Universität Leipzig
Institut für Informatik

Inhaltsübersicht zur Vorlesung von

Dieter Sosna
Datenschutz und Datensicherheit

gehalten im WS 08/09
(Stand 30.01.2009)

Diese Übersicht führt sichwortartig die wichtigsten Inhalte der Vorlesung auf und soll zur Wiederholung bzw. zur Prüfungsvorbereitung dienen. Sie ersetzt keinesfalls den Vorlesungsbesuch bzw. das Selbststudium.

Literatur:
WEB: BSI (Bundesamt für Sicherheit in der Informationstechnik)
Grundschutzhandbuch (PDF: Achtung ca. 3000 Seiten)

IT-Sicherheitshandbuch

Handbuch für die sichere Anwendung der Informationstechnik ,
hrsgg. vom BSI, 1992
http://www.bsi.de/literat/kriterie.htm

Die folgenden Bücher befinden sich im Semesterapparat bzw im Präsenzbestand, sind also in der ZW Informatik der UB stets verfügbar (sollte dies im Einzelfall zeitweilig nicht zutreffen, sprechen Sie mit der Bibliothekarin bzw. informieren Sie mich.

Empfohlene Literatur:

H.Kersten:
Einführung in die Computersicherheit.
Oldenburgverlag 1991, ISBN 3-486-21873-5 **(unbedingt lesen)**
(Präsenzbestand ZW-IfI **ST 277 K41 E3)**

Castano u.a.:
Database Security.
Add.-Wesley 1994 ISBN 0-201-59375-0

Bruce Schneier:
Angewandte Kryptographie
Add.-Wesley (mehrere Ausgaben, auch engl.)
- speziell zu Kap. 3

Ergänzende Literatur:
W. Gerhardt:
Zugriffskontrolle bei Datenbanken
Oldenburgverlag

Verschiedene Artikel der Zeitschriften CT und IX (Heise Verlag)

Weitere Quellen: Wikipedia (und gedruckte Enzyklopädien)

---

1. Einführung

Begriffe *Informationen vs. Daten*

Daten sind Informationen, die durch physikalische Zustände dargestellt werden.
(materialisiert, Speicherung durch Felder)
Beipiele aus der IT:

- Bildschirmen (Ansicht des Bildes – ohne Hilfsmittel lesbar, Zustand von Speichern, Strahlung)
- Arbeitsplatzrechnern (Speicher)
- Kommunikationskanäle incl. drahtloser Übertragungswege
- Disketten, Platten, Bänder und Kassetten, auch Sicherungskopien (Zustand magnetisch gespeichert) , CD, DVD
- Druckerlisten, evt. noch Lochkarten, Lochstreifen (prizipiell ohne Hilfsmittel lesbar)

Beispiel aus anderen Bereichen:
Sport: Dopingproben
Kriminalistik: DNA-Proben

Wert von Daten (<> Wert von Information)
Was bestimmt den Wert der Daten ?
Wert
als zeitabhängige Größe,
als individuell bewertete Größe,
als gesellschaftspolitisch bewerte Größe,
als Größe, die von der physischen Darstellung der Information abhängt.

Wann sind Daten schutzwürdig ?

Vertrauliche Daten: Eine Person oder eine Gruppe von Personen ist vom Besitz der dargestellten Information ausgeschlossen.

Datenschutz: gesellschaftspolitische, volkswirtschaftliche, rechtliche, organisatorische fachliche (Informatik) und technische Aspekte.

Begriffe Datenschutz, Datensicherheit
(Begriffe in der Literatur nicht einheitlich verwendet)

Was bedeuten der Begriff Datenschutz?
Datenschutz: Schutz vor Verlust der Vertraulichkeit.
Gültigkeitsbereich des Begriffes Datenschutz mit Blick auf das Bundesdatenschutzgesetz (in Deutschland , im internationalen Vergleich).

Wachsende Bedeutung von Datenschutz und Datensicherheit auf Grund der immer umfassenden Nutzung elektronischer Medien.
Auswirkungen der allgemein verfügbaren Vernetzung. Gefahr durch moderne Entwicklungen (RFID-Chip, Krankenkassen-Chip, - Profilerstellung.
Beispiele der Jahre 2007/2008 zur Verletzung von Datenschutzinteressen.

Doppelrolle des Bundesdatenschutzgesetzes zum Schutz der Bürger und als Normativ vor einem vermeintlichem Schutzbedürfniss.

Was bedeutet Datensicherheit?
Datensicherheit: Schutz vor Verlust.
- drei Unterbegriffe von Datenverlust
(physischer Verlust, Verlust der Integrität, Verlust der Verfügbarkeit)

Gesetzliche Regelungen
Bundesdatenschutzgesetz, Landesdatenschutzgesetze,
Bundes- und Landesstatistikgesetze, Meldegesetz, Fernmeldeanlagengesetz, Strafgesetzbuch, verschiedene Gesetze aus Bereich Medizin, Steuergesetze, Gesetze über Aufbewahrung von Geschäftsdaten. ...)
Gerichtsurteile (nicht jeder konkrete Fall ist im Gesetz eindeutig beschrieben)
Personenbezogene Daten – in DL natürliche Personen, keine jur. Personen.
Unauthorisierter Datenzugriff und/oder Datenmanipulation – Straftatbestand (StGB §) – damit auch jurist. Mittel zum Schutz anderer Daten. s.u.

”Zweiten Gesetz zur Bekämpfung derWirtschaftskriminalität“ -neue Paragraphen ins Strafgesetzbuch

- § 202a Ausspähen von Daten
(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

  § 202b Abfangen von Daten
  Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

- § 202c Vorbereiten des Ausspähens und Abfangens von Daten
(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

  1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
  2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

  herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet

oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
(2) § 149 Abs. 2 und 3 gilt entsprechend.

Kommentar: Softwarediebstahl, Ausspähen von Daten, Wirtschaftsverrat, Verschaffen von Unternehmensgeheimnissen.

- § 263a Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) § 263 Abs. 2 bis 7 gilt entsprechend.
(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

Kommentar: Jeder Eingriff in einen Datenverarbeitungsvorgang, der Vermögensschäden verursacht. Darunter fallen etwa Kontenmanipulationen in Bankcomputern oder das Erschwindeln von Sozialleistungen.

- § 268 Fälschung technischer Aufzeichnungen
(1) Wer zur Täuschung im Rechtsverkehr

1. eine unechte technische Aufzeichnung herstellt oder eine technische Aufzeichnung verfälscht oder
2. eine unechte oder verfälschte technische Aufzeichnung gebraucht,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Technische Aufzeichnung ist eine Darstellung von Daten, Meß- oder Rechenwerten, Zuständen oder Geschehensabläufen, die durch ein technisches Gerät ganz oder zum Teil selbsttätig bewirkt wird, den Gegenstand der Aufzeichnung allgemein oder für Eingeweihte erkennen läßt und zum Beweis einer rechtlich erheblichen Tatsache bestimmt ist, gleichviel ob ihr die Bestimmung schon bei der Herstellung oder erst später gegeben wird.

(3) Der Herstellung einer unechten technischen Aufzeichnung steht es gleich, wenn der Täter durch störende Einwirkung auf den Aufzeichnungsvorgang das Ergebnis der Aufzeichnung beeinflußt.

(4) Der Versuch ist strafbar.

(5) § 267 Abs. 3 und 4 gilt entsprechend.

- § 269
Fälschung beweiserheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen

würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) § 267 Abs. 3 und 4 gilt entsprechend.

Veränderung von Urkunden, die in Rechenanlagen gespeichert sind (”elektronische Urkundenfälschung“), zum Beispiel bei elektronischer Buchhaltung.

- § 303a Datenveränderung (StGB):
(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

  Kommentar: Veränderung oder Vernichtung von Daten, auch durch Viren.

- § 303b Computersabotage (StGB):

  (1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er
  1. eine Tat nach § 303a Abs. 1 begeht,
  2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
  3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

  wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

  (2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

  (3) Der Versuch ist strafbar.

  (4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
  1. einen Vermögensverlust großen Ausmaßes herbeiführt,
  2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
  3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

  (5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

  Kommentar: Anschläge auf die Datenverarbeitung durch Veränderung oder Vernichtung von Computerdaten, Datenträgern oder Anlagen.

- § 303c Strafantrag
In den Fällen der §§ 303, 303a Abs. 1 und 2 sowie § 303b Abs. 1 bis 3 wird die Tat nur auf Antrag verfolgt, es sei denn, daß die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

In DL sehr weitgehende Regelungen, dennoch spektakuläre Fälle des Verstoßes gegen Datenschutz und Datensicherheit. In der Praxisgroße Dunkelziffer:

- es ist vielfach die Befürchtung, dass der Ruf leidet (vgl. §303)
- Ermittlungen schwierig, da Nachweis durch unzureichende gerichtsverwertbare Spuren im Computer aufwendig.*
- Es fehlt geschultes Personal in ausreichender Menge (an verschiedenen Stellen)*

Es ist nicht das Ziel dieser Vorlesung, die rechtliche, die gesellschaftpolitische Seite darzustellen, deshalb Beschränkung auf technische (bauliche) , gerätetechnische, softwaretechnische und organisatorische Fragen.

Begriff *Angriff:*

Jedes Ereignis, das Verlust der Daten oder der Vertraulichkeit der Information nach sich zieht oder nach sich ziehen kann.

Klassifikation der Angriffe nach Ursache:

- Naturkatastrophen (Wasser, Erdbeben, Sturm, Regen , Blitzschlag)
- Krieg
- Feuer , Brandstiftung
- technische Ausfälle, Fehlfunktion, Fehlfunktion der Versorgungssysteme
- Durch Menschen direkt verursacht:
  ohne Vorsatz (fahrlässig):
  versehentliche Fehlbedienung, versehentliche mech. Einwirkung, mangelhafte Organisation, unbedachte oder unkontrollierte Entsorgung von Datenträgern.

  mit Vorsatz:
  - vorsätzliches Herbeiführen von Datenverlusten oder Verlust der Vertraulichkeit durch absichtliche Bedienfehler, Feuer, mech. Einwirkung…. - Sabotage
  - Terrorismus
  - Einbruch, Diebstahl

Unterteilung: **Angriffe von innen , von außen**

Abwehrmaßnahmen:
Grundsätzliche Klassifikation

- Technische Maßnahmen (darunter als wichtiger Teilaspekt : bauliche Maßnahmen),
- Organisatorische Maßnahmen
- Personelle Maßnahmen

i.A. Kombination von Maßnahmen aus diesen Bereichen, da sonst Schutz nicht erreicht werden kann (z.B. bei Katastrophen) oder umgangen werden kann (Angriffe durch Menschen).
Beispiel Feuer:

Bauliche Maßnahmen: Feuerhemmende Bauausführung (Vorschriften), Türen, Kabeldurchführung,
Technische Maßnahmen: Brandmelder, Feuerlöscheinrichtungen
Organisatorische M.:

- Regelmäßige Prüfung der technischen Einrichtungen (evt. durch unabhängige Fachleute) und Protokollierung der Ergebnisse – Behebung von Fehlern.
- Organisation von Betriebsabläufen (Lagerung (auch von Papier), Sicherung von Daten, Transport von Datenträgern)
- Modernisierung von Anlagen prüfen/durchführen, Problemdiskussionen (z.B. Wasserschaden durch Löschanlage vs. neue Anlage mit Inertgas)
- Aufstellen von Arbeitsplänen für den Brandfall,
- Mitarbeiterschulung / -training, Kooperation mit Feuerwehr.
- Zugangskontrolle

Die Wirkung von Angriffen ist häufig sowohl bei Datenschutz als auch bei Datensicherheit zu spüren – Abwehrmaßnahmen Wirkung in beiden Gebieten, zum Teil in gleicher Richtung (Zugangskontrolle und Beschränkung fordert Datenschutz und Datensicherheit) und zum Teil auch mit konträrer Wirkung (Redundante Datenhaltung zur Verbesserung der Datensicherheit bietet mehr Angriffspunkte, erfordert also evtl. mehr Aufwand bei Datenschutz - z.B. externes Archiv)

Die Maßnahmen wirken vielfach auch gegen mehrere Bedrohungen (Beispiel: Lagerung von Sicherungskopien an einem entfernten Ort: schützt vor Feuer, Wasser, Einbruch, ...)

Erstellung eines Sicherheitskonzepts

Definitionen „Sicherheit

- Absolute Sicherheit
  Ein System heißt absolut sicher, ...
  - Zwei Gründe für die Nichtrealisierbarkeit?
- Induktiv definierte Sicherheit
  ....
  - Beispiel: A**C**ID-Eigenschaften von Datenbanken
- Sicherheit mit Restrisiko
  Idee: Vergleich des Bedrohungsrisikos mit einem akzeptablen Restrisikos

Ablaufschema zur Erstellung eines Sicherheitskonzepts
im Modell „Sicherheit mit Restrisiko“

1. Feststellung des Wertes der Informationen
2. Festlegung der akzeptablen Restrisikos
3. Bewertung der real existierenden Risiken
4. Vergleich Summe der Risiken mit akzeptablen Restrisiko
   Ist die **Summe der Risiken < akzeptables Restrisiko** so **fertig, andernfalls**
   Maßnahmen zur Reduzierung der real auftretenden Risiken und Kostenanalyse

Sind die Kosten der Maßnahmen mit Wert der Information vereinbar
weiter bei 3. andernfalls bei
weiter 2 oder
Feststellung, dass der Schutz nicht erreicht werden kann.

Bedeutung der **Einbeziehung externen Fachwissens** in die Erstellung des Konzepts:

1. ...
2. ...

Feststellung: Sicherheit kostet Geld, i.A. ist es billiger, ein Konzept der Sicherheit zu Beginn einer Arbeit zu entwerfen als es später in ein Projekt zu integrieren (- insbesondere bei technischen und baulichen Maßnahmen).

2. Angriffsszenarien

Die Stellung des Menschen

Was zeichnet den Menschen gegenüber anderen Komponenten eines Sicherheitssystems aus?
Wodurch wird das Verhalten von Menschen beeinflußt?

Die besondere Gefährtung durch Angriffe von innen
Angriffe von innen vs von außen. (Statistische Zahlen ?)

Angriffe von Innen heterogen
nach Ziel (Spaß, Rache, Habgier, ...)
nach Grad interner Kenntnisse

Angriffe von innen mit Vorsatz (~30%) oder ohne Vorsatz (Rest; Unachtsamkeit, Fahrlässigkeit, Unkenntnis)

Warum sind Angriffe von innen besonders gefährlich ?
Absolut Abhängigkeit von IT-Spezialisten, Defizit bei der konkrteten Einschätzung durch nicht IT-Spezialisten (Heranziehen externen Sachverstands).
Nichterkennen einer Gefahr durch mangelnde techn. Organisation (z.B. Entsorgung von Altanlagen, Sparen am falschen Ort.
Sonderfall: Spionage – Ausstattung und Mittel , evt. Schutz durch Auftraggeber (Fremdstaaten)

Wodurch wird das Verhalten von Menschen beeinflußt?
(Familie (beständig vs. stark wechselnd, Freundeskreis, Religion, politische Anschauungen, Lebensstil – Verhältnis zu den Mitteln, bisheriges Leben (Erleben) , Erkrankungen – auch Spielsucht, Alkoholismus -> Geldprobleme, Bildung – Ausbildung, Anerkennung der bisherigen Lebensleistung)

Ansätze, die Wahrscheinlichkeit von Angriffen von inner zu reduzieren
(Menschenführung)

- Überprüfung der Mitarbeiter bei Einstellung und auch später (Lebenslauf analysieren, pol. Führungszeugnis, ...), evt. Auferlegung von persönl. Einschränkungen
- Klare Strukturierung der Firma, klare Festlegung von Verantwortlichkeiten und Aufgaben, der Unterstellungsverhältnisse.
- Ausreichende Qualifizierung der Mitarbeiter, Möglichkeit der Weiterqualifizierung (wenn sich die Technik, die Aufgaben ändern), Vermeidung von Überqualifizierung.
- Ausreichende Arbeitsaufgaben, Vermeiden von Überlastung, aber dabei auch Erkennen von Problemen mit der Arbeitseinstellung , Integration in Teams.
- Anerkennung für geleistete Arbeit (finanziell (gutes Gehalt zahlen, Gewährung von Sonderleistungen, Privilegien(gegenüber anderen Betrieben) : ideelle, moralische Anerkennung), Erzeugen einer moralischen Bindung an die Firma, Identifikation mit der Firma (Siemensianer)
- Überprüfung der Tätigkeit,
- Protokollierung der Tätigkeit (Mitarbeiter soll informiert sein, dass alles protokolliert wird. Auswertung der Protokolle, Ziehen von Konsequenzen (für die Firma, für den Mitarbeiter) bis zur Entfernung von Mitarbeitern, die gegen die gesetzten und bekannten Regeln verstoßen – auf allen Ebenen (auch leitende Mitarbeiter).

Die Umsetzung ist z.T. schwierig, weil es widersprüchliche Zielstellungen gibt. Z.B Eigeninitiative vs. Kontrolle: Ein (technischer) Mitarbeiter wird mit ausreichend Arbeitsaufgaben versehen, hat Probleme mit den Vorgesetzten vor Lösung zu besprechen und die Verwendung seiner Arbeitszeit detailliert zu dokumentieren - ....
Der Mitarbeiter, von dem neuartige Lösungen erwartet werden, darf nur eingeschränkten Zugang zur direkten Realisierung seiner Ideen haben, muss dazu die Hilfe eines technischen Mitarbeiters in Anspruch nehmen. - Vier-Augen- Prinzip s.u.

Prinzip: Moralische Werte und Abschreckung durch die Konsequenzen.
Für alle Beteiligten müssen die Konsequenzen von Fehlverhalten klar sein und auch praktisch erlebbar sein. („Für alle Beteiligten“ bedeutet zum Beispiel, dass das Fehlverhalten ohne Ansehen der Person geahndet wird.)
Das Wissen um die (fast) sichere Entdeckung eines Angriffes schreckt Angreifer von innen ab.
(Gegenbeispiel: Vorgesetzter unternimmt nichts gegen Datenmanipulation geschützter Daten durch einen seiner Mitarbeiter, obwohl die Manipulation leicht beweisbar wäre,
Mögliche Konsequenzen: für Mitarbeiter nach § 303a StGB bis 3 Jahre Haft.
Für den Leiter: Strafvereitelung nach § 258 (1) StGB (in diesem Fall auch bis 3 Jahre Haft),
Sollte für den Leiter § 258a zutreffen (Strafvereitelung im Amt) bis 5 Jahre Haft.

Aus dem Beispiel wird klar: Auch Angriffe gegen den Datenschutz / die Datensicherheit können mit rechtlichen Konsequenzen abgewehrt werden – auch dort wo Bundesdatenschutzgesetz nicht zutrifft -
Dunkelziffer wird sehr hoch eingeschätzt. Tatsächliche Strafen fallen häufig viel geringer aus, haben weniger erzieherische Wirkung.

Technisch bedingte Angriffe (Ausfälle)

Allgemeines

Lebenszyklus von Geräten
(Ausfallrate /-wahrscheinlichkeit, „Badewannenkurve“: Frühausfälle, Normalbetrieb, Verschleiß)
Künstliche Alterung

Faktoren, die die Ausfallwahrscheinlichkeiten beeinflussen:

- Betriebsbedingungen grenzwertig (zu hoch, zu niedrig) : elektrische Spannungen, Temperaturen,
- sonstige Umweltbedingungen (schmutz, Staub, chemische Einflüsse (Flüssigkeiten, Dämpfe, Gase),
- elektrische, magnetische Felder
- bei Halbleitern insbesondere ionisierende Strahlung.

Sicherung gegen technische Ausfälle

- Vorsorge durch Prüfung und Auswechseln
- Technische Maßnahmen:
  Einbau von Schutzeinrichtungen (Überspannung), Temperaturüberwachung, Abschirmung (gegen energiereiche Strahlung)
- Redundante Auslegung
  (Rechenzentrum mit zwei unabhängigen Anschlussen an elektr. Netz, Kombination von USV (kurzzeitige sofortige Energielieferung) und Notstromaggregaten (die nach Anlaufzeit Energie liefern, Dieselaggregate – Pressluft liefert Startenergie), Rechnerverbünde, RAID-arrays bei Platten.
- Administrative Maßnahmen
  Maßnahmen zur Sicherung gegen technische Ausfälle (Pläne zur Organisation von Wartung usw., Verbote von Gefährdungen (Autoelektronik (Airbag, Abgasregelung) gestört durch starke HF-Felder, Hersteller verbietet Betrieb von Funkgeräten im Auto bzw. schreibt Platz für Montage der Antennen sowie abgestrahlte Maximalleistung vor).

Ausgewählte technische Ereignisse

Blitzschlag / Überspannung

Literatur: Führende Hersteller von Geräten, Materialien zum Blitzschutz, zur Überspannungsableitung beschreiben die Wirkung des Blitzes in Broschüren oder auf ihren WEB-Seiten. Es ist nicht möglich, dass hier Namen genannt werden.
(Google, Suchwort „Blitzschutz“)

Wirkung des Blitzes relevant für IT-Anlagen, Schutz ist möglich, Kenntnisse werden von Informatiker erwartet, da einfache Maßnahmen / Kenntnisse in tägliche Arbeit einfließen.
Planung und Ausführung von Blitzschutzanlagen nur durch Fachfirmen !
Wirkmechanismus: Blitzstrom erzeugt Überspannungen, die zur Zerstörung der Halbleiter führen.

Blitzparameter:
I=100 … 200kA,
U= mehrere MV, Durchschlag in Luft mehrere hundert Meter.
dI/dt ~100kA/µsec (Stromanstiegsgeschwindigkeit)
Blitzdichte in DL: ca. 4 Blitze / km².Jahr, abhängig von Landschaft.

Schäden (nach Versicherungsmeldungen in DL):
mehrere 100T Fälle/Jahr mit je ca. 1000 Euro Schaden.

Schadenswirkungen der Einschläge:
Direkteinschlag:

- Ohne äußeren Blitzschutz: Stromweg durch Gebäude, gesamte Installation unbrauchbar
  schwere Gebäudeschäden – Brände
- Mit äußeren Blitzschutz (Blitzableiter, Erder und Potentialausgleich:
  Übergangswiderstand Erder (Fundamenterder) – Erde : 1 Ohm (0,25 Ohm) -
  Gebäude auf 100 – 200kV „angehoben".
  Versorgungsleitungen bleiben auf Niveau des fernen Versorgers (ca. 0 Volt)
  -> Durchschläge (auch durch Mauern) , ca 100kV zwischen Adern des Stromnetzes (gn-ge wird angehoben, sw und bl bleiben auf 0 Volt. Kabeldurchschlag,
  100kV am Netzteil des Computers. 100 kV zwischen Gehäuse und Stromnetz – Totalausfall.

- Äußerer und innerer Blitzschutz
  Stufenweise Abbau der Überspannung durch Grobschutz, Mittelschutz (1,5kV) und Feinschutz (0,6kV/5kA). (0,4kV ist normale Spitzenspannung.) , eine richtig dimensionierte Schutzmaßnahme führt die Ströme im kA-Bereich kurzzeitg (msec) ab.
  Wichtig: Stufenkonzept – Feinschutz ohne Grobschuz bzw. ohne Mittelschutz ist zu schwach - d.h. Steckdoseneinsätze zu schwach – Zerstörung, ausreichende Leitungslänge zwischen Grob-Mittel-Feinschutz wirkt als Induktivität und bildet mit den Schutzelementen einen Tiefpass, dieser ist für Funktion wichtig.

  Analoge Konzepte für jede Ader jeder Leitung (Telefon, Fernsehen, …)
  -> aller Leitungen im Haus sind etwa auf dem Niveau der PAS, unabhängig von der Potentialhöhe.
  Am Gerät verbleiben nur so geringe Spannungsdifferenzen, dass sie unschädlich sind.

  Dazu noch Wirkung des Blitzstroms wie bei Einschlag in der Umgebung beschrieben.

Einschlag in der Umgebung:

- Potentialtrichter -> auch Anhebung des Potential wie bei Direkteinschlag, aber in geringerem Maße.

- Wirkung des Blitzstroms

dI/dt ~100kA/µsec (Stromanstiegsgeschwindigkeit)

- in einer Schleife wird eine Spannung induziert u = k dI/dt, k~ 5000V/(kA/µsec)
- Annahme, das der Blitz in einen Mast (Baum) einschlägt, der 1m vom Haus entfernt ist. Im Haus wird über die PAS folgender Leitungsverbund gebildet, der geometrisch ein Rechteck mit 10m Seitenlänge ist: Computer (Netzteil, Gehäuse) – Netzleitung – PAS – Telephonleitung – Modem (kleine unterbrechung (max. 10mm) – Datennetzkabel – Rechner (Netzkarte).
  Am Rechner entstehen zwischen Netzkarte und Gehäuse (bzw. zwischen Dateneingang und Masse) ca. 500kV (bei dieser Spannung haben Grob, Mittel und Feinschutz angesprochen, der Spannungsabfall über ihnen ist gleich der Brennspannung, Schalter u.ä. werden durch Lichtbogen überbrückt -> Fast 500kV Zerstören mindestens die Netzkarte.
- Schutz: keine großflächigen Schleifen (In einem Kabel von 10m Länge werden unter ähnl. Bed. ca. 1kV induziert.), Überspannungsableiter kurz vor Kabeleinführung in Computer (Gerät liegt im Nebenschluß des Ableiters)
  Omas Schutzschaltung: Bei Gewitter trenne man alle nicht unbedingt benötigten Geräte vom Netz (Stecker ziehen) und lege die Stecker mind. 1/2m von der Steckdose ab. Leider nicht 100% sicher, aber die ingenieurtechn. Lösung auch nicht und im gewerblichen Einsatz nicht ausführbar.

Engl. Stichworte: EMP – electromagnetic pulse, lightning.

Beispiele, wo Resistenz gegen Blitzschlag notwendig ist:

- Flugsicherung, Flugzeugelektronik und -informationssysteme,
- moderne Kraftfahrzeuge,
- Steuerungen von Industrieanlagen mit gefährlichen Stoffen (chem. Reaktoren, kerntechnische Anlagen, ...)

Details zu ingenieurtechnischer Lösung: Materialien von Firmen, die Blitzschutz anbieten. Verschiedene Schutzklassen möglich. Kein absoluter Schutz.

Kriegseinwirkung NEMP (nuclear electromagnetic pulse): eine Atomwaffenexplosion in der Ionosphäre erzeugt dort unvorstellbar starke Elektronen- und Ionenströme, deren elektromagnetische Wirkung auf der Erde großflächig (z.B. fast europaweit) alle ungeschütze Elektronik zerstört. (Suche in Wikipedia: NEMP)

Wirkung der Sonne

Sonne Strahlungsquelle für Strahlen aller Frequenzen. auch im UV-, Röntgen-, Gammabereich.
Zerstört Halbleiter (wichtig für Anwendungen im Weltraum)
Kommunikation (Internet) z.T. über Satelliten, Verfügbarkeit kann gestört werden.
Sonnenwind – Nordlichter – starke Ionenströme in Ionosphäre (mehrere 100 kA bis MA) – Magnetstürme.
Magnetstürme: beeinflussen Kurzwelle, Mittelwelle, Langwelle, Überreichweiten bei UKW
Stärke des Magnetfelds auf der Erde so, dass Transformatoren nicht mehr arbeiteten
Info: http://www.valdostamuseum.org/hamsmith/13Mar89.html#13Mar89.
6Mill. Menschen in der Province Quebec ohne Strom.

Technische Probleme beim Datenschutz:

Jede Datenübertragung an elektromagnetische Wellen gebunden.
Mit Ausnahme der Lichtübertragung über Lichtwellenleiter gibt es stets eine Abstrahlung dieser Wellen – bei Funkübertragung gewollt, bei Kabelübertragung ungewollt. - Ansatzpunkt für Angriffe.
Funkübertragung: Empfänger i.A. nicht feststellbar, E. muß sich nur im Empfangsgebiet aufhalten
Abwehr: kleine Sendeleistung,Richtantennen (Empfangsgebiet einschränken) – Verschlüsselung. (Problem verlagert zur Qualität der kryptograph. Verfahren) - Abschirmung von Räumen (Röhrenmonitor: liefert analoge Hochfraquenzsignale mit Bildinhalt – aus 10-20m sicher empfangbar, Schutz bauliche Maßnahmen, Abschirmung LCD: keine Aussage.).
Kabelübertragung: Abschirmung (verringert das Gebiet, wo das Feld zum Abhören reicht), Verschlüsselung – s.o.
Schutz des Kabels durch bauliche Maßnahmen vor Anzapfen, z.B. in Rohren mit Übertruck, Messung der technischen Parameter des Kabels.

Stand allgemein verfügbarer Technik:
Literatur: „SAT-Spionage für Insider. Geheime Satsignale sichtbar, lesbar machen“
PC + Empfänger für ca. 3000 Euro – alles übliche Handelsware.

Es ist nicht offengelegt: Was leistet Spezialhardware

Allg. Sicherheitsprobleme im DV-Anlagen
Wandel der Anforderunge in der Zeit:
früher: DV-Anlage setzte geschultes Personal voraus
Zugang /Besitz eines Rechners nicht allgemein, ausgewählter Personenkreis
heute: allgemeine Verfügbarkeit von Technik mit einer Leistung, die früher nur im Großrechenzentrum vorhanden war.
Vernetzung (Angriff von außen ohne phys. Anwesenheit)
Benutzung des Rechners ohne große Kenntnisse, es ist nicht kontrollierbar, welcher Nutzer tiefe Kenntnisse hat.
Miniaturisierung von Rechnern und Datenträgern (1CD ~ 350 000 Seiten Text, Speicher-Stick 16GB ~ 8 Mill. Seiten Text)

Folgen heute:
geringe Kenntnisse -> Passworte – schwache PW, Lexikonangriff , ...
Bewegliche Datenträger (Daten mit nach außen bringen, Daten einbringen, Viren einbringen)
(Schutz:
Baulich: Personenschleusen, Schleusen f. Datenträger,
Org. Maßnahmen: Sicherheitsrelevante Bereiche,
Überwachung, ZUgangskontrolle, Protokolle
Techn. Maßnahmen: (keine Laufwerke,..., Videoüberwachung)

Kontrolle des Transports (Organisatorisch, Verschlüsselung)

Strenge Kontrolle des Fernzugriffs: Protokolle, Kryptograph. Protokolle

3. Kryptographisches Grundwissen

Kryptographie: wichtiges Hilfsmittel zur Gewährleistung des Datenschutzes und für Teilaufgaben der Datensicherheit (Erkennung veränderter Daten). Dies gilt sowohl zum Schutz auf einer Maschine als auch insbesondere zum Schutz der Daten bei einer Übertragung in Kommunikationsnetzen.
Durch das Internet hat sich die Bedeutung dieser Verfahren deutlich erhöht.
Ziel der Verschlüsselung :primär *Schutz der Inhalte.,* heute auch die anderen Ziele.
Zu diesem Kapitel Literatur: Bruce Schneier: ...

Teilbereiche der Kryptographie:
Kryptologie, Kryptoanalyse, Steganographie
(Inhalte)

Was ist an Kryptographischen Verfahren geheim?
Auszug aus der WEB-Seite des BSI:
Der Einsatz von Freier Software ist mit technischen und strategischen Vorteilen verbunden, die durch die Freiheiten Freier Software wirksam werden: Einsatz, Lernen, Erweitern, Verteilen. Beim Einsatz der Freien Software sind dem BSI folgende technische Aspekte besonders wichtig:

1. Warnmeldungen über bei Sicherheitsprüfungen gefundene Fehler können veröffentlicht werden, weil es kein Non Disclosure Agreement gibt. Der Anwender kann so bei Sicherheitslücken schnell informiert werden und Gegenmaßnahmen ergreifen.
2. Die Prüfung von Software auf Sicherheitslücken sollte immer möglich sein. Beim Einsatz von Software kann dies ein KO-Kriterium sein. Es steht Vertrauen versus Wissen.

<Endes des Auszugs>

Was hier für Software gesagt wird, ist in ähnlicher Weise auch für die Kryptographie zutreffend. Die Verfahren, Protokolle und selbst die Implementierungen sollten aus Sicht des Anwenders offen sein. Nur so können Fehler (aller Art) gefunden werden. Die Sicherheit entsteht durch die geheime Wahl eines Parameter.
Warum ist das sicherer?
Allg. Feststellung: Moderne Kryptographie beruht auf Wissenschaft.
- Schwachstellen eines Verfahrens werden (in wissenschaftl. Gemeinschaft) gefunden und diskutiert.
- Der Angreifer darf nicht unterschätzt werden, er hat i.A. dasselbe Wissen wie der Hersteller der Verschlüsselung, selbst wenn er zeitweilig ein Verfahren nicht kennt – er wird es bald kennen.
- Mit Herstellung eines Verfahrens sind meist mehrere Personen befasst. Wenn das Verfahren geheim ist, müssen die alle zuverlässig sein. Es ist sicherer, wenn nur zwei (Seiten) einen geheimen Parameter eines sonst offenen Verfahrens vereinbaren.

Def.: Protokoll – Folge von Einzelaktionen, die i.A. verteilt zwischen mehren Partnern ablaufen, um von einen Ausgangszustand des Systems zu einem Zielzustand zu gelangen.

Datenübertragungsmodell: (Quelle) Sender – Kanal – Empfänger (SENKE)
(Kanal kann auch als ein Speicher oder eine andere techn. Einrichtung realisiert sein).
Im Modell gilt der **Kanal** als gestört bzw. hier als **unsicher.**

Siehe auch: Klaus Köhler: Krypologie , Vorlesungsscript, FH München
(http://www.informatik.fh-muenchen.de/~koehler/crypto/krypto.pdf)

Kryptographische Protokollbeschreibungen gehen i.a. von Rollen aus, die bestimmte Eigenschaften realisieren.

Rollen in Protokollbeschreibungen:
Alice, **B**ob, **C**arol / Charly , **D**ave (allg. Teilnehmer – Eigenschaften protokollabhängig)
Eve (Eaves dropper – passiver Angreifer, kann nicht verändern)
Mallory / Oscar (malique – aktiver Angreifer, kann verändern usw.)
Trent (trusted person -Notar: Grundeigenschaften: absolut vertrauenswürdig, wird von allen akzeptiert, macht keine Fehler)
Viktor (verifier)
Peggy (proof)
Walter (watcher – beobachtet bei manchen Protokollen wie ein Wächter im Besuchsraum eines Gefängnisses aus gewisser (respektvoller) Entfernung, z.B. bei verdecktem Kanal))

Detaills und weitere Rollen: http://en.wikipedia.org/wiki/Alice_and_Bob

Typische Angriffe: (Liste erweiterbar,)
a) Passives Mitlesen eines Datenstroms (eye dropper -Eva) ,
Schutz: Verhindern des Zuganges, Krypt. Verschlüsselung.

b) Aktive Teilnahme mit Datenveränderung (malique - Mallet),
Schutz : + div. Kryp.Protokolle
Hier Man-in-the-middle einordnen
(Serverangriffe – Identität eines Dienstanbieters annehmen und fehlerhafte Dienste erbringen, Nameserverattaken)
MiM-Attacke ist grundsätzlich immer dann möglich, wenn es kein vorher auf einem sicheren Wege vereinbartes Geheimnis gibt .
– vgl. Schlüsselaustausch im ssh-Protokoll
c) Empfänger leugnet Erhalt des Inhalts: Vergleich mit Einschreiben, Zustellung durch Gerichtsvollzieher, ohne Mitarbeit des Empfängers nur durch Einsatz eines glaubwürdigen Drittens (Zeuge, Notar), elektron. Lösung ist nicht besser.

d) Sender leugnet, gesendet zu haben: unsymm. Kryptographie.
- hier wird mehr erreicht als im Leben.

Was ist schützenswert?

a) Inhalt der Nachricht – Schutz: Schutz vor Mitlesen, Verschlüsselung
b) Senderidentität (Anonymisierungdienste)
c) Empfängeridentität (Rundsprüche, Anonymisierungsdienste)
d) Tatsache, dass eine Kommunikation stattfand (Anonymisierungsdienste, Rauschen)

Was ist zu sichern?

a) Integrität der Nachricht
b) Nachweis der Identität des Senders und der Tatsache des Sendens
c) Nachweis der Tatsache des Empfangs.

Die unterschiedlichen Schutzziele und die Forderung nach Resistenz gegen die Verschiedenen Angriffe bestimmt die Auswahl der Verfahren und der Protokolle zur Anwendung der Verfahren.

Theoretische Sicherheit von Verschlüsselungsverfahren.

Def. Theoret. Sicherheit. (a-posteriori-Wahrscheinlichkeiten)

One-time-pad als theoretisch sicheres Verfahren,
Redundanz reduziert Sicherheit (Beispiel) – erfordert bei Datenschutz evt. Kompensationsmaßnahmen.

Symmetrische und unsymmetrische Verfahren

Definitionen:

Symmetrische Verschlüsselungsverfahren,
unsymmetrische Verschlüsselungsverfahren.

Beispiele:
Symmetr.: One-time-pad, DES (http://de.wikipedia.org/wiki/Data_Encryption_Standard)
Symmetr. Verschlüsselung sagt nur, dass derselbe Schlüssel zum Ver- und zum Entschlüsseln genommen wird, die Art der Berechnung für beide Richtungen wird sich im allgemeinen unterscheiden (z.B. DES Reihenfolge der Runden)

Unsymmetr.: RSA,
(Mathematische Grundlagen zum RSA-Algorithmus in der Literatur nachlesen bzw. auf http://de.wikipedia.org/wiki/RSA-Kryptosystem)

Vergleich: Symmetr. vs. unsymmetr. Verfahren

Komplexität der Schlüsselverwaltung,
Arbeitsgeschwindigkeit , Rolle von hybriden Verfahren.
DES- Hardware – Sprachverschlüsselung möglich.

In der Praxis: Hybride Verfahren - Wie arbeiten diese im Prinzip?

Protokolle:

Definition Protokoll:
Folge von Handlungen, die ein System aus einem (bestimmten) Ausgangszustand in einen Endzustand mit bestimmten Eigenschaften überführt.

Schlüsselaustauschproblem (Def. des Problems)
(bei symmetr. Verfahren, bei unsymmetr. Verfahren),

Verfahren zum Schlüsselaustausch mit /ohne Notar bei symmetr. Verfahren.
Direkter Nachrichtenaustausch (Nachweis des Senders – Beweis gegenüber Dritten, Nachweis des Empfangs ?)
Nachrichtenaustausch über Notar **ohne** Archivierung der Nachrichten
Nachrichtenaustausch über Notar **mit** Archivierung der Nachrichten

Schlüsselaustausch bei unsymm. Verfahren, Authentizitätsproblem,
(the man-in-the-middle-Angriff: wie erfolgt er?) , Vertauenshierarchien (Schlüsselzentren).
Wann ist ein Verfahren grundsätzlich nicht immun gegen Man-in-the-middle-Angriff?

Diffie-Hellman:
http://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch
Ablauf

Signaturen
Verschlüsselung zur Signatur (Symmetr. / unsymmetr.).
Was bedeutet „Signatur“ ?
(Bestätigung einer Eigenschaft eines Dokuments ,
Willentlicher Vorgang, vergleichbar mit Unterschrift – kein Signierautomat !
Bestätiger ist identifizier)

Einfache elektronische Signatur: Merkmale, rechtliche Beweiskraft ?
fortgeschrittene elektronischen Signatur : (§2 Nr.2 SigG)
LIT: http://de.wikipedia.org/wiki/Elektronische_Signatur

Was beweist Signatur?
(Bei symmetr. Verfahren kein Beweis (der Id. des Senders oder der Eigenschaften) gegenüber Dritten,
bei unsymmetr. Verfahren Identifikation des Senders und der Eigenschaften gegenüber Dritten. Die „Willentlichkeit der Signaturhandlung) muss durch organisatorische Maßnahmen i.a. abgesichert werden!)

Problem der Empfangsbestätigung (Notar vs. schrittweiser Austausch)

Hashfunktionen und Signatur.
Definition Hashfunktion, Was sind „hard problems“; Kollisionsproblem, Erzeugung eines Dokuments gegebenem Inhalts und gegebenen Hashwerts.
Vorteile des Einsatzes von Hashfunktionen. (geringeres Volumen. Varianten der

Bestätigung des Senders ohne den Inhalt zu offenbaren mit Notar.)

Was ist außer dem Inhalt noch schützenswert?
(Senderidentität,
Empfängeridentität,
Tatsache der Kommunikation):

Geheimhalten der Kommunikation an sich:
a) Rauschen auf dem Kanal .
b) Verdeckte Kanäle (Steganographie,
[Was ist ein verdeckter Kanal? Progammstart-Beispiel, Kanäle im Hashwert,
in Signatur,..., Länge der Grashalme in einer Strichzeichnung ergibt Morsekode, Nutsi])
c) Anonymisierungsdienste als Netzwerk. (Funktionsschema, Sicherheit durch großes Datenaufkommen,

Senderidentität: Anonymisierungsdienste
Empfängeridentität: Broadcasting, Anonymisierungsdienste

Geheimnisteilung
grundsätzliches Verfahren ,

(m,n)-Schwellwertverfahren,

4. Grundfunktionen sicherer Systeme

1. Indentifikation
2. Authentifizierung
3. Rechteprüfung
4. Rechteverwaltung
5. Protokolle und Protokollauswertung
6. Fehlererkennung, Fehlerbehebung
7. Wiederaufbereitung
8. Probleme im Netz.

4.1 Identifikation: Jede Komponente im System hat eine Identität, insbesondere Nutzer. Es wird unterstellt, dass diese Identität fest ist, genauer, dass es schwierig ist, die Identität zu wechseln (ohne dass dies bemerkt wird). (Unterschied: Nutzer in Betriebssystem vs. Teilnehmer an P2P-Systemen, bei letzterem ist Wechseln leicht, Nichtwechseln wird aber „belohnt“.)

4.2 Authentifizierung: Nachweis, dass eine Komponente die angegebene Identität wirklich besitzt.

Unvernetzte Rechner (oder Konsole): Unterstellung, dass der Rechner korrekt arbeitet, nur der Nutzer authentisiert sich. (im Netz: kein Vertrauen – wechselseitige Authentisierung

-ssh).

Authentisierung durch Besitz (von Gegenständen , auch von biometr. Merkmalen) oder durch Wissen.

Besitz: Gefahr durch Verlust, Fälschung , Erpressung

Fälschung nicht verhinderbar, Sicherheit: Aufwand zur Fälschung muß höher sein als der erzielte Nutzen, schützt nicht vor idealistischem Fanatismus.

Wissen: Versch. Verfahren.

Mit Übertragung des Wissens (z.B. Passwortverfahren): Übertragung des Wissens ist verfahrensbedingte Schwachstelle (im unvernetzten Rechner und Stand der Rechnerverbreitung 1985 akzepierbar, 2005 unakzepabel, zusätzlicher Schutz nötig (z.B. ssh, ...)). Dazu noch Anwenderbedingte Schwachstellen: schwache Passwörter.

Verbesserungen:
Einmalpassworte: (Bespiel TAN), Schutz vor Wiederverwendung; Algorithmus zur Verwendung von Einmalpassworten mit Hashfunktion.

Zero-Knowledge-Protokolle (Authentifizierung ohne Übertragung des Wissens):

Beispiel Cardani-sche Formel.

Nichteignug eines Public.key-Verfahrens (PGP, RSA) (es wird Wissen übertragen, Nutzer signiert Nachricht, deren Bedeutung er nicht kennt (falls kommutativ Schlüssel vorliegen : Unterschrift unter beliebiges Dokument möglich!)).

Geeignete spezielle Public-Key-Verfahren:
Feige-Shamir (1 bit wird noch übertragen)
Fiat-Feige-Shamir

Details zu beiden Verfahren: Wikipedia.

http://de.wikipedia.org/wiki/Fiat-Shamir-Protokoll

http://en.wikipedia.org/wiki/Feige-Fiat-Shamir_Identification_Scheme

4.3 /4.4 Rechteprüfung / Rechteverwaltung:

Subjekt-Objektmodell: Definitionen Subjekte, Objekte, Doppelrolle von Programmen

Rechte: Attribute der Beziehung zwischen Subjekten und Objekten.

Arten der Rechte: read, write, append, create, alter, ..., grant, revoke.

Grant – Revoke: Problem der Rechteweitergabe und von Entzugsketten, Rechtegraph.

Klassifikationen: Offen vs. abgeschlossen

Definition: Offenes System:
Abgeschlossenes System:

Diagramm zur Rechteprüfung im abgeschl. und im offenen System.

Folgerung zur Sicherheit.

Klassifikation: Zentrale Verwaltung vs. dezentrale Verwaltung

Vor- und Nachteile.

Klassifikation: MAC vs. DAC (Stand 15.1.08)
MAC (mandadory access control) Regelbasierte Zugriffskontrolle, vorgeschriebener Zugriffsschutz.

s. auch: http://de.wikipedia.org/wiki/Mandatory_Access_Control

DAC (discretionary access control) Individuelle Zugriffskontrolle
s. Auch: http://de.wikipedia.org/wiki/Discretionary_Access_Control

MAC liefert tendenziell sicherere Systeme – bei höheren Anforderungen Pflicht (s. später F-Klassen),

Weitergabe von grant und revoke : siehe oben.

Häufig Mischformen Windoes, UNIX (individuelle Vergabe, aber Regeln zur Vererbung in Unterverzeichnisse, Regeln bei neu erstellte Dateien, ...)

in Betriebssystemen: Rechte auf Datei und Verzeichnisebene, Trend zur feineren Unterscheidung, z.B. in DBVS: Rechte auf Attributbasis, bisher wenig realisiert Rechte auf Contentbasis (in DB: nur Zugriff auf aggregierte Daten, nicht auf Einzelwerte,) oder kontextabhängige Rechte (wertabhängig , zeitabhängig, history-abhängig).

Realisierungen: (Beispiele)

Matrix-Modell: Matrix der Subjektze-Objekte. Elemente: Vektor der Rechte, die ein konkretes Subjekt an einem konkreten Objekt hat.

Leicht zu implementieren, Hoher Aufwand, zur Verwaltung, insbesondere wenn Prinzipien durchzusetzen sind.

Verbesserungen: Gruppeneinteilungen – Rollen, Übergang zu regelbasierten Systemen oder Mischformen.. Rechtevergabe auf Gruppenbasis, Gruppenmitglieder „erben“ die Rechte der Gruppe.

Schutzklassenmodelle (multi level systems)

Bell – LaPadulla Modell (1976 ? David Elliott Bell , Leonard J. LaPadula, US-Air-Force)
Wie klassifizierbar: MAC; Mehrstufensystem kombiniert mit Prinzip der Zuständigkeit.

s. auch: http://de.wikipedia.org/wiki/Bell-LaPadula

Ziel: Verhindert „Abfluß“ von sehr schutzenswerten Informationen in Bereich mit weniger Vetrauen.

Leseregel

Schreibregel

Probleme: Person mit hohem Vetrauen kann nur hoch zu sichernde Informationen erzeugen; Lösung: Abstufung der erzeugten Informationen durch Berechtigten (Fachkenntnisse ? , Flaschenhals ?)

oder Person darf selbst abstufen (Sicherheitslücke)

Zustand „system high“: Wenn eine Systemkomponente das Stufenprinzip nicht erfüllen kann, nimmt das gesamte System den Zustand an, der durch die höchste auftretende Sicherheitsstufen bei den Objekten definiert ist.

Biba-Modell (1977 Kenneth J. Biba)

s. auch: http://de.wikipedia.org/wiki/Biba-Modell

Sicherung der Integrität und Qualität der Daten.

Schreibregel:

Leseregel:

Beispiel: Computer liest Liste vertrauenswürdiger Hosts. Er darf nur Listen lesen, die nicht niedriger eingestuft sind als sein eigenes Sicherheitsniveau. Die Liste kann maximal das Niveau des Schreibers haben.

Clark-Wilson- Modell(1987 David D. Clark , David R. Wilson)

s.auch: http://de.wikipedia.org/wiki/Clark-Wilson-Modell

Regeln auf Server, Veralgemeinerung der Transaktionseigenschaften.

Menge sicherer Transaktionen nur solche werden im sicherheitsrelevanten Bereich ausgeführt. Zertifizierung notwendig.

4.5 Protokolle

Forderungen an Protokolle:

1.

2.

3.

Diskussion Umfang der Protokolle vs. Auswertbarkeit
Semiautomatische Auswertung

Rollen, Autonomie der Rollen
Mögliche Rollen mit Funktionstrennung:

Leitung des Unternehmens (wirtschaftliche, technische)
Leitung der IT-Abteilung
Systemverwaltung

Systemprogrammierer
Anwendungsprogrammierer
Techniker
Nutzer, Kunden
Kontrollperonal (Protokollauswertung)

4.6 Fehlererkennung, Fehlerkorrektur

Mittel: Redundanz.
Genaue Zielanalyse als Voraussetzung für Lösung
Lösung können Hard- und Softwarebasiert sein (fehlerkorrigierende Kodierung – s.a. intene Datenspeicherung auf Festplatten)

Kritische Bewertung der konkreten Lösungen –

Raid-Array Fehlertoleranz durch Redundanz der Platten,
neue Schwachstelle: Raid-Kontroller – aber Ausfallwahrscheinlichkeit der Elektronik geringer als die der mechan. Platten.

Raid-Array ungeeignet als Backup-Ersatz:
1) Versehentlich falsche Daten werden „durchgeschrieben“ - keine Speicherung des Zustands vor dem Schreiben , keine Rückkehr möglich.

2) Backup kann räumlich getrennt von operativen Daten gelagert werden – Schutz vor Vernichtung durch Katastrophen, Diebstahl, ...

Redundante Stromversorgung: USV -kurzzeit, Notstromaggregate: Dauerlösung, Abgestimmtes Konzept notig, Anlauf- und Übernahmezeiten.

Festgelegte Werte zur Ausfallsicherheit: Flugzeuge, Industrieanlagen
Math. Untersuchungen mit Mitteln der Bedienungstheorie.

Begriff Hochverfügbar

4.7 Wiederaufbereitung

Aufgabe des Betriebssystems,

Historische Entwicklung

Anforderungen

5 Zertifizierung

Lit.: IT-Grundsicherungshandbuch : a.a.O., insbes. Kap.7

Aus WEB-Unterlagen des BSI:

Allgemein anerkannte Zertifikate setzen **Maßstäbe** und schaffen **Vertrauen**. Auch im Bereich der Informationssicherheit sind verlässliche Standards wünschenswert, die den Anwendern Orientierung zur Sicherheit von Produkten, Systemen und Verfahren bieten. So gibt es bereits seit vielen Jahren international anerkannte Kriterienwerke, auf deren Grundlage die

Sicherheitseigenschaften von Produkten und Systemen durch unabhängige Zertifizierungsstellen bestätigt werden können.

Seit Herbst 2005 gibt es mit der aus dem British Standard 7799 entstandenen ISO**-Norm 27001** erstmals einen internationalen Standard, der die Zertifizierung von Managementsystemen für Informationssicherheit ermöglicht. Es lag nahe, das bisherige IT-Grundschutz-Zertifikat an dieser Norm auszurichten und zum **ISO 27001-Zertifikat auf Basis von IT-Grundschutz** weiterzuentwickeln. Eine IT-Grundschutz-Zertifizierung wird damit auch für international tätige Organisationen attraktiv.

6.

1989 Orange Book USA erster Standard,

Klasse D (minimaler Schutz) – praktisch unzureichend.
Klasse C1 (benutzerbestimmbare Zugriffsrechte - DAC)
Klasse C2 (kontrollierte Zugriffe - MAC)
Klasse B1 (Kennzeichen)
Klasse B2 (Strukturierung)
Klasse B3 (Sicherheitsdomänen)
Klasse A [Unterteilung vorgesehen] (Verifikation gefordert)

Kritische Wertung des Orange book.
Was ist Gegenstand der Zertifizierung

Was wird mit Zertifizierung erreicht.

F-KLassen in DL

Vergleich mit Orange book.

F1-F5 aus Kompatibilitätsgründen abgestimmt:
F1 – (C1): Benutzerbestimmbarer Zugriffsschutz.
F2 – (C2): Mechanismen zur Protokollierung.
F3 – (B1): Festgelegter Zugriffsschutz.
F4 – (B2) : Vertrauenswürdiger Zugriffspfad.
F5 – (B3/A) : ¨Überwachung sicherheitskritischer Ereignisse.

Weitere Merkmale, die nicht im O.B.

F6 – Systeme mit hohen Anforderungen an die Datenintegrität (etwa Datenbanken).
F7 – Systemverfügbarkeit (etwa bei Prozeßrechnern)

Weitere Kriterien : Arbeit im Netz, Realisierung erfordert i.A. kryptographische Techniken

F8 - Integrität der Daten bei Datenübertragungsmodell
F9 - Geheimhaltung der Daten bei Datenübertragung
F10- Vertraulichkeit und Integrität in Netzen

IT-Sicherheitshandbuch:
„Die in den Sicherheitskriterien vorhandenen Funktionalitätsklassen können ergänzt werden. Aus einem Sicherheitskonzept können sich Anforderungen an die Funktionalität eines Systems ergeben, die durch keine der vorgegebenen Funktionalitätsklassen abgedeckt sind. In diesem Fall können entweder vorhandene Funktionalitätsklassen kombiniert werden oder die Anforderungen einer Funktionalitätsklasse können um die notwendigen Anforderungen ergänzt werden. Dabei kann es sich um Zusatzforderungen an eine Grundfunktion handeln, die erst in einer anderen Funktionalitätsklasse definiert sind.
Prinzipiell können IT-Systeme oder Teile davon nach allen - von Herstellern oder Anwendern - formulierten Sicherheitsanforderungen evaluiert werden. Für eine Evaluierung sind also beliebige Anforderungen möglich, die außerhalb der oben beschriebenen Funktionalitätsklassen liegen. Deshalb sind evaluierte Systeme denkbar, die in keine der vorgegebenen Funktionalitätsklassen passen.“

Qualitätsstufen
(Quelle: Kersten : a.a.O)
(Q = Stärke des Mechanismus + Qualität der Implementierung)
Warum Zusammenfassung ?

Stärke des Mechanismus
Definition Mechanismus: Methode, Verfahren, Algorithmus, mit denen eine Funktion realisiert wird.

Bewertungen:

a) *ungeeignet*: nicht wirksam
b) *schwach:* Abwehr unbeabsichtigter Angriffe
c) *mittelstark:* Schutz bei beabsichtigten Angriffen, mit mittlerem Aufwand bei normalen Systemkenntnissen auszuhebeln.
d) *stark:* gute Abwehr beabsichtigter Angriffe,
großer Aufwand od. aufwendige Hilfsmittel zur Überwindung
Falls org. Maßnahmen nötig , dann einfach, wenig fehleranfällig
bei fehleranfälligen Maßn. - Mechanismen zur Fehlererkennung.
e) *sehr stark:* sehr guter Schutz, Bruch erfordert sehr gr. Aufwand und sehr aufwendige Mittel. Org. Maßnahmen rel. einfach und systemüberwacht, werden mit zertifiziert.

f) nicht überwindbar: gelten zur Zeit als nicht überwindbar, Org.
Maßnahmen durch System praktisch vollständig abgesichert.

Bewertung zeitabhängig, bezieht sich auf den aktuellen Stand der Technik, des Wissens, der Möglichkeiten.
Beispiel: Wörterbuchangriff 1970 und heute.

Für einige Funktionen liegen Anforderungen in Form von Zahlenparametern vor:

Korrektheit der Implementierung
unzureichend (A), getestet (B), methodisch getestet (C), methodisch getestet u. teilanalysiert (D), informell analysiert (E), semiformal analysiert (F), formal analysiert (G), formal verifiziert (H)

In den IT-Sicherheitskriterien werden Maßstäbe für die Bewertung der Qualität von IT-Systemen und ihren Bestandteilen vorgegeben. Der Begriff "Qualitä" ist dabei im Sinn von Vertrauenswürdigkeit zu verstehen.

Die Qualität wird durch die folgenden Aspekte bestimmt: (IT-Sicherheitshandbuch)

- Darstellung der Sicherheitsanforderungen,
- Art der Spezifikation,
- Stärke, mit der die Mechanismen realisiert sind,
- Abgrenzung zu nicht sicherheitsrelevanten Funktionen,
- Verfahren bei der Herstellung,
- Verfahren im Betrieb,
- Güte der Dokumentation für den Anwender, die eine korrekte Anwendung der Sicherheitsfunktionen ermöglichen

Überblick Qualitätsstufen
Konjunktive Verknüpfung Besonderheit bei Q0: disjunktiv

Stufe	**Mechanismus**	**Korrektheit**
Q0	unwirksam/schwach	unzureichend (A)
Q1	mittelstark +)	getestet (B)
Q2	mittelstark	methodisch getestet (C)
Q3	stark +)	methodisch getestet u. teilanalysiert (D)
Q4	stark	informell analysiert (E)
Q5	sehr stark +)	semiformal analysiert (F)
Q6t	sehr stark	formal analysiert (G)
Q7	nicht überwindbar	formal verifiziert (H)

Besonderer Beachtung bei Prüfung: Schnittstellen zum unzertifizierten Teil, Gefahr eines verdeckten Kanals.

Vergleich mit Orange Book:
C1 ~ F1+Q2
C2 ~ F2+Q2
B1 ~ F3+Q3
B2 ~ F4+Q4
B3 ~ F5+Q5
A ~ F5+Q6

Beispiele.

(Suche im WEB nach „BSI Zertifikat“ - liefert u.a. Einträge (von Firmen) über (ihre) zertifizierten Produkte.)

Kostenfragen

(Quelle Kersten, a.a.O.) Stand 1990:

(Team 3-6 Personen, 50% der Arbeitszeit, vollständige Dokumente, keine Nachbesserungen, Testinstallation vorhanden)

Evaluationsdauer (in Monaten)

Produktklasse	Q1	Q2	Q3
PC	3	3-6	6
UNIX	6	9	12
Main-Frame	12	24	>24

Wahrscheinlich sind diese Zeiten veraltet, da Betriebssysteme auf PC viel Komplexer geworden sind, andererseits mehr Erfahrungen vorliegen, was zu schnelleren Resultaten führen kann, dennoch geben Sie eine Vorstellung vom Aufwand!

Evaluierung setzt Erfahrung voraus und die ständige Weiterbildung der Mitarbeiter.

Evaluierungsprozess:

3 Phasen, Zertifizierung als kooperativer Prozess

Vorbereitungsphase:

Beratung, Festlegen der *angemessenen F-Klassen und Q-Stufe*.
Festlegen der Unterlagen, Hardware, ... -> Vetrag

Evaluierungsphase: (Auditoren)

Testinstallation,
Einreichung und Prüfung der Unterlagen, der Dokumentation.
Tests des Produkts entsprechend der angestrebten F-Klasse und Q-Stufe mit Protokoll, evt. Nacharbeiten/Nachbesserungen (Nachbesserungszyklen)
-> Interner Bericht

Abschlußphase: (Zertifizierungsstelle)

Überprüfung der Berichte und Protokolle auf Konsistenz (unabhängiges Team)
Erstellung des Zertifikats und der

Inhalte: Erreichtes Level, Anmerkungen zum Einsatz.

Das eigentliche Zertifikat enthält die vom evaluierten IT-System erfüllte Funktionalitätsklasse oder Kombination von Funktionalitätsklassen und die erreichte Qualitätsstufe. Fällt das System in keine der vordefinierten Funktionalitätsklassen, werden,

eventuell ergänzend zu einer vordefinierten Funktionalitätsklasse, die erfüllten Sicherheitsanforderungen des evaluierten Systems beschrieben. Im Zertifikat sind auch die Randbedingungen beschrieben, unter denen das Zertifikat Gültigkeit hat, wie beispielsweise die Version des Systems und die Hardware- und Software-Konfiguration, die evaluiert worden ist. Ebenso wird die Version der zugrundeliegenden IT-Sicherheitskriterien angegeben.

Der öffentliche Teil des Anhangs enthält eine detaillierte Beschreibung der erfüllten Sicherheitsanforderungen. Der Leistungsumfang der vorhandenen Sicherheitsfunktionen wird darin genau beschrieben, z.B. die Art und die Granularität der vorhandenen Zugriffsrechte und der Objekte, welche der Rechteverwaltung und der Rechteprüfung unterliegen, oder die Bedingungen, die bei der Beweissicherung spezifiziert werden können. Alle Hardware- und Software-Konfigurationen, für die das Zertifikat Gültigkeit hat, werden aufgeführt. Die Dokumente für den Anwender, die für den Betrieb des evaluierten Systems erforderlich sind, werden aufgelistet. Für den Anwender von besonderem Interesse sind die Hinweise auf kritische Bereiche bei den einzelnen Sicherheitsfunktionen, da sie für die Systemauswahl entscheidend sein können. Beispielsweise wird auf notwendige organisatorische Maßnahmen hingewiesen, ohne die Schwächen von Mechanismen zu Sicherheitslücken werden können.

Der nicht-öffentliche Teil des Anhangs enthält Informationen über den Entwicklungsvorgang, die interne Struktur des Produkts und den Evaluationsprozeß, die nur für den Hersteller und die Prüfbehörde wichtig sind.

Gültigkeit:

abhängig von Art, kann zeitlich befristet sein.

muss ergänzt werden, wenn die Voraussetzung verändert sind (z.B. bei Software neuer Compiler, neue Bibliotheken, Kombination mit anderer Software, evt. auch bei Weiterentwicklung (neue Algorithmen, neue Funktionalität)

Wichtige Eigenschaften des Zertifikats (IT-Sicherheitshandbuch)

Das Zertifikat eines Systems

- enthält keine Aussage, ob das System den operationellen Anforderungen für eine spezielle Anwendung genügt,
- enthält ab Qualitätsstufe Q2 Aussagen darüber, gegen welche Bedrohungen die Sicherheitsfunktionen des evaluierten Systems wirken,
- garantiert nicht, daß das System fehlerfrei ist,
- bürgt nicht für absolute Sicherheit,
- verliert seine Gültigkeit, wenn das System nicht unter den vorgeschriebenen Randbedingungen oder nicht vorschriftsmäßig eingesetzt wird. Beispielsweise kann eine Modifikation des Systemprogramms Sicherheitsfunktionen außer Kraft setzen.