Datenschutz und Datensicherheit

1. Datenschutz

→ Aufgabe:

- die Privatsphäre
- das Selbstbestimmungsrecht und
- die persönliche Integrität von Personen
  vor dem Missbrauch durch Dritte zu schützen

Datenschutz schützt Personen vor dem Missbrauch ihrer Daten durch Dritte.

→ **natürliche und juristische Personen**

Datenschutz erstreckt sich auf

- Erhebung von persönlichen oder personenbezogenen Daten
- Speichern von persönlichen oder personenbezogenen Daten
- Übermittlung von persönlichen oder personenbezogenen Daten
- Verarbeitung von persönlichen oder personenbezogenen Daten
- Veränderung / Löschung von persönlichen oder personenbezogenen Daten

Datenschutz ist keine Erfindung der Neuzeit

- Beichtgeheimnis
- Bankgeheimnis
- ärztliche Schweigepflicht
- Postgeheimnis

aber: Nutzung der elektronischen Datenverarbeitung vereinfacht das missbräuchliche Sammeln, Verarbeiten, Weitergeben von Daten sehr.

↓

gesetzliche Regelung in umfangreichen Maß notwendig!

↓

Datenschutzgesetz

gilt für:

→ öffentliche Stellen und

→ nicht öffentliche Stellen, die gewerbsmäßg mit personenbezogenen Daten arbeiten

1.1 Gesetzliche Grundlagen für den Datenschutz

Bezüglich des Datenschutzes gelten in Deutschland mehrere Gesetze und Verordnungen

- das Grundgesetz der Bundesrepublik Deutschland (GG)
- das Bundesdatenschutzgesetzt (BDSG)
- die einzelnen Landesschutzgesetze (LDSG)
- das Telekommunikationsgesetz (TKG)
- die Telekommunikation-Kundenschutzverordnung (TKV)
- das Informations- und Kommunikationsdienste- Gesetz (IuKDG)
- das Signaturgesetz (SigG)
- die Signaturverordnung (SigV)
- die Europäische Datenschutzrichtlinie

Das Datenschutzgesetz benennt die Grundsätze des Datenschutzes sowie besondere Rechte des Einzelnen gegenüber Eingriffe in seine Privatsphäre.

1.2 Grundsätze des Datenschutzes

- Relevanz / Sparsamkeit bei der Datenerhebung (§ 3a, 6a, 6b, 13, 28)
  Es dürfen nur Daten erhoben, gespeichert und verarbeitet werden, die für dn beabsichtigten Zweck relevant sind.
- Publizität / Transparenz / Öffentlichkeit (§ 4, 4a, 19, 19a, 33, 34)
  Jeder Betroffene hat das Recht auf Auskunftserteilung, welche personenbezogenen Daten gespeichert worden sind.
- Richtigkeit ($ 6, 20, 35)
  Jeder Betroffene hat das Recht auf Richtigkeit der gespeicherten Daten. Dies beinhaltet ebenfalls das Recht auf Berichtigung bzw. Löschung falscher Daten.
- Weitergabebeschränkung ($ 4b, 9, 15, 16, 19, 28, 28a)
  Regelungen zur Kontrolle der Datenverwendung und Einschränkungen der Datenweitergabe bzw. -übermittlung.
- Verpflichtung zu Datensicherungsmaßnahmen (§ 9, 9a)
- Geheimhaltungspflicht (§ 5)
  aktenkundige Belehrung über Umgang mit Daten
- Schaffung von Kontrollorganen (§ 4f, 4g, 24, 38)

1.3 Absicherung gegen Viren, Würmer und Trojaner

Virus:

- Programmcode, der auf Schaden an Soft- und/oder Hardware abzielt
- allein nicht lauffähig, braucht unbedingt ein Wirtsprogramm, dessen Ablauf durch die Infektion verändert wird
- reproduziert sich
- versteckt sich
- mehrere Funtkionsteile
  - Reproduktion
    - Erkennungsteil (Scan auf eigene Signatur)
    - Infektionsteil (Kopieren in ein Programm)
  - Funktionsteil
    - Auslösefuntkion
      prüfen ob Schadfunktion werden soll
    - Schadensfunktion
      verschiedene Möglichkeiten, i.d.R. Zerstörung/Manipulation von Soft-/Hardware

<u>Einteilung von Viren</u>

(je nach Kriterien verschiedene)

- Einteilung nach dem Infektionsziel
  - Bootviren
    schreiben Anweisungen in den Bootsektor eines Boot Datenträgers
  - Dateiviren
    schreiben Anweisungen in ausführbare Programmdateien
  - Makroviren
    schreiben Makros in Anwenderdateien

<u>Infektionswege</u>

- Datenträgeraustausch
- Kopieren von Programmen
- Netzwerke

<u>Gegenmaßnahmen</u>

- Verzicht auf (s.o. Infektionswege) wenn möglich
- stilllegen nicht benötigter Laufwerke/Datenträger

- keine fremden Dateien ungeprüft einlesen
- regelmäßiger Virenscan mit aktueller Antivirensoftware und Datenbank
- Organisation, Regelungen
- neue Programme in einer virtuellen Umgebung testen
- Rechtesysteme sinnvoll nutzen

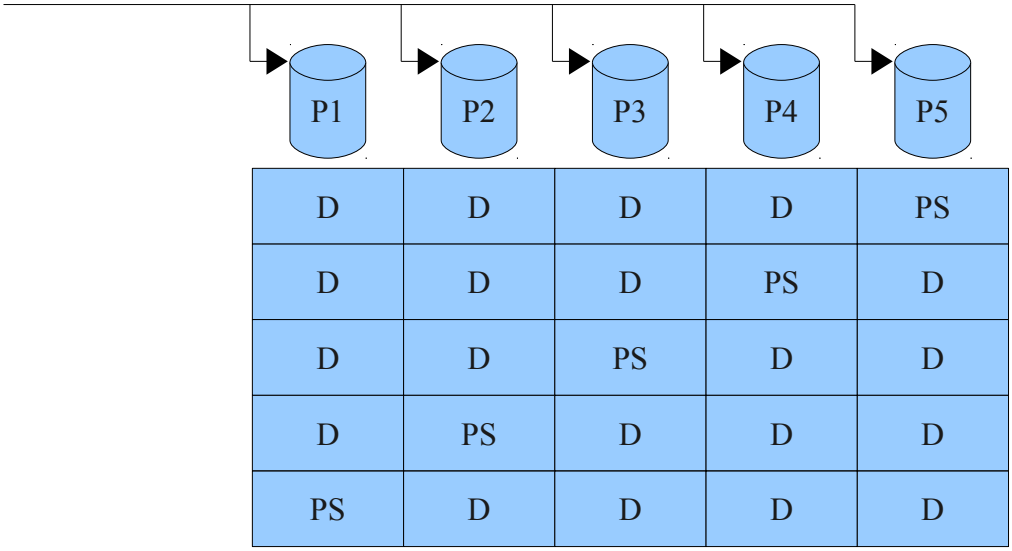
Würmer:
- sind selbstständig lauffähige Programme, die auf eine Schadenswirkung abzielen
- Würmer reproduzieren sich durch massenweises kopieren
- mögliche Schadenswirkung wie Viren
- Würmer haben keine markante Signatur
- bekannte Würmer können von Virenscannern am Namen erkannt werden

Trojaner
- selbstständig lauffähiges Programm
- reproduzieren sich nicht
- führt im Hintergrund eine Schadfunktion aus
- i.d.R. Datensammlung, Passwörter, öffnet Ports usw. → Spionage

1.4 Fehlerüberbrückung
Sinn ist, auftretende Fehler in ihren Auswirkungen zu begrenzen, indem
die Verfügbarkeit der Daten nicht eingeschränkt wird
→ RAID – Systeme (interne Datensicherung)
die Verfügbarkeit der Daten schnellstmöglich wiederhergestellt werden kann
→ Backup (externe Datensicherung)
trotz eingeschränkter Verfügbarkeit der Daten die Integritat erhalten bleibt
→ Unterbrechungsfreie Stromversorgung

interne Datensicherung mit RAID – Systemen
RAID: Redundant Array of inexpensiv Disks (redundantes Feld aus billigen Platten)
mehrere Platten werden an einem eigenen Controller (RAID-Controller) betrieben
verschiedene Level:
RAID 0
→ Striping-Set
→ keine Sicherheitsmaßnahmen, Ziel ist schnelleres Schreiben / Lesen
→ keine Sicherheit gegen Datenverlust
RAID 1
→ Mirroring
→ Plattenspiegelung
→ 2 identische Platten notwendig
→ Information wird immer auf 2 Platten gleichzeitig geschrieben
→ bei Plattenausfall Warnung, Weiterarbeiten mit Spiegelplatte möglich
→ Platte darf ggf. hot-plugged gewechselt werden
→ trotz Fehler Verfügbarkeit nicht eingeschränkt
→ unökonomisch, da alles doppelt gespeichert wird
RAID 5
→ Plattenarray mit separater Platte für Prüfsummen
→ mehrere identische Platten notwendig
→ Daten und Prüfsummen werden über alle Platten verteilt
→ bei Ausfall einer Platte kann fehlende Information errechnet werden
→ bei Plattenausfall Warnung, Weiterarbeit möglich

→ Platte darf ggf. hot-plugged getauscht werden
→ trotz Fehler Verfügbarkeit nicht eingeschränkt



Sicherungsstrategie

Wie oft sollte eine Sicherung durchgeführt werden?

→ es gibt keine allgemeingültige Regel für die Häufigkeit von Datensicherungen
→ Entscheidungskriterium sind die Kosten für die Wiederherstellung verlorener Daten
(Arbeitskraft, verlorene Zeit, entgangener Umsatz)
→ dabei ist immmer vom schlimmst-möglichen Fall auszugehen
→ wichtige Dateien und Verzeichnisse, die öfter geändert werden, ggf. mehrmals täglich sichern, Arbeitsstationen nur einmal
→ Virenbefall kann sich erst verspätet auswirken, deshalb mehrere Sicherungen aufbewahren
(tägliche Sicherung, Wochensicherung, Monatssicherung)

Das Archivbit

Wird eine Datei erstellt oder geändert, wird vom Betriebssystem ein Archivbit gesetzt.
Bei einer Vollsicherung oder einer Zuwachssicherung durch ein Backupprogramm wird das Archivbit zurückgestezt. Bei einer Differentialsicherung oder einer Kopiersicherung bleibt das Archivbit unverändert.

Vollsicherung

Es werden alle Daten eines Datenträgers gesichert.
Vorteile:
→ es existiert immer eine aktuelle Sicherung des gesamten Datenträgers
→ Dateien und Verzeichnisse sind leicht zu finden
Nachteile:
→ Vollsicherungen sind zeitaufwendig
→ unveränderte Dateien sind redundant gesichert

Differentialsicherung

Es werden ale Dateien gesichert, die seit der letzten Vollsicherung erstellt oder geändert wurden.
Vorteile:
→ geringer Zeitaufwand bei Sicherung und Wiederherstellung
→ für eine Wiederherstellung nach Totalsausfall werden nur 2 Medien benötigt
letzte Vollsicherung
letzte Differentialsicherung
Nachteile:
→ nach der letzten Vollsicherung erstellte, dann aber unveränderte Dateien werden redundant gesichert

Zuwachssicherung
Es werden alle Dateien gesichert, die seit der letzten Vollsicherung oder der letzten Zuwachssicherung erstellt oder geändert wurden.
Vorteile:
→ geringster Zeitaufwand bei Sicherung, da nur die neuesten Dateien gesichert wurden
→ beste Medienauslastung, da keine Redundanz
Nachteile:
→ Sicherungen sind auf mehrere Medien verteilt: letzte Vollsicherung und alle folgenden Zuwachssicherungen
→ hoher Zeitaufwand für Wiederherstellung, da letzte Vollsicherung und alle folgendenn Zuwachssicherungen nacheinander wieder hergestellt werden müssen

Unterbrechungsfreie Stromversorgung (USV)
unvorhergesehener plötzlicher Stromausfall
→ schränkt die Verfügbarkeit der Daten ein
→ kann zu Datenverlust führen
→ Schreib-Cache noch nicht geleert
→ Datei nicht geschlossen, d.h. Dateisystem nicht aktualisiert
→ Datei bei Absturz beschädigt und unlesbar

Datenverlust kann verhindert werden durch
→ geordnetes Beenden der Programme
→ geordnetes Herunterfahren des Betriebssystems

→ USV überwacht Netzspannung
→ stellt Spannung aus Akkumulatoren bereit, wenn Netzspannung ausfällt
→ signalisiert Spannungsabfall über eine Schnittstelle an Rechner

→ 2 Arten:
Offline USV:
Zuschaltung bei Bedarf
Umschaltverzögerung von einigen ms
kann u.U. Daten schädigen
preiswertere Variante
Online USV:
Stromversorgung wird anständig von Akku gepuffert
keine Umschatzverzögerung
meist höhere Akkukapazität für kurzen Betrieb
teuere Variante

1.5 Benutzerkontrolle / Berechtigungen
verschiedene Verfahren
- Identifikation
  System verfügt über Datenbank
  Benutzerdaten sind gespeichert und werden mit Eingaben verglichen
- Verifikation
  System hat keine Datenbank
  vergleicht nur ob die auf mitgebrachten Datenträger gespeicherten Informationen mit Eingaben übereinstimmen

identifizierende und verifizierende Verfahren arbeiten mit:
→ Wissen (Passwort, PIN, Benutzername)
→ Besitz (Schlüssel, Chipkarte, RFID-Chip, Fingerabdruck, Iris, Gesicht)
→ Wissen und Besitz

1.6 Zugriffskontrolle

benutzerspezifische Zugriffskontrolle setzt voraus:
- Multiuser-Betriebssystem
  → Unix und alle Abkömmlinge
  → Windows NT, 2000, XP
- Dateisystem, das Berechtigungen speichert
  → Linux ext3
  → Windows NTFS

benutzerkontrolle durch Login-Programm über Benutzerdatenbank:
- Benutzername und Passwort verschlüsselt
- Benutzer können Benutzergruppen zugeordnet werden

prinzipieller Aufbau eines Dateisystems:
- 2 unabhängige Ordnungsmittel
  → Dateizugriffstabelle
    - pro Cluster des Datenträgers Eintrag frei / belegt durch Datei
    - dient dem schnellen Auffinden von freiem Speicher
  → Inhaltsverzeichnis
    - pro Verzeichnis / Datei Eintrag und Namen, belegte Cluster Zugriffsrechte, Datum / Uhrzeit letzter Zugriff, Statusbits
    - dient dem schnellen Auffinden von Dateien / Verzeichnissen
    - Verwaltung von Zugriffsrechten
  → Ordnungsmittel müssen auch nach jedem Schreibvorgang aktualisiert werden
  → Zuordnungsfehler können entstehen, wenn z.B. wegen Absturz
    - keine Aktualisierung stattfindet
    - nur teilweise aktualisiert wird
  → Überprüfung des Dateisystems beseitigt Zuordnungsfehler

Zugriffsrechte des Unix-Dateisystems
- unterschieden werden 3 Nutzerarten
  → Eigentümer eines Verzeichnisses / einer Datei
  → Mitglieder der gleichen Arbeitsgruppe
  → alle anderen
- unterschieden werden 3 Benutzerrechte
  → Lesen eines Verzeichnisses / einer Datei
  → Schreiben / Überschreiben / Löschen eines Verzeichnisses / einer Datei
  → Ausführen von Dateien
- daraus können 3 x 3 = 9 Rechte für jedes Verzeichnis / jede Datei abgeleitet werden
- jeder Benutzer kann für sein Eigentum die Rechte setzen

1.7 Übertragungssicherheit

Ziel ist Schutz vor

- Manipulation
- unberechtigem Zugriff

auf dem Übertragungsweg → Verschlüsselung

1.7.1 Ver- und Entschlüsselung

- lesbare Daten nennt man Klartext
- Umwandlung in Daten, die ohne besondere Maßnahmen unlesbar sind, nennt man chiffrieren oder verschlüsseln
- Verschlüsseln von Klartext ergibt ein unleserliches Zeichengewirr
- bei Verschlüsselung bleiben die Informationen

1.7.2 Verschlüsselung mt Computer

- einfachste Verschlüsselung auf basis logischer Verknüpfungen = XOR
    - XOR = exclusiv-OR:
        - Ausgang = 1, wenn Eingänge entgegengesetzt
- Verschlüsseln
    - Klartext-Zeichen werden mit einem Schlüssel-Zeichen XOR verknüpft
    - Ergebnis ist Verschlüsselungstext
    - Schlüssel kann frei gewählt werden
- Entschlüsseln
    - gleichen Schlüssel verwenden
    - Verschlüsselungstext-Zeichen werden mit Schlüssel XOR verknüpft
    - Ergebnis ist Klartext

1.7.3 Schlüssel

- Schlüssel sind im Prinzip sehr lange Zeichenketten
- die Schlüsselgröße wird in Bit abgegeben
- je länger der Schlüssel, desto sicherer ist der verschlüsselte Text
- Bitfolge als Dualzahl → auch beliebige reversible mathematische Verfahren möglich

1.7.4 Verschlüsselungsverfahren

- symmetrische Verschlüsselung
    - konventionelle Verschlüsselung
    - Verschlüsselung mit Geheimschlüsseln oder symmetrischen Schlüsseln
    - gleicher Schlüsselt für die Ver- als auch Entschlüsselung
    - Beispiel:
      Data Encryption Standard (DES) ist ein für ein konventionelles Verschlüsselungssystem, das häufig auf Regierungsebene eingesetzt wird
    - Vorteil:
        - die konventionelle Verschlüsselung ist sehr schnell
        - besonders sinnvoll um Daten zu verschlüsseln, die nicht übertragen werden
    - Nachteil:
        - Absender und Empfänger müssen sich auf einen Schlüssel einigen
        - Schlüssel muss streng geheim gehalten werden
        - wird Schlüssel bei der Übertragung angefangen, können die verschlüsselten Datenspäter ausgelesen, geändert oder verfälscht werden
        - für jede verschlüsselte Kommunikation eigener Schlüssel notwendig
    - Lösung:
        - Schlüssel kann auch ausgehandelt werden
        - entsprechende Verfahren auf Basis von Primzahlen und Modulodivision

- Verfahren sind nicht reversible
- ausgetauschte Daten können mitgelesen werden, Schlüssel trotzdem sicher

- X möchte an Y verschlüsselt Daten senden und teilt dies Y öffentlich mit
- X und Y generieren beide per Zufallsgenerator eine beliebige ganze Zahl (a, b)
- X generiert und übermittelt an Y:
  - Basiszahl B
  - Primzahl P
- X und Y berechnen aus diesen 3 Werten je eine neue Zahl wie folgt:
  $ZX = B^a \bmod P$ $ZY = B^b \bmod P$
- X und Y berechnen daraus den gemeinsamen geheimen Sitzungschlüssel
  $S = ZY^a \bmod P$ $S = ZX^b \bmod P$
- X verschlüsselt seine Daten mit dem Schlüssel S überträgt sie
- Y entschlüsselt die Daten mit Schlüssel S und erhält Klartext

- **asymmetrische Verschlüsselung**
  - Konzept 1975 von Whitfield Diffie und Martin Hellman eingeführt
  - Kryptografie mit öffentlichen Schlüssen ist asymmetrisches Schema
  - zur Ver- und Entschlüsselung wird ein Schlüsselpaar verwendet
  - mit einem Schlüssel werden Daten verschlüsselt
  - mit dem zugeordneten 2. Schlüssel werden Daten entschlüsselt
  - der 1. Schlüssel ist öffentlich
  - der 2. Schlüssel ist privat
  - jeder kann mit dem öffentlichen Schlüssel Daten verschlüsseln
  - nur der Besitzer des entsprechenden privaten Schlüssel kann die Daten entschlüsseln
  - privater Schlüssel kann nicht aus dem öffentlichen Schlüssel angeleitet werden
  - Vorteil:
    - kein Übertragen von geheimen Schlüsseln zwischen Absender und Empfänger
    - für jede Kommunikation sind nur noch öffentliche Schlüssel erforderlich
    - private Schlüssel werden nicht übertragen
    - Verwendung für digitale Unterschriften möglich
  - Nachteil:
    - sehr rechenintensiv