



CHARITÉ CAMPUS BENJAMIN FRANKLIN

Institut für
**Medizinische Informatik,
Biometrie und Epidemiologie**

Univ.-Prof. Dr. rer. nat. Thomas Tolxdorff

Datensicherheit und Datenschutz

Prof. Dr. Thomas Tolxdorff

Vorlesung an der Charité - Universitätsmedizin Berlin

- Begriffsbestimmung
- Bedrohung durch Programme / Netzwerk
- Erkennung / Abwehr der Bedrohung
- Gesetzliche Grundlagen zum Datenschutz
- Kryptographie

Wenn Sie diese Vorlesung absolviert haben, dann können Sie:

- eine Begriffsabgrenzung zwischen Datenschutz und Datensicherheit vornehmen,
- schädigende Programme identifizieren und abwehren,
- die relevanten Gesetze zum Datenschutz im Gesundheitswesen benennen,
- kryptographische Verfahren zum Schutz sensibler Daten definieren.

■ **Datensicherheit**

- ist die Menge der Maßnahmen um die Funktionsfähigkeit von DV-Systemen zu gewährleisten
- insbesondere zum Schutz vor
 - Verfälschung und Verlust von Daten
 - unberechtigten Zugriff auf Daten

■ **Datenschutz**

- Aufgabe des Datenschutzes der Schutz personenbezogener Daten vor Missbrauch
 - bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung)

- **Vertraulichkeit**
 - Schutz der gespeicherten und übermittelten Daten gegen unbefugte Einsichtnahme
- **Zurechenbarkeit**
 - Der Urheber bzw. Verantwortliche von erhobenen, gespeicherten oder übermittelten Daten muss jederzeit eindeutig feststellbar sein

- **Integrität**
 - Schutz der Daten gegen unerwünschte Änderungen des Inhalts
- **Verfügbarkeit**
 - Schutz vor Verzögerung des Zugriffs auf Daten
 - Verfügbarkeit von Betriebsmitteln für berechtigte Benutzer zur ordnungsgemäßen Durchführung von Operationen

- **Zugriff durch unbefugte Personen**
 - Mitarbeiter innerhalb des Betriebes (z. B. durch Passwortdiebstahl)
 - Daten, die von Mitarbeitern mitgenommen und auf den heimischen Rechner kopiert werden

- Computerviren
 - Zerstörung von Daten
 - Spionage relevanter Daten
- Entwenden der Hardware, z. B. durch
 - Diebstahl
 - Weiterverkauf einer Festplatte, die nicht sicher gelöscht wurde

- Malicious Software (**malware**) bezeichnet Programme mit den verdeckten Eigenschaften:
 - Löschen, Überschreiben oder sonstige Veränderungen von Daten
 - Negative Wirkung auf Vertraulichkeit und Verfügbarkeit von Daten oder Programmen

- Verschiedene Gruppen von *malware*:
 - **Viren**
 - Boot-Virus
 - File-Virus
 - Makro-Virus
 - **Würmer**
 - **Trojaner**

- **Viren:**

- **Boot-Virus:**

- Befindet sich im Sektor eines Datenspeichers (z.B. Diskette, Festplatte), der beim Startvorgang (*booten*) eines Computers angesprochen wird -> automatischer und unbemerkter Start des Virus beim Einlegen des Datenspeichers

- **Viren:**

- **File-Virus:**

- Virus ist Teil eines „Wirtsprogramms“ und wird beim Starten des Programms aktiviert

- **Makro-Virus:**

- Befinden sich in Daten-Dateien, (z.B. MS-Word- oder MS-Excel-Dokumenten) und nutzen die Steuersequenzen des öffnenden Programms (z.B. MS-Office) um Schaden zu erzielen

- **Würmer:**
 - Eigenständige Programme (kein Wirtsprogramm, kein Bootsektor), die sich durch Selbstreproduktion meist über das Netzwerk verbreiten
 - Verbrauchen Ressourcen, selbst wenn keine spezielle Schadensfunktion enthalten ist

- **Trojaner (Trojanisches Pferd):**
 - Verbirgt sich in scheinbar nutzvollen Programmen (Anwendungen, Spiele)
 - Schadensfunktionen:
 - Löschen, Verändern von Daten (→ Viren)
 - Einrichten einer „Hintertür“ für externen Angreifer

- Regelmäßig Datensicherung durchführen
- Sicherheitskopien von Datenträgern sicher aufbewahren
- Schreibschutz bei allen Disketten aktivieren, auf die nicht geschrieben werden muss
- Aktuelle Viren-Schutzsoftware verwenden

- Alle ein- und ausgehenden Datenträger auf Viren überprüfen. Ausgehende Datenträger mit Schreibschutz versehen
- Notfalldiskette erstellen
- Boot-Reihenfolge im CMOS-RAM auf "C:, A:" einstellen (kein Booten von Diskette)

- **Drei-Stufen-Strategie:**
 1. **Erkennung:**
Infektion lokalisieren
 2. **Identifikation:**
Virus-Typ identifizieren
 3. **Entfernung:**
 - Virus vom infizierten Programm entfernen
 - Ursprünglichen Zustand herstellen
(ggf. durch virenfreie Datensicherung)

- Gegenstand:
 - Nicht autorisierter Datenverkehr
- Ziel :
 - Schwachstellen des Systems oder Dienste zu erkennen
- Zweck:
 - Schädigung oder Spionage

- An den Netzwerk- oder Systemgrenzen:
 - Firewall
- Innerhalb der eigenen Grenzen:
 - Intrusion-Detection

- Verbindungsglied zwischen innerem und äußeren System/Netzwerk
- Regelt und überwacht den Datenverkehr
- Potentielle Komponenten/Funktionen:
 - Packet Filter
 - Application Gateways

■ **Packet Filter:**

Regelt Transit der Daten auf Basis von:

- IP Header (Quell- und Zieladresse)
- Art des Übertragungsprotokolls
(TCP, UDP, ICMP)
- TCP/UDP Header, (Quell- und Zielport)
- Regeln entscheiden über „allow“ oder „block“
- Implementierungsbeispiel: „*iptables*“ (Linux)

- **Application Gateway:**
 - Vermittelt zwischen Client und Anwendung
 - Analyse der Kommunikation
 - Differenzierte, anwendungsbezogene Regeln
 - Protokollierung der Anwendungskommunikation

- **Beispiel für Implementierung:**

- Bereich ...
z.B. Fire
- Bereich ...
Persona



- **Annahme:**
Verhalten eines Eindringlings (Intruders) ist vom autorisierten Benutzer unterscheidbar
- Techniken:
 - Statistical Anomaly Detection
 - Rule-based Anomaly Detection

- **Statistical Anomaly Detection (SAD):**
 1. Sammlung von Netzwerkdaten autorisierter Benutzer in einer bestimmten Zeitspanne
 2. Entscheidung über das beobachtete Verhalten mittels statistischer Tests, basierend auf den gesammelten Daten

- **Angewandte Testansätze:**
 - mittlere absolute Abweichung eines Parameters
 - Korrelationen zwischen zwei oder mehreren Variablen (z.B. Prozessorzeit vs. Ressourcenauslastung)
 - Markov – Modell für Übergangswahrscheinlichkeiten zwischen Zuständen (z.B. Kommando-Reihenfolge)
 - Zeitreihenmodell zur Analyse von Ereignissequenzen

- **Rule-based Anomaly Detection:**

1. Erstellung von Regeln, die ein Benutzungsmuster beschreiben
2. Abgleich des aktuellen Benutzer-Verhaltens mit den Regeln

Regeln können entweder autorisiertes oder verdächtiges Verhalten beschreiben

- **Regelerstellung:**
 - Regeln sind individuell aufzustellen (systemabhängig)
 - Regeldefinition durch Experten, basieren auf:
 - Interviews mit Systemadministratoren und IT-Analytikern
 - Interviews mit Straftätern (**Crackern**)

Intrusion Detection

The screenshot shows the 'Policy Editor - Official' window. The title bar includes 'File View Options Help'. The main window title is 'bad-traffic'. On the left, there is a 'Folder Items' tree with 'local' and 'exploit' folders. Under 'local', the 'bad-traffic' folder is expanded, showing a list of 14 signatures, each with a checkbox and a document icon. The main area displays the configuration for the selected signature group:

- Name: bad-traffic
- Last Modified Date: [empty]
- # of Rules: 14
- # of Active Rules: 0
- Base Directory: \$RULE_PATH/ [Set All Groups]
- Description: These signatures are representative of traffic that should never be seen on any network. None of these signatures include datagram content checking and are extremely quick signatures

At the bottom, a table lists the signatures with their configurations:

Signature Name	Action	Protocol	Source IP/Port	Direction	Destination IP/Port
<input checked="" type="checkbox"/> BAD-TRAFFIC tcp port 0 traffic	alert	tcp	\$EXTERNAL_NET/any	<>	\$HOME_NET/0
<input checked="" type="checkbox"/> BAD-TRAFFIC udp port 0 traffic	alert	udp	\$EXTERNAL_NET/any	<>	\$HOME_NET/0
<input checked="" type="checkbox"/> BAD-TRAFFIC data in TCP SYN pac...	alert	tcp	\$EXTERNAL_NET/any	->	\$HOME_NET/any
<input checked="" type="checkbox"/> BAD-TRAFFIC loopback traffic	alert	ip	any/any	<>	127.0.0.0/8/any
<input checked="" type="checkbox"/> BAD-TRAFFIC same SRC/DST	alert	ip	any/any	->	any/any
<input checked="" type="checkbox"/> BAD-TRAFFIC ip reserved bit set	alert	ip	\$EXTERNAL_NET/any	->	\$HOME_NET/any
<input checked="" type="checkbox"/> BAD-TRAFFIC 0 ttl	alert	ip	\$EXTERNAL_NET/any	->	\$HOME_NET/any
<input type="checkbox"/> BAD-TRAFFIC bad frag bits	alert	ip	\$EXTERNAL_NET/any	->	\$HOME_NET/any
<input checked="" type="checkbox"/> BAD-TRAFFIC Unassigned/Reserve...	alert	ip	\$EXTERNAL_NET/any	->	\$HOME_NET/any

At the bottom of the window, a status bar shows: Total Rules: 2035 | Rules Enabled: 1679 | Rules File: C:\Programme\Activeworx\IDSPolMan\Official\snort.conf

- Ärztliche Schweigepflicht
- Brief- und Fernmeldegeheimnis
- Personalakteneinsicht des Arbeitnehmers / der Arbeitnehmerin (BetrVG)

- Hessisches Datenschutzgesetz 1970
- Bundesdatenschutzgesetz (BDSG) 1977
- Volkszählungsurteil 1983
 - Recht auf informationelle Selbstbestimmung:
 - Befugnis des Einzelnen, grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen
- Geltung der EU-Datenschutzrichtlinie in Deutschland 1995

- EU-Datenschutzrichtlinie
- BDSG
- Landesdatenschutzgesetze
- Bereichsspezifische Regelungen

- Ziel war die Vereinheitlichung des Datenschutzrechts durch Rahmenvorgaben an die Mitgliedsstaaten
 - Erleichterung des Datenverkehrs innerhalb der EU

- Sitz der verantwortlichen Stelle
 - Innerhalb der EU
 - Maßgeblich ist das für den Sitz des Unternehmens geltende Recht
 - Außerhalb der EU
 - Maßgeblich ist der Ort, an dem Erhebung, Verarbeitung und Nutzung personenbezogener Daten erfolgt

- Nur zulässig, wenn dort angemessenes Datenschutzniveau
 - Feststellung durch EU-Kommission
- Ausnahmen
 - Einwilligung bzw. Vertrag mit dem Betroffenen
 - Lebenswichtige Interessen des Betroffenen
 - Wichtiges öffentliches Interesse (Rechtverfolgung)

■ **BDSG**

- Öffentliche Verwaltung des Bundes
- Nicht-öffentlicher Bereich (Privatwirtschaft)

Aufsicht:
Bundesbeauftragter

■ **LDSGe**

- Öffentliche Verwaltung der Länder und der Kommunen

Aufsicht:
Landesdatenschutzbeauftragter

- Bereichsspezifische Regelungen
 - Sozialgesetzbuch (**SGB**)
 - Betriebsverfassungsgesetz (**BetrVG**)
 - Telekommunikationsgesetz (**TKG**)

- Was sind personenbezogene Daten?
 - § 3 (1) BDSG: Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person

- Zulässigkeit der Datenverarbeitung
 - § 4 (1) BDSG: Die Verarbeitung und Nutzung personenbezogener Daten ist prinzipiell verboten
 - Ausnahmen:
 - BDSG
 - Andere Rechtsvorschriften
 - Einwilligung des Betroffenen
 - → Verbot mit Erlaubnisvorbehalt

- Erlaubnisvorschriften
 - § 28 BDSG: DV für eigene Geschäftszwecke
 - Z. B. Abwicklung von Kauf-, Kredit-, Bank-, Versicherungs-, Dienst- oder Arbeitsverträgen
 - § 29 BDSG: DV zum Zweck der Übermittlung
 - Z. B. Schufa
 - § 30 BDSG: DV zum Zweck der anonymisierten Übermittlung

- Ärztliche Schweigepflicht
 - Nach § 203 StGB macht sich strafbar, „wer unbefugt ein fremdes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als Arzt (...) anvertraut oder sonst bekannt worden ist

- Grundsätze
 - Personenbezogene Daten sind nach „Treu und Glauben“ zu behandeln.
 - D.h. die Daten dürfen nur für einen eindeutigen und rechtmäßigen Zweck verwendet werden

- Grundsätze
 - Die Person deren Daten erhoben werden,
 - muss ihre Einwilligung zur Speicherung und Verarbeitung der Daten geben.
 - D.h. wenn eine Einwilligung zur elektronischen Datenverarbeitung nicht vorliegt, müssen die Daten weiterhin schriftlich erhoben werden!
 - besitzt grundsätzlich ein Auskunftsrecht (Einsicht in die Daten).
 - Ausnahme: Psychiatrische Erkrankungen

- Grundsätze
 - Die Person deren Daten erhoben werden,
 - besitzt ein Widerspruchsrecht.
 - D.h. eine Einwilligung kann zurück gezogen werden

- Datenübertragung
 - Die Art der zu übertragenden Daten ist auf ein Minimum zu beschränken
 - Die Datenübertragung sollte verschlüsselt erfolgen. Dieses Vorgehen ist immer notwendig, sofern die Daten das eigene LAN verlassen (z.B. per Internet)
 - Es dürfen diejenigen Daten übertragen werden, die zur sachgerechten Behandlung des Patienten notwendig sind

- Gesundheitskarte
 - soll zum 1. Januar 2006 eingeführt werden
 - **Vorgesehene Anwendungen**
 - **Pflichtanwendungen:**
 - Verwaltungsdaten
 - Elektronisches Rezept
 - **Freiwillige Anwendungen:**
 - Arzneimitteldokumentation
 - elektronischer Arztbrief
 - elektronische Patientenakte
 - Notfalldaten

- Gesundheitskarte
 - Verwaltungsdaten
 - beinhalten den gleichen Datensatz wie auf der jetzigen Krankenversichertenkarte.
 - Datenschutzrechtliche Probleme bestehen hier nicht

- Gesundheitskarte
 - Elektronisches Rezept
 - soll das bisherige Papierrezept ablösen. Aus datenschutzrechtlicher Sicht muss dabei sichergestellt sein, dass:
 - nur berechnigte Personen ein Rezept ausstellen können,
 - die Rezeptdaten nicht verändert werden können und
 - nur berechnigte Personen diese Daten lesen können

- Gesundheitskarte
 - Dies soll mit dem Einsatz von **Heilberufsausweisen**, die sowohl die Berechtigung der Person nachweisen können, als auch eine Signaturfunktion und eine Verschlüsselungsfunktion beinhalten, sichergestellt werden
 - Freiwillige Anwendungen:
 - Es gilt:
 - **Der Patient muss Herr seiner Daten sein!**

- Gesundheitskarte
 - Dies soll zum einen durch eine informierte **Einwilligung** des Patienten in die jeweilige Anwendung und zum anderen durch **Lese- und Lösungsrechte** bezüglich jedes einzelnen Datums der jeweiligen Anwendung erfolgen.
 - Weiterhin soll der Patient durch die Vergabe von **Leserechten gegenüber den Heilberufen** auch deren Zugriff im Einzelnen steuern können

- Gesundheitskarte
 - Arzneimitteldokumentation
 - soll die Sicherheit des Patienten vor Medikamentenunverträglichkeiten, unerwünschten Nebenwirkungen und negativen Folgen von Medikamentenmix erhöhen.
 - Dabei muss sichergestellt sein, dass die Dokumentation nicht manipuliert werden kann

- Gesundheitskarte
 - **elektronischer Arztbrief**
 - soll den bisherigen papiergebundenen ersetzen und eine schnellere Information und bessere Möglichkeiten zur Weiterverarbeitung gestatten.
 - Aus datenschutzrechtlicher Sicht muss dabei sichergestellt sein, dass nur berechtigte Personen einen Arztbrief ausstellen und lesen können und dessen Inhalt nicht manipuliert werden kann. Dies soll mit dem Einsatz von Heilberufsausweisen sichergestellt werden

- Gesundheitskarte
 - **elektronische Patientenakte**
 - soll eine bessere Versorgung des Patienten ermöglichen und unnötige Doppeluntersuchungen verhindern. Behandelnde Ärzte können somit auf elektronischem Wege auf Untersuchungsergebnisse und andere relevante ärztliche Dokumente schnell, sicher und unbürokratisch zugreifen.

- Gesundheitskarte
 - **elektronische Patientenakte**
 - Aus datenschutzrechtlicher Sicht muss dabei sichergestellt sein, dass nur berechnigte Personen Zugriff erhalten und dass die Inhalte nicht verändert werden können. Dies soll mit dem Einsatz von Heilberufsausweisen sichergestellt werden

- Gesundheitskarte
 - **Notfalldaten**
 - sollen als zusätzliches Sicherheitsmerkmal auf die Karte aufgebracht werden, um im Notfall die notwendigen Information schnell verwerten zu können.
 - Datenschutzrechtliche Probleme sind hier nicht zu erwarten

- Definition:
Ver- und Entschlüsselung von Daten mit Hilfe mathematischer Verfahren
- Ziel:
 - Schutz vor unbefugter Einsichtnahme oder Manipulation von Daten
- Klassifizierung:
 - Symmetrisches Verfahren
 - Asymmetrisches Verfahren

- Merkmale:
 - Sender und Empfänger verwenden **einen gemeinsamen Schlüssel**
 - **Verschlüsselung / Entschlüsselung** stets mittels ***gemeinsamen* Schlüssel**

- Merkmale:
 - Sender und Empfänger verwenden jeweils **zwei** Schlüssel:
 - Öffentlicher Schlüssel (*public-key*)
 - Privater Schlüssel (*secret-key*)
 - **Verschlüsselung** stets mittels *public-key*
 - **Entschlüsselung** stets mittels *secret-key*

- Implementiert asymmetrisches Verschlüsselungsverfahren
- Kostenlose Verfügbarkeit:
 - GNU Privacy Projekt (gnupp: <http://www.gnupp.org>) beinhaltet:
 - GNU Privacy Guard (gnupg: <http://www.gnupg.org>)
 - GNU Privacy Assistant (gnupa)
 - Basiert auf OpenPGP (<http://www.openpgp.org>)

- Definition:
 - Gesamtheit der für die Verwendung von Public-Key-Verfahren erforderlichen Komponenten und Dienste
 - U. a. Schlüsselerzeugung, Zertifizierungs-, Verzeichnis-, Sperrdienste

- Definition:
 - Elektronische Unterschrift
 - Verfahren bei welchem durch die Verwendung asymmetrischer Verfahren die Integrität und Authentizität einer elektronischen Nachricht sichergestellt werden kann
- Anwendungsbereiche:
 - Warenbestellungen
 - Arztbrief

- Signaturgesetz (SigG)
 - Elektronische Signatur
 - Fortgeschrittene und qualifizierte Signatur
- Elektronische Signatur
 - Anfügen des Namens oder einer eingescannten Unterschrift
 - Keine Sicherheit, da diese Unterschrift kopiert werden kann

- Fortgeschrittene und qualifizierte Signatur
 - Kann die Identität des Unterzeichners bestätigen (z. B. bei der Nutzung von PGP)
 - Prüfung, ob Daten nachträglich verändert wurden
 - Beim Signieren wird ein Hashwert (Prüfsumme) für die elektronischen Dokumente berechnet
 - Veränderungen am Dokument können durch das Abweichen des Hashwertes festgestellt werden

- Fortgeschrittene und qualifizierte Signatur
 - Zur Sicherheit des Signaturverfahrens ist der Signaturprüf Schlüssel durch eine vertrauenswürdige Stelle (Zertifizierungsanbieter) mit einem elektronischen Zertifikat einer Person zuzuordnen
 - Der Signaturprüf Schlüssel (z. B. Chipkarte) ist geheim zu halten und vor unbefugter Nutzung zu schützen

- Notwendigkeit der Datensicherheit
 - Erkennung und Abwehr von Bedrohungen
- Wesentliche Gesetze und Regelungen zum Datenschutz
 - z. B. BDSG, EU-Richtlinie, ärztliche Schweigepflicht
- Gesundheitskarte / Elektronisches Rezept
- Kryptographische Verfahren zum Schutz sensibler, medizinischer Daten