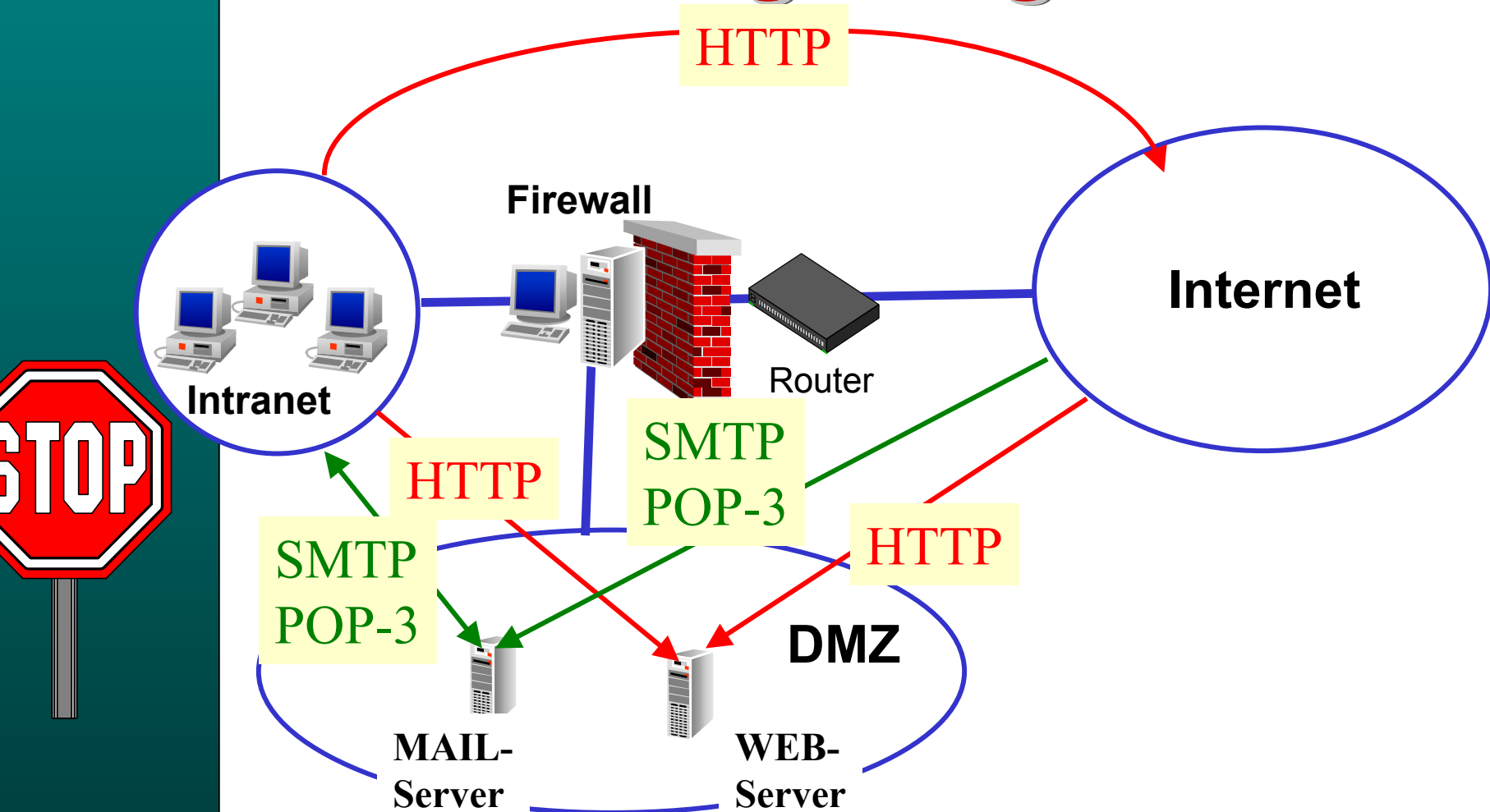
No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Any	Firewall_local	Any	drop	Alert	Gateways	Any	No access to firewall
2	Internet	Local_Net	Any	drop	Long	Gateways	Any	Disallow the Internet access to local network
3	Local_Net	Internet	http https	accept		Gateways	Any	Allow the local network to access the Internet
4	Any	Email_Server	smtp pop-3	accept	Long	Gateways	Any	Allow access to E-Mail Server
5	Any	Web_Server	http	accept	Long	Gateways	Any	Allow web traffic to the Web Server
6	Any	Any	Any	drop	Long	Gateways	Any	Disallow all other traffic and send an alert is encountered

For Help, press F1

*local Read/write

Start | Exploring - C:\ | Microsoft PowerPoin... | AccessControl - ...

Verkehrsregelung



Viren und Vandalen

Was ist ein Virus?

- Ein Computervirus ist ein Programm das sich selber reproduzieren kann in dem es andere Programme mit sich selber modifiziert.
- Ein Virus muss nicht immer Schaden anrichten.
- Viren werden übertragen, wenn verseuchte Programme kopiert werden oder wenn ein infiziertes Dokument geöffnet wird.
- Viren können durch ihre Signatur erkannt.

www.icsa.nct/virus

www.virusbtn.com/WildLists/

Virenarten

- **Bootviren**
- **System-(Cluster-)Viren**
- **Programm-Viren**
- **Polymorphe Viren**
- **Stealth-Viren**
- **Retro-Viren**
- **Daten-Viren (Makro-Viren)**
- **Würmer**

Virus-Infektionen

- International Computer Security Association (ICSA) 1998 Virus Prevalence Survey: Viren-Infektionen treten mittlerweile in 99.33% aller Firmen auf.
- Die Verseuchung erfolgt mittlerweile bei 80% via email attachements.
- Schäden weltweit werden beziffert auf über 2 Mia \$.

Virenschutz

- **Virenerkennung**
 - ॐ mit verschiedenen Virens Scanner
 - ॐ auf Workstation / Server / Firewall
 - ॐ Viren-Shield
- **Berechtigungssteuerung**
 - ॐ Kein Zugriff auf Systemebene
 - ॐ Keine Software-Installation möglich
- **Hilfestellungen**
 - ॐ Benutzer-Sensibilisierung / Merkblatt
 - ॐ Helpdesk-Unterstützung

Virenerkennung

URL's mit weiteren Informationen

www.esafe.com

Aladdin

www.virusbtn.com

Virus-Bulletin

agn-www.informatik.uni-hamburg.de/vtc/eng.htm

www.av.ibm.com

IBM

www.mcafee.com

McAfee

www.norton.com/region/de/product/antivirus/



Was ist ein Vandal?

- Neue Art der Bedrohung
- Werden durch Anti-Viren-Programme nicht erkannt
- Sind „auto-executable“ Programme
- Vandalen treten auf als
 - ॐ Java Applet, ActiveX Controls, plug-ins,
 - ॐ Sind in Erweiterungen von Web-Seiten und emails

Wo sind Vandalen eingebunden

- Emails
- Web-Seiten
- Trusted Web-Seiten
- File downloads
- Push content
 - ॐ push-client auf PC pollt provider-server für neuste updates von Programmen und Informationen

Vandalen sind gefährlicher als Viren

- Die Gefahren zielen weniger auf Zerstörung als Viren. Vandalen sind Background Programme, die u.a. folgende Funktionen ausführen:
 -  Diebstahl von Passwörtern um maskiert
 - in geschützte Bereiche auf dem Web einzudringen
 - auf fremde Bankkonten zu gelangen (Rabobank Attacke)
 -  Funktionen zusammen mit denjenigen des Benutzers auszulösen wie
 - zusätzliche Zahlungsaufträge (Quicken Attacke)

Schutz vor Vandalen

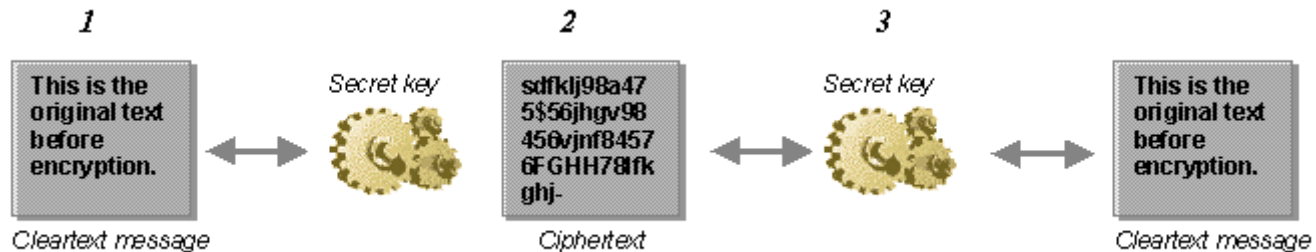
- Blocking
 - ॐ Kein Durchlass von ActivX, Java-Applets, VB-Scripts
- Zertifizierte Webseiten
 - ॐ Kein 100% Schutz, Absender bekannt
- The only practical way to minimize vandal damage is by utilizing access control means and monitoring all auto-executable applications in real-time.

Verschlüsselung / Chiffrierung



- Symmetrische / Asymmetrische Verschlüsselung
- Authentication
- HASH / elektronische Unterschrift
- Key Management
- Umsetzung im Internet mit ISAKMP/Oakley (IKE)

Symmetrische Verschlüsselung



1. Der Originaltext (cleartext) wird durch den Verschlüsselungs-Algorithmus gelassen, zusammen mit dem geheimen Schlüssel, um das vertrauliche Chiffertext zu erhalten.
2. Das Resultat heisst Ciphertext.
3. Der Empfänger entschlüsselt den Ciphertext mit dem gleichen Algorithmus und mit dem gleichen Schlüssel.

Symmetrische Verschlüsselung

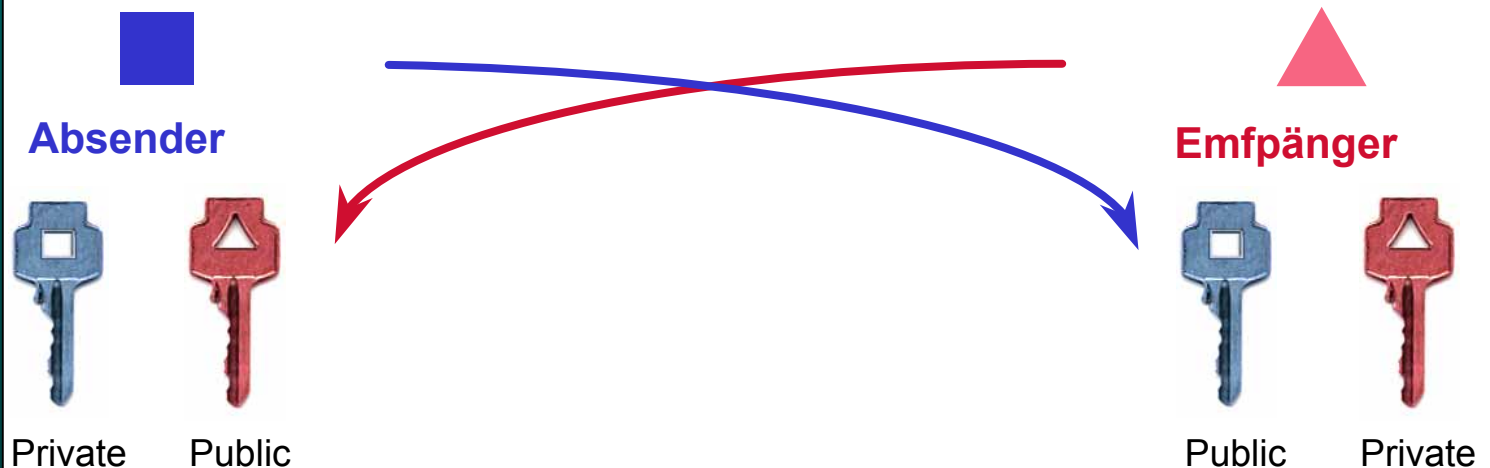
- Vertreter dieses Verfahrens ist **DES** (Data Encryption Standard)
- Sehr schnell
- Sicherheit von der Schlüssellänge und Computer-Leistung abhängig
- Die Schwierigkeit / Nachteil liegt bei
 - Schlüsselübermittlung
 - Schlüsselverwaltung
 - Schlüsselwechsel
 - Beweisführung, dass Absender wirklich der Absender ist

Anwendungen von **symm.** **Verschlüsselung**

- Linklevel Verschlüsselung zwischen zwei Netzanschlüssen
- Verschlüsselung von Dateien für
 - ॐ Sichere Speicherung
 - ॐ Sichere Übermittlung
- Verschlüsselung Logonid-Record von Lotus-Notes (Key = Passwort)

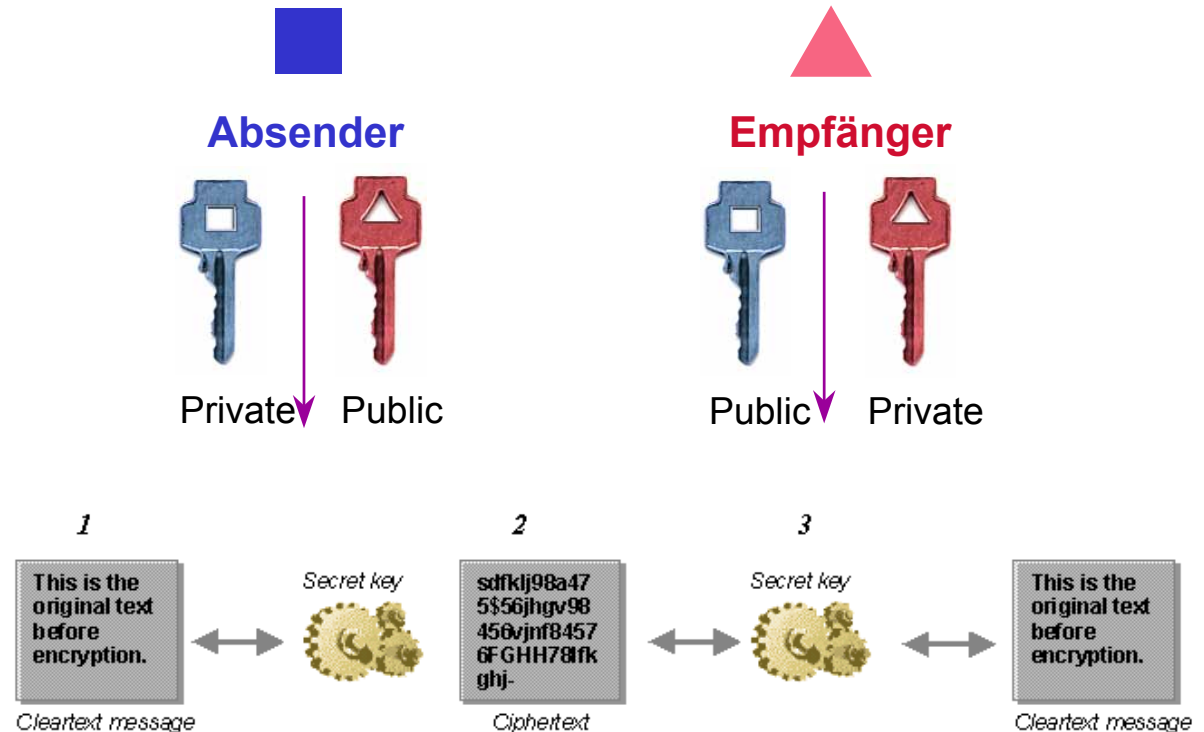
Asymmetrische Verschlüsselung

- ॐ Beide Partner generieren je 2 Schlüssel aus langen Primzahlen (>200 Stellen)
- ॐ Beide Partner stellen einen der beiden Schlüssel dem anderen zur Verfügung



Asymmetrische Verschlüsselung

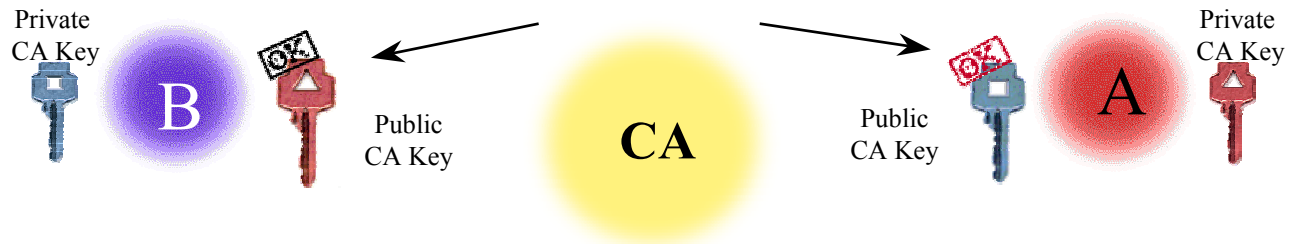
Klartext wird entweder mit dem eigenen PRIVATE-KEY oder dem fremden PUBLIC-KEY verschlüsselt



Asymmetrische Verschlüsselung

- Vertreter dieses Verfahrens ist RSA (Riest, Shamir, Adleman; 1978)
- Die Stärke ist die Schlüsselverwaltung
- Sicherheit ist von der Primzahlenlänge abhängig
- Beweisführung, dass Absender wirklich der Absender ist, wird mit diesem Verfahren möglich
- Sehr langsam

Certificate Authority



- Certificate Authority (CA) ist der öffentliche Schlüsselkasten
- Die CA hat sowohl A als auch B authentisiert (Zertifikat dass A auch A ist)
- Die CA garantiert für die Echtheit des Public Keys von A bzw. B

Anwendung für asymm. Verschlüsselung

- Lösungen im Bereich e-Commerce zusammen mit einer CA
- Mail-Verschlüsselung auf dem SMIME-Protokoll
- Pretty Good Privacy
- Übermittlung von symmetrischen Verschlüsselungs-Keys
- Single Signon: Sichere Benutzer-Authentisierung gegenüber einer public key infrastructure (PKI)

PGP (Pretty Good Privacy)

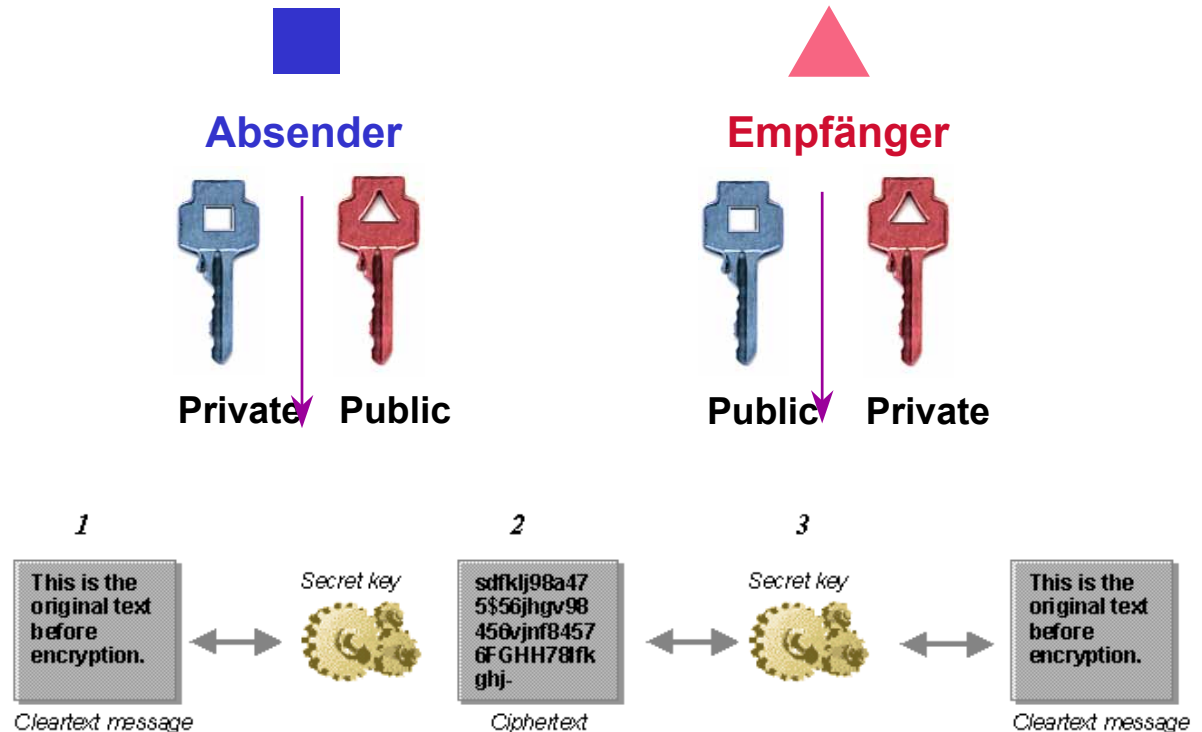
- PGP zu deutsch "recht gute Privatsphäre"
- Basiert auf RSA
- 1. Download von <http://www.pgpi.com>
- 2. Einfache Installation und Integration in Outlook
- 3. Key-Generierung und Public Key Hinterlegung unter pgp.sufnet.nl

PGP (Mail-Verschlüsselung)

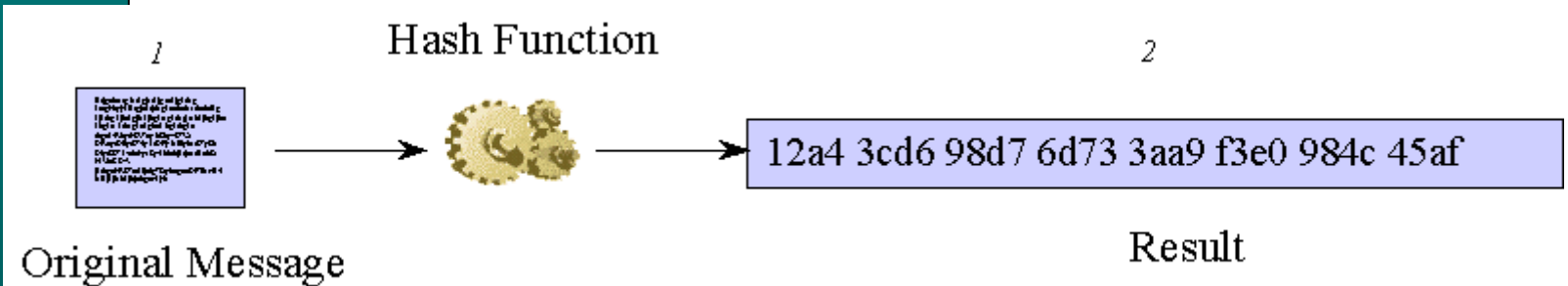
1. Im Outlook PGP-Menü
2. Neues Mail erstellen
3. Holen PGP-Key Empfänger (Launch PGPkeys)
4. Verschlüsselung bei Versand (Encrypt on send)
5. Entschlüsselung bei Empfang (Decrypt mit Passwortschutz des Privat Keys)

Authentication / Non Repudiation

Klartext wird sowohl mit dem eigenen PRIVATE-KEY als auch mit dem fremden PUBLIC-KEY verschlüsselt. Damit kann der Absender und Empfänger die Kommunikation und deren Richtigkeit nicht leugnen.

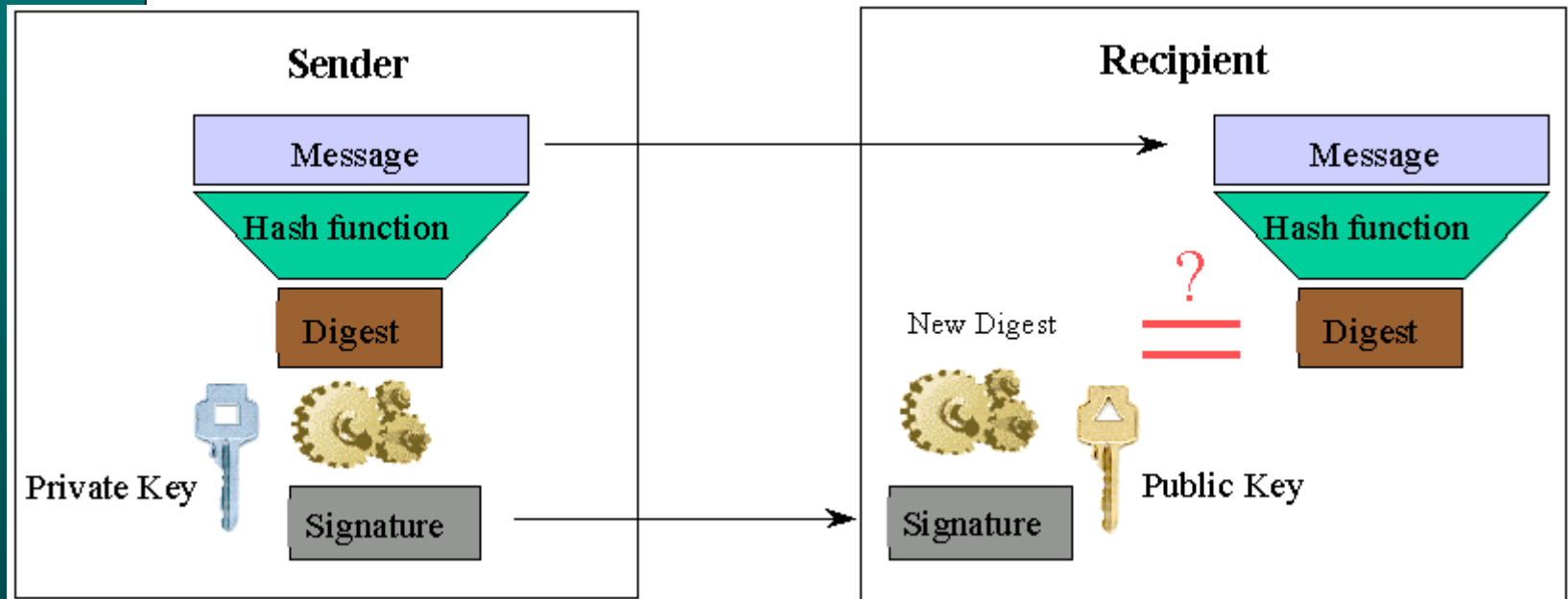


One way hash function

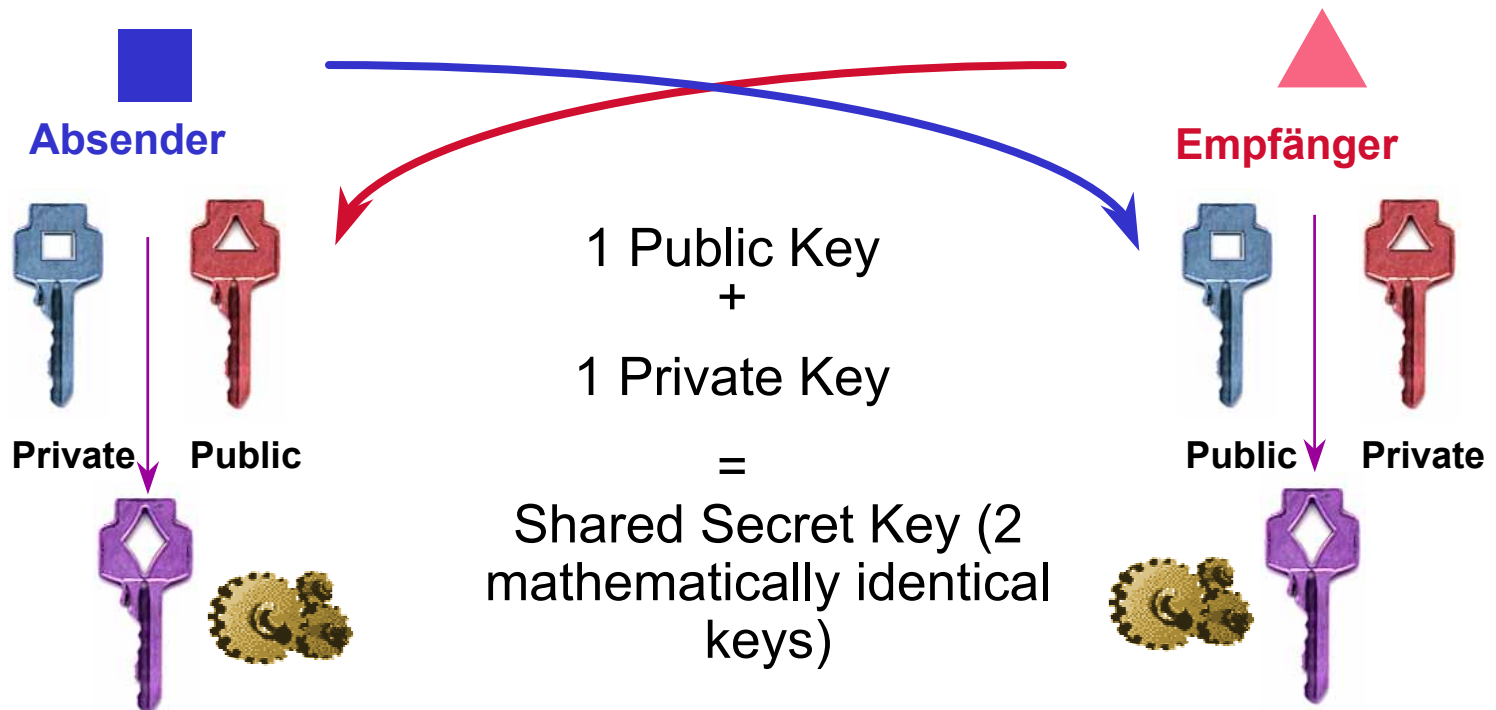


- Ein Hash ist eine „kryptographische Quersumme“
- Der Originaltext wird nicht verschlüsselt
- Nutzung für Datenintegrität und kryptographische Unterschrift

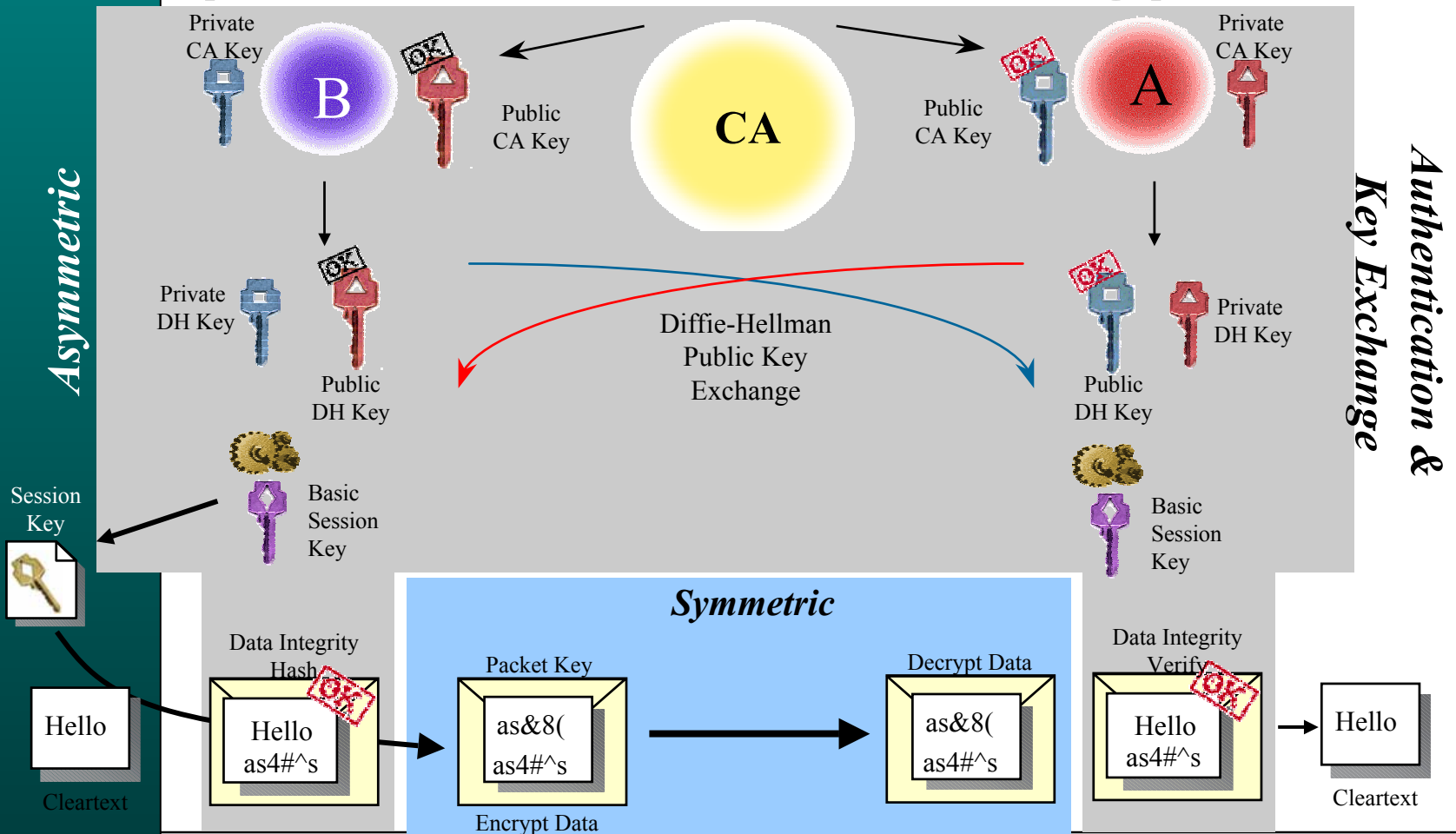
Kryptographische Unterschrift



Diffie-Hellman Key Scheme



Encryption Key Mgmt (Zusammenfassung)



ISAKMP/Oakley (IKE) Encryption Scheme



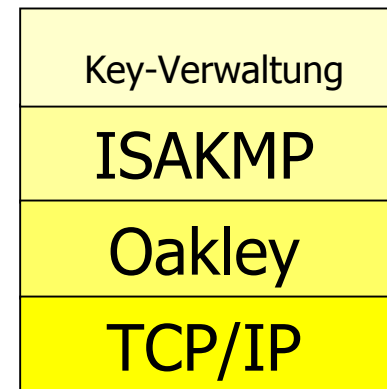
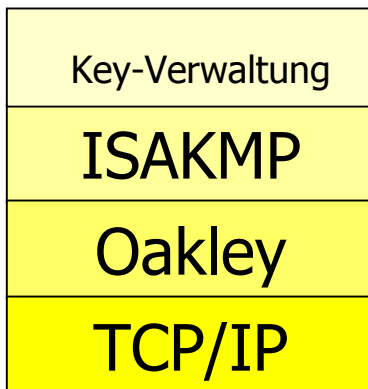
Server

Ciphertext auf dem Netzwerk



Client

PKI



IPSec (IP Security Protocol)

- Ein Sub-Committee der Internet Engineering Task Force (IETF) ist verantwortlich für die Standardisierung der IP Layer Sicherheit wie Verschlüsselung und Integrität.
- IPSec wurde als Standard publiziert, der ein allgemeines Framework für Verschlüsselung der IP Pakete (DES und Triple DES) und Authentisierung (MD5 and SHA-1) definiert.
- IPSec kann manuell (Manual IPSec) oder mit automatischem Schlüsselaustausch (ISAKMP und SKIP) eingesetzt werden.

IPSec Encapsulation



Server

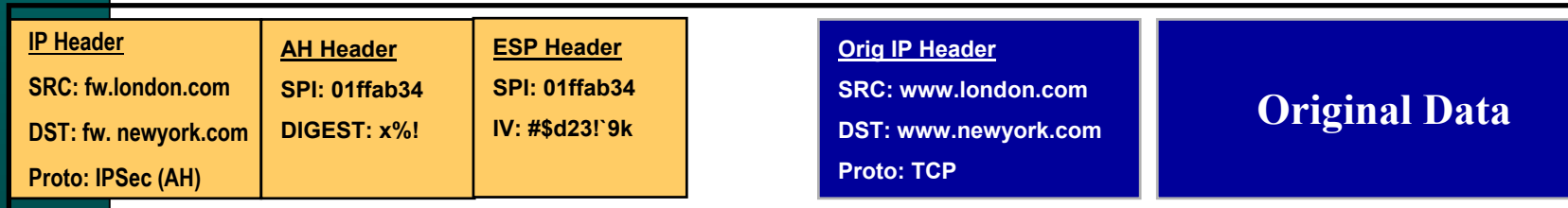
Ciphertext auf dem Netzwerk



Client

Authenticated

Encrypted



Encapsulation Headers



Original Packet

Encryption Scheme

SPI 0x32fd567f

Encryption (ESP): *DES*

Authentication (AH): *SHA-1*

DES Key (64 bits): *0x2983a7b31abb5f3e*

SHA-1 Key (160 bits): *0x354354afbd354ad4354ceaca35c639aec98fbbb8*

ISAKMP

- **Internet Security Association and Key Management Protocol**
- **Ist ein Verschlüsselungs-Standard der Internet Engineering Task Force (IETF)**
- **ISAKMP ist ein Key Management Protokoll**
- **ISAKMP liefert ein konsistentes Framework zum Austausch von Schlüssel und Authentisierungs-Informationen, unabhängig von den Verschlüsselungs-Mechanismen.**
- **ISAKMP delegiert den sicheren Schlüsselaustausch an IKE.**

Oakley or IKE

- **Oakley bzw. neu IKE (Internet Key Exchange)**
 - ॐ Ist ein Internet encryption Protokoll
 - ॐ Führt den gesicherten Austausch von Schlüsseln aus
 - ॐ Übernimmt keine Parteien-Authentisierung
- **Als Basis dient der Diffie-Hellman key-exchange Algorithmus.**
- **Das Oakley Protokoll (IKE) hat Schnittstellen zum ISAKMP Protokoll**
- **Das Oakley Protokoll nutzt das IPSec-Protokoll**

PKI (public-key infrastructure)

- Die PKI ist eine öffentliche Certificate Authority.
- ISAKMP benötigt eine PKI, um zwischen Client und Server eine sichere Verbindung aufzubauen.
- Vertrauenswürdige, öffentliche PKIs sind die Voraussetzung für jeglichen sicheren elektronischen Handel.
- Beispiele solcher PKI's sind Verisign, Baltimore, Swiskey

SecureNet



Post, Bank

SecureNet auf dem Internet



Browser /
SecureNet

- Download SecureNet via www.post.ch
- Installation
- Einbindung SecureNet Zertifikat in Browser (Zertifikat muss im Browser installiert werden)
- Verschlüsselung basiert auf 128 Triple DES

SecureNet

1. Start SecureNet startet den Browser für die sichere Verbindung zu Post / Bank
2. Start www.post.ch
3. Yellow Net
4. Private / Business
5. Anmeldung mit
 1. Yellow Net-Nummer
 2. Passwort
 3. Streichlisten-Nummer