Veranstaltung
Pr.-Nr.: 10 1023 V

Wirtschaftsinformatik für Wirtschaftswissenschaftler

IT-Sicherheit

Dr. Chris Bizer

WS 2007/2008

1. Einführung: IT-Sicherheit

Unter IT-Sicherheit versteht man Strategien, Vorgehensweisen und technische Maßnahmen, die den unerlaubten Zugriff, ungewollte Veränderungen, den Diebstahl oder die physische Beschädigungen von Informationssystemen und den darin enthaltenen Informationen verhindern, sowie Maßnahmen, welche die Zurechenbarkeit von Aktionen und Nachrichten zu Benutzern und Kommunikationspartner gewährleisten.

Schutzziele der IT-Sicherheit:

1. **Verfügbarkeit von Anwendungssystemen**
   - da beim Ausfall von zentralen Anwendungssystemen die Geschäftstätigkeit des Unternehmens zum Erliegen kommt.
2. **Vertraulichkeit von Informationen**
   - da beispielsweise geschäftsrelevante Informationen nicht bei der Konkurrenz landen sollten.
3. **Integrität von Informationen**
   - da die Verfälschung von Informationen hohe Kosten verursachen kann.
4. **Zurechenbarkeit zu spezifischen Benutzern und Kommunikationspartnern**
   - da es beispielsweise bei Rechtsstreitigkeiten entscheidend seien kann, nachzuweisen, wer eine Aktion durchgeführt hat.

Typische Bedrohungen für Informationssysteme

Bedrohung	Ursache
Hardware-Fehler	Feuer, Stromausfall, sonstige Katastrophen, hohes Alter der Systeme
Softwarefehler	Mangelhafte Spezifikation und unzureichender Test der Software, Gefahr der Veränderung oder Zerstörung von Anwendungsdaten.
Anwenderfehler	Fehlerhafte Aktionen berechtigter Personen (aus Unwissenheit heraus oder böswillig)
Diebstahl von Daten oder Hardware	Unzureichende Sicherung von Räumen und IT-Systemen gegen Einbruch
Schlecht konfigurierte und gewartete IT-Systeme	Rechtevergabe zu lax gehandhabt, überarbeitete Administratoren, aktuelle Software-Updates nicht eingespielt
Unsichere Vernetzung und Internet-Anbindung	Sensitive Systeme werden nicht ausreichend gegen Angriffe aus dem Internet geschützt
Sicherheitserfordernisse werden nicht beachtet	Bequemlichkeit, mangelndes Verständnis, mangelhafte Schulung, z.B. sorgloser Umgang mit Passwörtern
Unzureichende Sicherheits-Politik	IT-Sicherheit hat zu geringen Stellenwert im Unternehmen, Vorgaben und Verfahren werden nicht befolgt, Kontroll-mechanismen versagen, fehlende Sensibilisierung und Schulung der Mitarbeiter

Kapitel 8: IT-Sicherheit

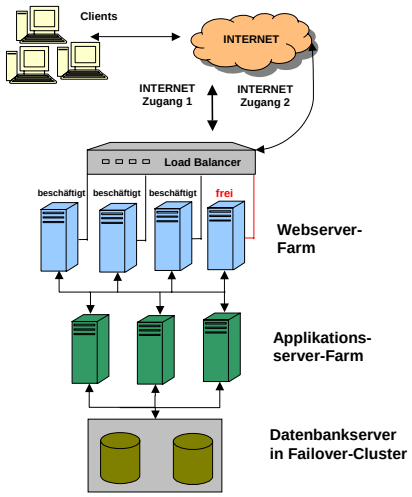
2. Sicherheit von lokalen Informationssystemen

- **Schutzziel: Verfügbarkeit**
  - Gewährleistung, dass Anwendungssysteme und Daten stets zur Verfügung stehen.
- **Maßnahmen:**
  - Verwendung von Hochverfügbarkeitslösungen
  - Desaster Recovery

Hochverfügbarkeitslösungen

Werkzeuge und Techniken, wie z.B. doppelt vorgehaltene Hardware-Komponenten, die einen unterbrechungsfreien Systembetrieb gewährleisten.

- **Hochverfügbarkeit wird erreicht durch**
  - redundante Server
  - redundante Datenspeicherung
  - redundante Stromversorgung
  - redundanten Internet-Zugang
- **Fallt eine Komponenten aus, übernimmt automatisch die Ersatzkomponente deren Funktionen.**
- **Lastenausgleich (Load Balancing): Verteilung sehr vieler Zugriffsanforderungen auf mehrere Server, so dass ein einzelnes Gerät nicht überflutet wird.**
- **Spiegelung: Duplizieren aller Prozesse und Transaktionen eines Servers auf einem Backup-Server, um Unterbrechungen des Dienstes zu verhindern, falls der primäre Server ausfällt.**



Desaster Recovery

Planung, Einführung und Testen von Maßnahmen zur System- und Datenwiederherstellung nach einen Katastrophenfall.

- **Mögliche Katastrophen**
  - **Brand im Rechenzentrum**
  - **Zerstörung von Daten durch Programmfehler, Computerviren oder Hacker**
  - **Diebstahl von Rechnern**
- **Maßnahmen**
  - **Datensicherung (engl.: Backup)**
    - **Anlegung von Sicherungskopien aller Daten**
    - **Verwahrung der Kopien an einem zweiten, sicheren Ort**
  - **Vorhalten von Ersatz-Rechenzentren**
- **Outsourcing an Sicherheits-Dienstleister, die Reserve-Systeme vorhalten, für kleinere und mittelgroße Unternehmen oft sinnvoll.**

DaimlerChrysler-Rechenzentrum 250 m unter der Erde in Kapfenberg

Vertraulichkeit, Integrität und Zurechenbarkeit

- **Maßnahmen zur Gewährleistung der Vertraulichkeit von Informationen**
  - **Zugriffsschutz auf Ebene des Anwendungssystems**
    - **Nur berechtigte Benutzer dürfen Informationen lesen**
    - **Vorraussetzung: Authentifikation von Benutzern**
  - **Zugriffsschutz auf organisatorischer Ebene**
    - **Sicherung der Räumlichkeiten gegen unbefugten Zutritt**
- **Maßnahmen zur Gewährleistung der Integrität (Korrektheit und Vollständigkeit) von Informationen**
  - **Maßnahmen während der Systementwicklung**
    - **Ausführlicher Test der Systeme, um Programmfehler zu eliminieren**
  - **Maßnahmen während des Systembetriebs**
    - **Nur berechtigte Benutzer dürfen Informationen hinzufügen oder ändern**
    - **Überprüfung logischer Integritätsbedingungen bei der Eingabe oder Änderung von Daten (z.B Email-Adresse enthällt @ oder Bestellsumme > 1 Mio. € verdächtig)**
    - **Transaktionsverarbeitung (z.B. Soll-und-Haben Buchung gemeinsam oder gar nicht ausführen).**
- **Maßnahmen zur Gewährleistung der Zurechenbarkeit von Aktionen zu spezifischen Benutzern**
  - **Protokollierung (Logging) welcher Benutzer welche Aktion ausgeführt hat.**

Beispiel: Rollen-basierte Zugriffsrechte

SICHERHEITSPROFIL 1

Benutzer: Buchhalter in Personalabteilung
Ort: Abteilung 4711
Angestelltenidentifikation
Codes mit diesem Profil: 00753, 27834, 37665, 44116

Datenfeldbeschränkungen	Zugriffstyp
Alle Angestelltendaten in Abteilung 4711	Lesen und Aktualisieren
• Krankheitsaufzeichnungen	Nein
• Gehalt	Nein
• Verdienstdaten	Nein

SICHERHEITSPROFIL 2

Benutzer: Personalabteilungsleiter
Ort: Abteilung 4711
Angestelltenidentifikation
Codes mit diesem Profil: 27321

Datenfeldbeschränkungen	Zugriffstyp
Alle Angestelltendaten in Abteilung 4711	Nur Lesen

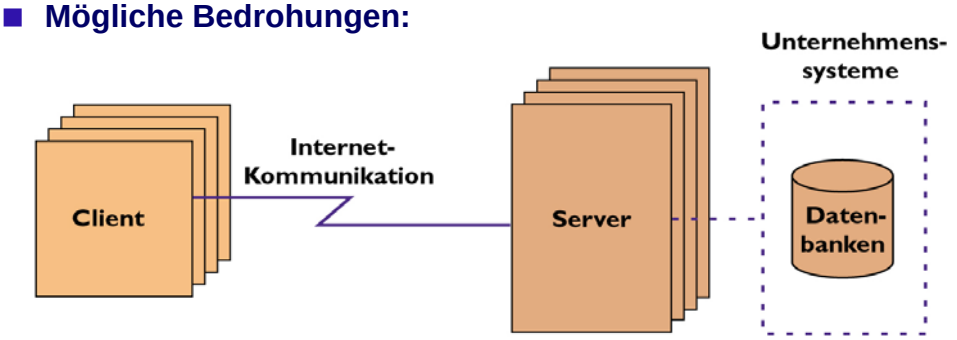
Authentifikation

Unter Authentifikation versteht man die Überprüfung der Identität eines Benutzers.

- **Authentifikationsverfahren**
  1. **Kenntnis eines Geheimnisses**
     - **Beispiel: Kennwort, PIN/TAN-Kombination**
  2. **Besitz eines Gegenstandes, der nicht weitergegeben werden darf und schwer duplizierbar ist**
     - **Beispiele: Autoschlüssel, Chipkarte**
  3. **Körperliche Merkmale (biometrische Verfahren)**
     - **Beispiele: Fingerabdruck, Geometrie der Hand, Netzhaut, Iris, Gesichtsform, Stimme**
- **Exkurs: Wahl eines guten Passworts**
  - **Mindestens achtstelliges Passwort, das nicht in einem Wörterbuch steht**
  - **Keine Bestandteile des eigenen Namens oder des Geburtsdatums**
  - **Mindestens ein Sonderzeichen oder eine Ziffer**
  - **Passwörter sollten häufig gewechselt werden**
  - **Verschiedene Passworte für verschiedene Systeme verwenden**
  - **Passwort nicht aufschreiben**
  - **Vorschlag: Die Anfangsbuchstaben der Wörter eines Satzes. Dieser Satz soll einem etwas bedeuten, damit er leicht merkbar ist.**

3. Sicherheit von verteilten Informationssystemen

- Mögliche Bedrohungen:



- Computerviren
- Abgehörte Leitungen
- Verlust einer Maschine

- Abhören
- Sniffing
- Abänderung von Nachrichten
- Diebstahl und Betrug

- Hacking
- Computerviren
- Diebstahl und Betrug
- Abhören von Leitungen
- Vandalismus
- DoS-Angriffe

- Diebstahl von Daten
- Kopieren von Daten
- Änderung von Daten

IT-Schutzziele im Bezug auf die Nachrichtenübertragung im Internet

- **Geheimhaltung**
  - Daten, die über das Internet übertragen werden, sollen für Dritte nicht einsehbar sein.
  - Wird durch Verschlüsselung gewährleistet.
- **Nachrichtenintegrität**
  - Übertragene Daten sollen auf ihrem Weg vom Sender zum Empfänger nicht von Dritten verändert werden können.
  - Wird durch digitale Signaturen gewährleistet.
- **Nachrichtenauthentizität**
  - Empfänger müssen sicher sein können, dass Nachrichten wirklich vom angegebenen Sender stammen.
  - Wird durch digitale Signaturen gewährleistet.
- **Nichtabstreitbarkeit**
  - Es muss sichergestellt sein, das Sender nicht im nachhinein abstreiten können, eine Nachricht verschickt zu haben.
  - Wird durch digitale Signaturen gewährleistet.

3.1 Symmetrische Verschlüsselung

Nachrichten werden mit dem gleichen, geheimen Schlüssel ver- und entschlüsselt.

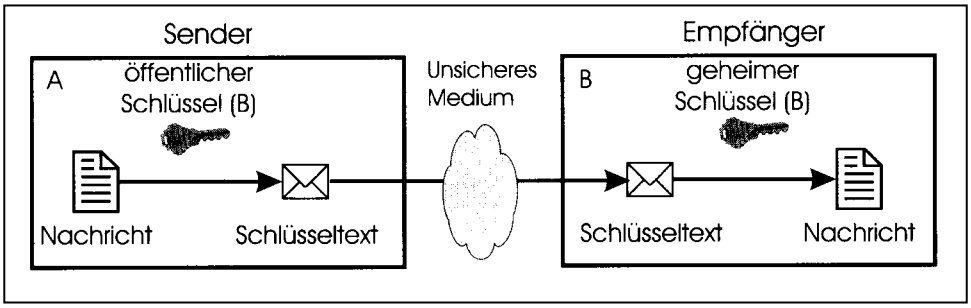
- **Verschlüsselungsverfahren: DES, Triple-DES, IDEA**
- **Vorraussetzung: Beide Kommunikationspartner kennen den Schlüssel.**
- **Vorteil symmetrischer Verschlüsselung:**
  - **Beansprucht geringe Rechenleistung. Daher lassen sich auch größere Datenmengen mit geringem Zeitaufwand verschlüsseln.**
- **Problem symmetrischer Verschlüsselung:**
  - **Die Schlüsselvereinbarung muss über einen sicheren Kanal (z.B. bei einem persönlichen Treffen) erfolgen.**
  - **Eine Schlüsselvereinbarung über das unsichere Internet ist nicht direkt möglich!**

Asymmetrische Verschlüsselung

- **Asymmetrische Verschlüsselung beruht auf zusammen-gehörigen Schlüsselpaaren.**

Nachrichten, die mit einem Schlüssel eines Schlüsselpaares verschlüsselt wurden, können nur mit dem anderen Schlüssel des Schlüsselpaares wieder entschlüsselt werden.

- **Anwendung: Verschlüsselte Nachrichtenübertragung**
  - **Der öffentliche Schlüssel des Empfängers dient zur Verschlüsselung der Nachricht durch den Sender der Nachricht.**
  - **Der geheime Schlüssel des Empfängers dient dem Empfänger zum entschlüsseln der Nachricht.**



Asymmetrische Verschlüsselung

- **Vorteil asymmetrischer Verschlüsselung:**
  - Es ist keine Schlüsselvereinbarung über einen sicheren Kanal nötig.
  - Öffentliche Schlüssel können über das Internet übertragen werden.
- **Nachteil asymmetrischer Verschlüsselung:**
  - Verfahren sind sehr rechenintensiv und daher für große Datenmengen nur bedingt geeignet.
- **Bekanntester asymmetrischer Verschlüsselungsalgorithmus**
  - RSA (1978 von Rivest, Shamir, Adlerman erfunden)
  - Es ist extrem aufwendig, die RSA-Verschlüsselung bei ausreichender Länge der Schlüssel (1024-Bit aufwärts) zu knacken.
  - Daher ist RSA von der amerikanischen National Security Agency (NSA) als Waffe klassifiziert und mit Exportrestriktionen belegt.

Pretty Good Privacy (PGP)

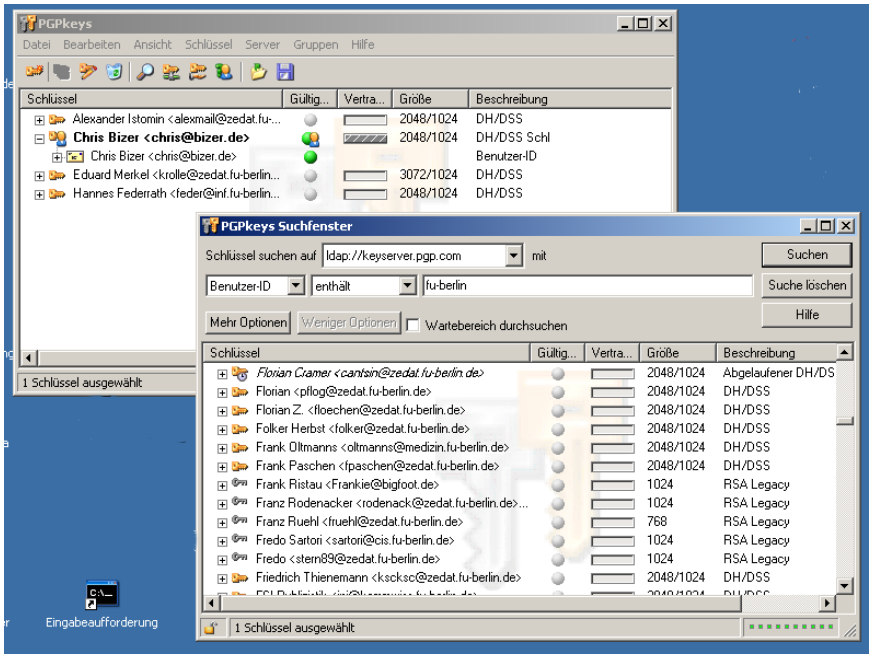
- **Weltweit verbreitetes Public Domain Programm zur Verschlüsselung von**
  - Dateien und
  - Emails
- **mittels symmetrischer und asymmetrischer Verschlüsselungstechnik.**
- **Implementiert den RSA-Algorithmus.**
- **1991 von Phil Zimmermann geschrieben**
  - Zimmermann wurde wegen Verstoß gegen die US-Exportgesetze inhaftiert.
  - Infos zum Autor und der Geschichte vom PGP gibt es unter: http://www.philzimmermann.com/
- **Die internationale Version wird heute vom PGPi-Projekt gepflegt:**

  The PGPi project is a non-profit initiative, whose purpose is to make PGP freely and legally available worldwide. Because the US versions of PGP contain restrictions and limitations which are not relevant outside the US, we remove these limitations and add new features, while keeping compatibility with the US versions.
- **Akutelle Windows-Version von PGPi zum kostenlosen Download unter: http://www.pgpi.org/**

Ein öffentlicher PGP-Schlüssel

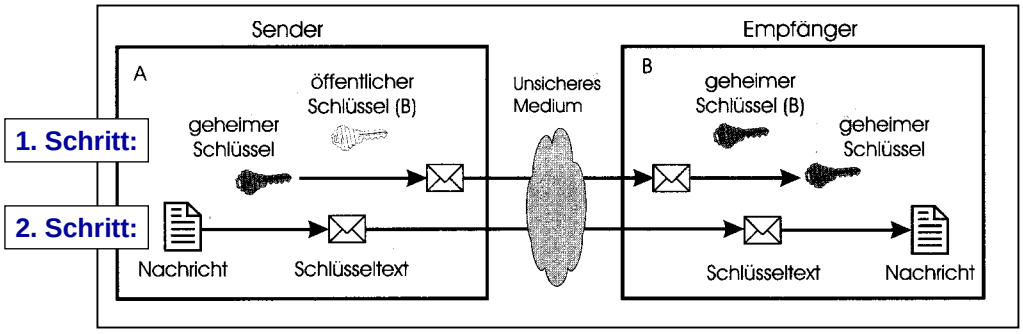
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 7.0.3 for non-commercial use <http://www.pgp.com>
mQENBDxw7eQBCAC2Qu/j5Olri6h1LEBi60Q5INBSdWFW0IUxubh9q8kZhbFnGKiU
XJLN2kKlwxNP+aMFAzZ9ETi7c3vWxDde1gXAxvIV+phSn9RgsEPdz4cxwvTldGgB
xeRE7x8+YVfKjRjDwRO6BDuXvvkqvEAHD/L9OxxgihKkEJFSM2szz+gx/Ab5vEP8
QpzY7ipyNtOCGBM2pRV+xB+BeA3ybIiO7zyqRpR6ZqaWlWci7Rwg7oFZk1D3iM0S
lDBhRaYexuCv4fLLmBX6mrFLnun+JBt15ojM9H0xfPnF/XMJ6FHI3VlXLJ5HVwZl
isZFHy2DYrW4ZHOvBOZXXPMOgkazbdsr0Pj1ABEBAAG0HENocmlzIEJpemVyIDxj
aHJpc0BiaXplci5kZT6JAS4EEAECABgFAjxw7eQICwMJCAcCAQoCGQEFGwMAAAAA
CgkQJWGsstdhZY0q/wgArJyy3sXSUER9GVwun9q2qDbcJsAN0BzVzf1lwgkJ5iUZ
TEz2Sua6GPZ4wgZ5OfOTse5B7GRKTY1dgGl+4VoLpq3Tv/M0slre7AXwD2Li9E/K
aHEl7gFPHxbpXjCDSQnWLUi2+lbO9rTf3ia6gxtFgv3Sm7rAsQNE4q7eMQ022QUO
63AH/j5bn1WVdfaYT70EhhGNFOaW1HIXB/edouQFMWVDCN5LoFKKFNgUnUG1iaku
U6LGmc3VA9XbKEg0Tz6DQW6Dt38c/AyDCxBcVp53puLl0PDmN8QrcMilazpoSJ3Q
zLVkxKFmwJGQuifETUMBoX/SidQL6pu6sLAraZro/JUQmrlmYleLiu3jA3JSUGMB
Eyr6XqMJ69UZ4qBdFSxLqn7oDgG1XTLEF1XW5M7vUX2i1lxPKbZx4eI2TbseNaXc
-----END PGP PUBLIC KEY BLOCK-----
```


PGP-Schlüsselverwaltung und PGP-Schlüsselserver



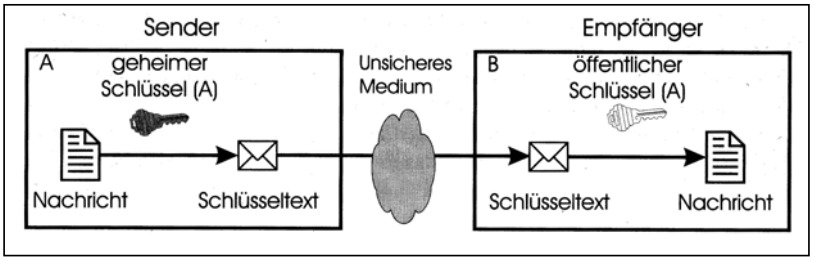
Hybride Verschlüsselungsverfahren

- **Hybride Verschlüsselungsverfahren kombinieren die Vorteile symmetrischer und asymmetrischer Verschlüsselung:**
  1. **Schritt: Für jeden Kommunikationsvorgang wird ein neuer geheimer, symmetrischer Schlüssel generiert. Dieser Schlüssel wird mit Hilfe eines asymmetrischen Verschlüsselungsverfahren ausgetauscht. (➔ Schlüsselaustausch über unsichere Kanäle möglich)**
  2. **Schritt: Die eigentlichen Daten werden mit diesem Schlüssel symmetrisch verschlüsselt. (➔ Geringerer Rechenaufwand)**



Integrität, Authentizität und Nichtabstreitbarkeit

- **Asymmetrische Verfahren haben die angenehme Eigenschaft,**
  - **dass sich eine Nachricht, die mit dem privaten Schlüssel verschlüsselt wurde, nur mit dem öffentlichen Schlüssel wieder entschlüsseln lässt und**
  - **diese Entschlüsselung keine Rückschlüsse auf den privaten Schlüssel zulässt.**
- **Über diesen Mechanismus lässt sich Nachrichtenintegrität, Nachrichtenauthentizität und Nichtabstreitbarkeit garantieren:**
  1. **Sender verschlüsselt die Nachricht mit seinem geheimen, privaten Schlüssel (A) und verschickt die Nachricht an den Empfänger.**
  2. **Der Empfänger entschlüsselt die Nachricht mit dem öffentlichen Schlüssel des Senders (A) und kann sicher sein, dass die Nachricht vom Sender stammt und bei der Übertragung nicht verändert wurde.**



3.2 Grundkonzept digitale Signatur

- Das gerade vorgestellte Verfahren erfordert sehr viel Rechenleistung, da die gesamte Nachricht mit dem geheimen Schlüssel verschlüsselt wird.
- Deshalb gehen digitale Signaturen einen anderen Weg:

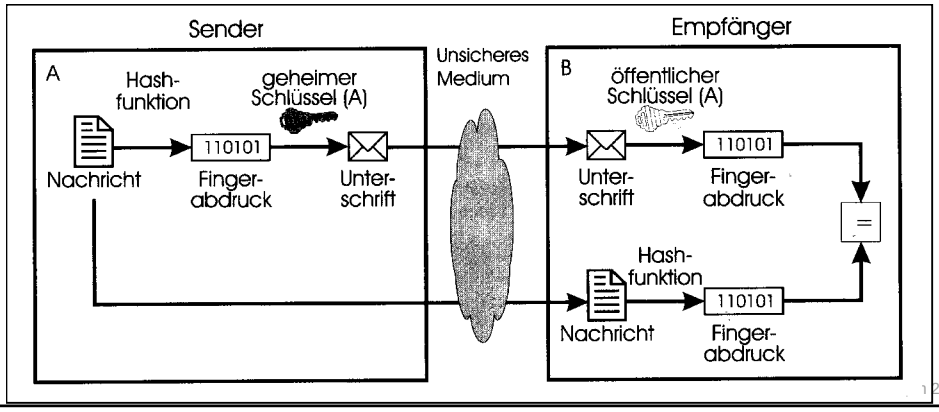
  Über eine Hash-Funktion wird ein digitaler Fingerabdruck des Dokuments in Form eines Hash-Werts errechnet. Nur dieser Fingerabdruck wird anschließend asymmetrisch verschlüsselt.

- Eine Hash-Funktion ist ein Algorithmus, der
  - aus einer Bitfolge beliebiger Länge (Nachricht), eine Bitfolge vorgegebener Länge errechnet (Hash-Wert).
  - Schon bei minimalen Änderungen der Nachricht, ergibt sich ein völlig anderer Hash-Wert.
  - Bekannte Hash-Funktionen: MD5, SHA1, CS4

Grundkonzept digitale Signatur

1. Sender errechnet über eine Hash-Funktion den Hash-Wert (=Fingerabdruck) seines Dokuments.
2. Der Hash-Wert wird asymmetrisch mit dem geheimen Schlüssel des Senders (A) verschlüsselt.

   Verschlüsselter Hash-Wert eines Dokuments = Digitale Signatur
3. Der Empfänger der Nachricht entschlüsselt den Hash-Wert mit dem öffentlichen Schlüssel des Senders ➔ Nachrichtenauthentizität und Nichtabstreitbarkeit sichergestellt.
4. Der Empfänger berechtet aus der Nachricht mit der gleichen Hash-Funktion selber den Hash-Wert der Nachricht.
5. Er vergleicht diesen Wert mit dem Hash-Wert aus der Digitalen Signatur. Stimmen beide überein, kann er sicher sein, dass das Dokument vom Sender stammt und nicht verändert wurde.

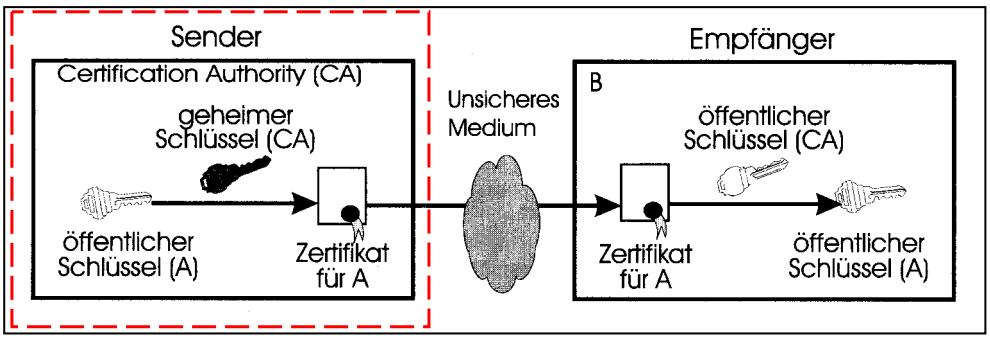


Beispiel: Mit PGP signierte E-Mail

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hallo,
das ist eine E-Mail.

Viele Grüße
Chris Bizer


-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 7.0.3 for non-commercial use http://www.pgp.com

iQA/AwUBPSmt7+GZwkfJQZ3VEQL/FQCg28NRXPjwn25y4D2PCiQSrwRV3DsAn3XA
m36XN1hVhKrpsJlMHmH+NNH/=li+9

-----END PGP SIGNATURE-----
```

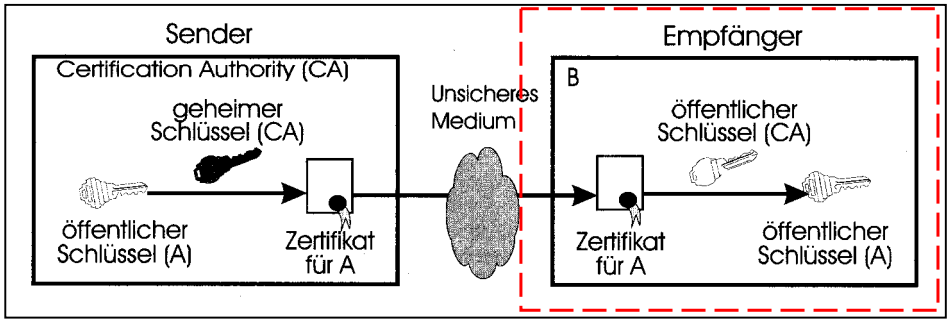

3.3 Public-Key-Infrastrukturen

- Bleibt nur noch ein Problem: Wie kann sichergestellt werden, das ein öffentlicher Schlüssel auch tatsächlich vom gewünschten Kommunikationspartner stammt und nicht von einem Bösewicht, der vorgibt der Kommunikationspartner zu sein?
- Diese Aufgabe übernehmen Certification Authorities (CAs) bzw. Trust Center (TCs)
  - Sie überprüfen auf verschiedene Weise, dass ein öffentlicher Schlüssel auch wirklich einem Menschen oder einer Firma gehört. Im optimalen Fall muss man mit Personalausweis und öffentlichem Schlüssel persönlich bei der CA erscheinen.
  - Anschließend signiert die CA den öffentlichen Schlüssel ihres Kunden mit ihrem geheimen Schlüssel und garantiert somit, dass der öffentliche Schlüssel des Kunden auch tatsächlich dem Kunden gehört.



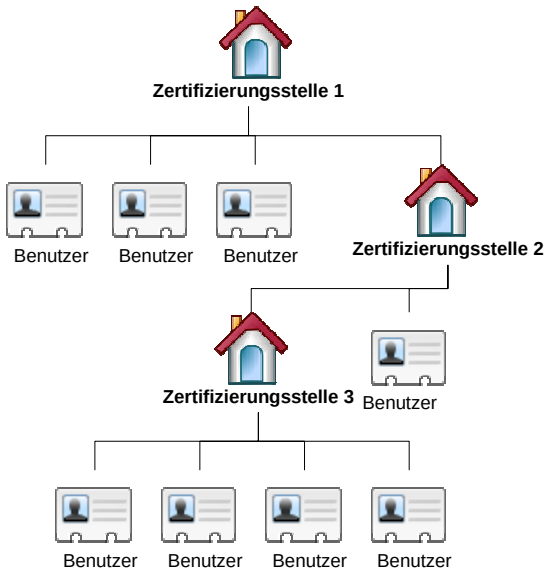
Public-Key-Infrastrukturen

Zertifikat = Von einer CA unterschriebener öffentlicher Schlüssel eines Nutzers.



- **Überprüfung des Zertifikats von A durch den Kommunikationspartner (B):**
  1. **B erhält von A Zertifikat.**
  2. **B überlegt sich, ob er der signierenden CA vertraut und ob er den öffentlichen Schlüssel der CA besitzt.**
     - **Öffentliche Schlüssel bekannter CAs sind beispielsweise im Internet Explorer integriert.**
     - **CA-Ketten: Ist dem Nutzer die CA unbekannt, kann er den öffentlichen Schlüssel der CA wiederum bei einer übergeordneten CA überprüfen. Dieser Vorgang wird wiederholt bis bekannte CA gefunden ist.**
  3. **Falls ja, entschlüsselt er das Zertifikat mit dem öffentlichen Schlüssel der CA und gelangt so an den öffentlichen Schlüssel von A.**
  4. **Er kann nur sicher sein den richtigen öffentlichen Schlüssel von A zu haben und kann somit sicher Nachrichten an A schicken bzw. die Signaturen von A überprüfen.**

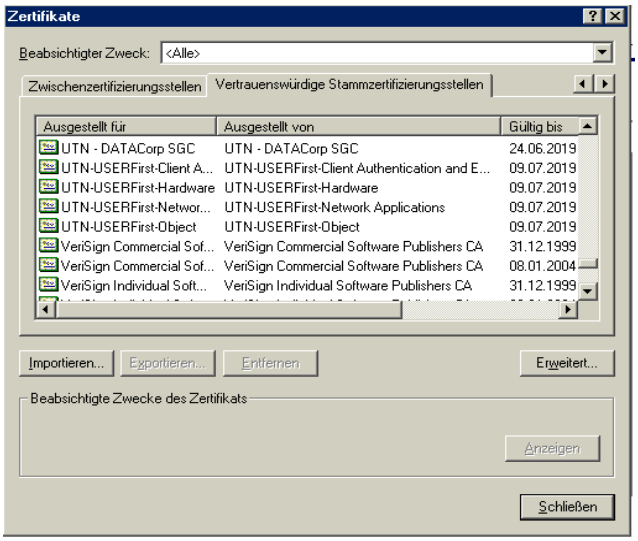
Zertifizierungs-Hierarchien



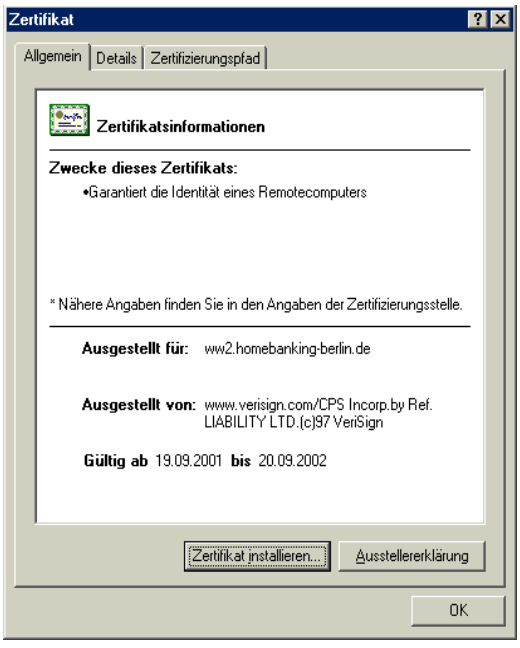
- **Zertifizierungsstellen (CA) können ihrerseits auch Zertifikate für andere Zertifizierungsstellen ausstellen.**
- **Anhand des öffentlichen Schlüssels einer oberen CA lässt sich das Zertifikat einer darunter liegenden CA überprüfen.**
- **Vorteil: Man muss nur den öffentlichen Schlüssel der obersten CA kennen (und darauf vertrauen, dass alle CA in der Kette vertrauenswürdig sind), um die Zertifikate aller Mitglieder der Hierarchie überprüfen zu können.**

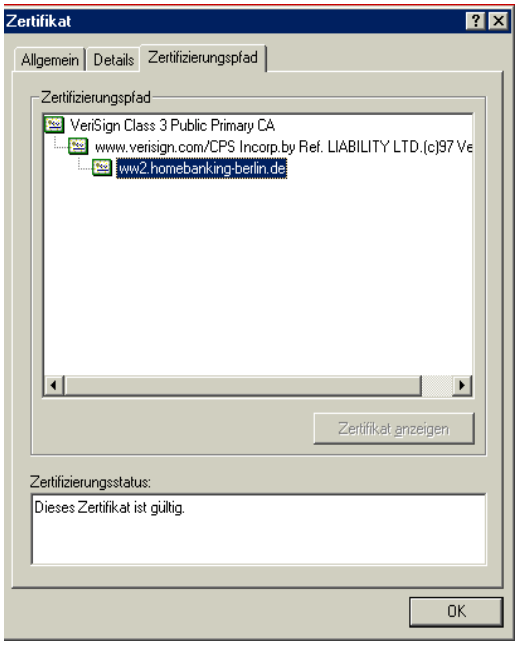
Zertifikate des Internet Explorers

- **Zusammen mit dem Internet Explorer wird eine Reihe von Zertifikaten „vertrauenswürdiger“ CAs ausgeliefert.**
- **Bekannte CAs:**
  - **VeriSign (USA)**
  - **Trustcenter.de**
  - **DFN-PCA**



Zertifikat der Berliner Sparkasse





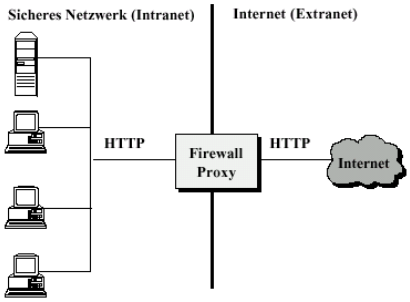
Secure Socket Layer (SSL)

- SSL ist der gängigste Sicherheits-standard im E-Commerce.
- Protokollschicht zwischen HTTP und TCP/IP zur sicheren Datenübertragung über das Internet.
  - Verschlüsselt die zu übertragenen Daten.
  - Stellt die Identität des Servers (und optional auch des Clients) sicher.
- Einsatz von SSL wird bei der Übertragung persönlicher Daten und erst recht bei Kreditkartennummern oder Online-Banking vom Kunden erwartet.
- SSL ist ein hybrides Verschlüsselungsverfahren. Die Kommunikation verläuft in 2 Phasen:
  1. Handshake-Sequence: Authentifizierung der Teilnehmer und Vereinbarung eines Schlüssels für die symmetrische Verschlüsselung (Masterkey) mittels asymmetrischer Verschlüsselungsverfahren.
  2. Datenübertragung: Symmetrische Verschlüsselung mit dem vereinbarten Schlüssel.

3.4 Firewalls

Eine Firewall ist eine Programm, das den Datenverkehr zwischen einem lokalen Netzwerk (LAN) und externen, als unsicher geltenden Netzwerken kontrolliert und die Einhaltung vordefinierter Sicherheitsrichtlinien gewährleistet.

- Ein Firewall dient der Sicherung von Computern und Netzwerken gegen ungewollte „Eindringlinge“.
- In der Firewall-Konfiguration wird festgelegt, welche Art von Daten die Firewall passieren darf.
- Man unterscheidet 3 Typen von Firewalls:
  - Paketfilter-basierte Firewalls
  - Proxy-basierte Firewalls
  - Desktop Firewalls



Paketfilter-basierte Firewalls

- Das Regelwerk der Firewall legt fest, welche Datenpakete auf Ebene der TCP/IP-Netzwerkschicht in welche Richtung passieren dürfen.
- Die Regeln basieren auf den IP/TCP Header-Informationen der Datenpakete: Absender Adresse (Port) und oder Empfänger Adresse (Port)
- Dienste (Mail, FTP, WWW) werden durch Freischalten des jeweiligen Ports zugelassen.

- Nachteil
  - Keinen Prüfbarkeit der übertragenen Inhalte, da Daten wie z.B. Trojaner, Viren oder nicht gewünschte Web-Inhalte auf mehrere Datenpakete verteilt sind.

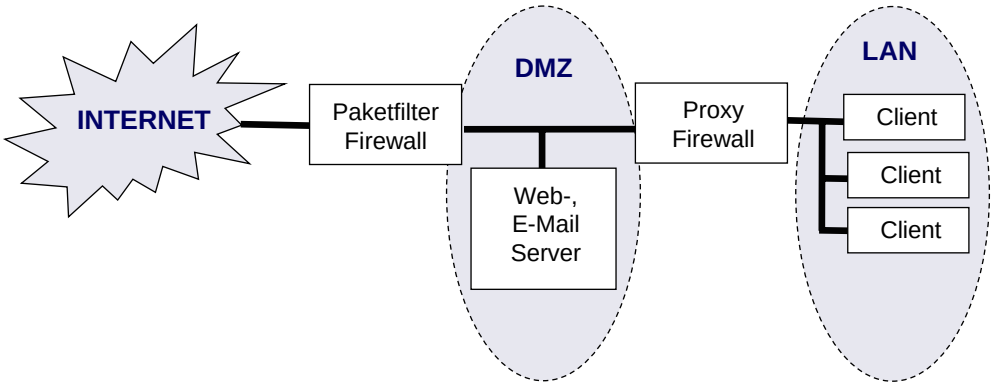
Proxy-basierte Firewalls

- Proxy-basierte Firewalls holen die gewünschten Daten aus dem Internet und schickt sie anschließend an den Rechner im LAN weiter, der sie angefordert hat.
- Es findet keine direkte Kommunikation zwischen den Computers im LAN und dem Internet mehr statt.
  - Die IP-Adressen der Computer im LAN liegen von außen „unsichtbar“ hinter dem Proxy und können somit nicht direkt erreicht (angegriffen) werden.

- Vorteil gegenüber Paketfilter basierten Firewalls:
  - Da der Proxy komplette Nachrichten und nicht nur einzelne Datenpakete verarbeitet, lassen sich die Kommunikationsinhalte nach Begriffen filtern und auf Viren überprüfen.

Firewall-Architekturen

- **Oft werden Paketfilter- und Proxy-Firewalls gemeinsam eingesetzt:**
  - **In einer aus dem Internet erreichbaren DMZ (Englisch: demilitarized zone) stehen die öffentlich zugänglichen Computer (Web-Server, E-Mailserver) des Unternehmens. Diese Zone wird durch eine Paketfilter-basierte Firewall geschützt.**
  - **Das eigentliche LAN des Unternehmens wird durch eine Proxy-Firewall gegen Zugriffe aus dem Internet abgeschottet, d.h. die Rechner des LANs sind aus dem Internet heraus unsichtbar und können somit nicht direkt angegriffen werden.**

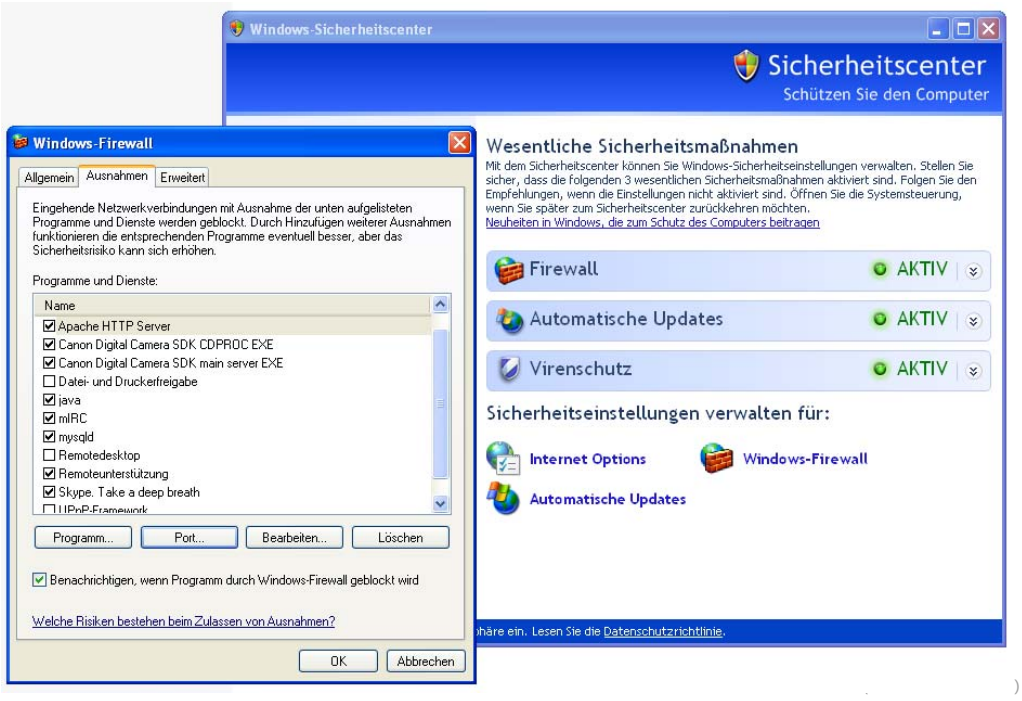


Desktop Firewalls

Desktop Firewalls (auch Personal Firewalls genannt) kontrollieren und beschränken die Kommunikation eines PCs oder Notebooks mit dem Internet.

- **Desktop Firewalls sollen verhindern, dass**
  - **schädliche Programme (Viren, Trojaner) sich auf Rechnern versteckt installieren können.**
  - **die Übertragung von sensiblen Daten (wie Kreditkartennummern) ohne Hinweis auf ein bestehendes Sicherheitsrisiko geschieht.**
  - **unberechtigte Zugriffe von außen auf den PC ausgeführt werden können.**

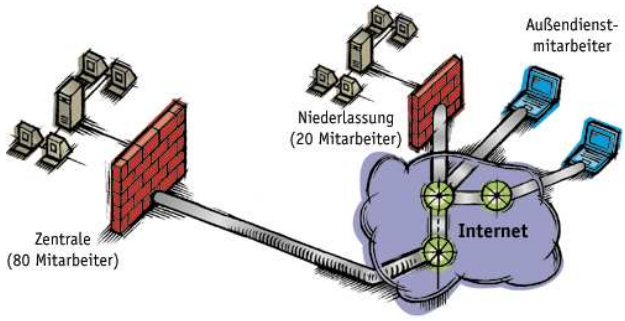
Die Windows Desktop Firewall



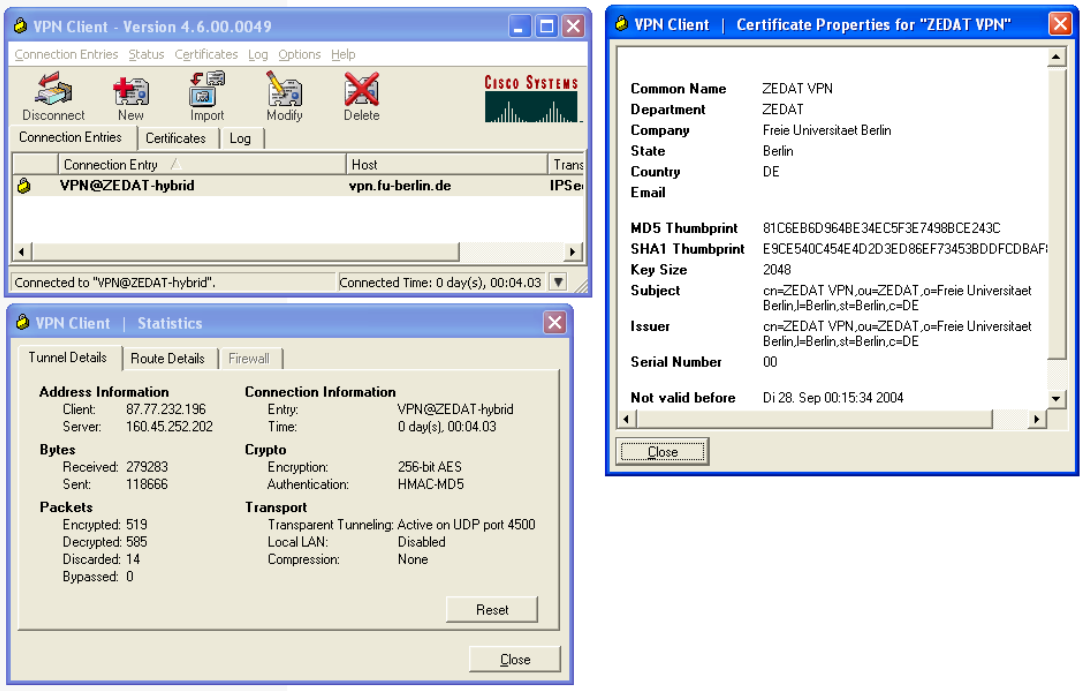
3.5 Virtual Private Networks (VPNs)

VPN ermöglichen die Übertragung von Daten mittels authentifizierter, verschlüsselter Kanäle (sogenannter Tunnel) über das Internet.

- **VPNs begegnen dem Problem, das**
  - **der Internet-Traffic von jedem Router mitgelesen werden kann.**
  - **Router Daten bei der Weiterleitung verändern können.**
- **Virtual Private Networks (VPNs) dienen der**
  - **sicheren Anbindung von Außendienstmitarbeitern über das Internet an das Unternehmensnetz.**
  - **sicheren Verbindung der LANs verschiedener Außenstellen über das Internet und**



Das VPN der Freien Universität



3.6 Malware

Als Malware (Kombination aus engl. malicious, „bösartig“ und Software) bezeichnet man Computerprogramme, welche vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen ausführen.

- **Typen von Malware**
  - **Virus: Softwareprogramm, das sich zur Verbreitung an andere Softwareprogramme oder Datendateien (gerne Office-Dokumente) anheftet.**
  - **Wurm: Softwareprogramm, das sich selbständig über Netzwerke verbreitet. Z.B. sich selber per eMail verschickt.**
  - **Trojaner: Harmlose erscheinendes Programm (z.B. Bildschirmschoner oder Updates), das jedoch versteckte Schad-Funktionen enthält.**
- **Mögliche Schad-Funktionen**
  - **Zerstörung oder Änderung von Daten oder Programmen.**
  - **Unbefugten Zugriff auf den Computer ermöglichen (Backdoor).**
  - **Vertrauliche Informationen (z.B. Passwörter) an Dritte verschicken (Spyware).**

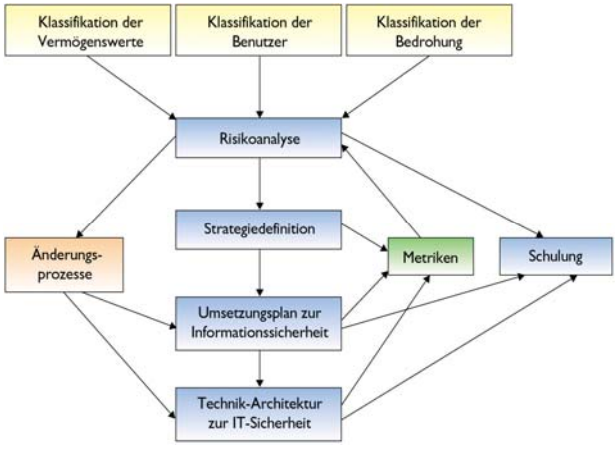
Schutzmaßnahmen gegen Malware

- **Verhinderung der Verbreitung von Malware**
  - **Einsatz von Antivirussoftware**
    - Antivirussoftware erkennt bekannte Viren, Würmer und Trojaner und kann sie meist auch eliminieren.
    - Antivirussoftware erkennt verdächtige Änderungen am System.
    - entscheidend ist die Aktualität der verwendeten Malware-Liste
  - **Signieren von Software durch den Herausgeber**
    - Nur signierte Software von vertrauenswürdigen Herausgebern installieren.
- **Begrenzung des Schadens durch Malware**
  - **Strenges Rechtemanagement**
    - begrenzt die Menge der Daten, den Viren verstören können
    - Z.B nicht als Administrator einloggen
  - **Sicherungskopien von Daten an sicherem Ort verwahren**
    - Um zerstörte oder geänderte Daten wiederherstellen zu können
  - **Verwendung von Desktop-Firewalls**
    - um ggf. unerwünschte Datentransfers oder Logins zu erkennen.

4. Sicherheitsmanagement

Sicherheitsmanagement beinhaltet die Gesamtheit der planenden, ausführenden und kontrollierenden Tätigkeiten zur Identifizierung von Risiken, Festlegung der IT-Sicherheitspolitik, Kontrolle dieser Sicherheitspolitik.

- **Elemente des Sicherheitsmanagements:**



- **Sicherheitsmangement ist eine permanente, zyklisch verlaufende Aufgabe.**
- **Guter Leitfaden: IT-Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik (BSI)**

Elemente einer IT-Sicherheitspolitik

- **Technischer Maßnahmen, z.B.**
  - Backup von Daten und sichere Lagerung der Backups
  - Einsatz von Verschlüsselungstechniken und Zertifikaten
  - Konfigurationsrichtlinien für Web-Server, Browser, Firewalls
  - Richtlinien für die Qualitätssicherung während der Systementwicklung
- **Organisatorische Maßnahmen, z.B.**
  - Klare Vorgaben für die Rechtevergabe
  - Regeln für die Wahl von Passwörtern und bei Verlust von Passwörtern
  - Verhaltensregeln für die Nutzung von Internetdiensten
  - Regeln zum Schutz gegen Malware (Viren, Trojaner, ...)
- **Personelle Maßnahmen, z.B.**
  - Schulung und Sensibilisierung der Mitarbeiter
  - Bestimmung von Verantwortlichen für die IT-Sicherheit
- **Baulich-physische Maßnahmen, z.B.**
  - Zugangskontrolle zu Gebäuden, Serverräumen, Verteilerschränken, etc.
  - Backup von Daten an gesicherten Orten
- **Vorgaben für die regelmäßige Kontrolle von Sicherheitsmaßnahmen.**