Grundlagen des Datenschutzes und der IT-Sicherheit (14)

Vorlesung im Sommersemester 2007
an der Universität Ulm
von Bernhard C. Witt

Grob-Gliederung zur Vorlesung

Topics zum Datenschutz:
- Geschichte des Datenschutzes
- Datenschutzrechtliche Prinzipien
- Vertiefung in ausgewählten Bereichen
- Verwandte Gebiete zum Datenschutz

Topics zur IT-Sicherheit:
- Einflussfaktoren zur IT-Sicherheit
- Mehrseitige IT-Sicherheit
- Risiko-Management

→ **Konzeption von IT-Sicherheit**

Übersicht zur Konzeption von IT-Sicherheit

- Erstellung sicherer IT-Systeme
- Gestaltung der IT-Infrastruktur
- Datenschutzfreundliche Techniken

Konzeption von IT-Sicherheit (2)

Sicherheit im laufenden Betrieb von IT-Systemen:

- Sensibilisierung und Schulung der Mitarbeiter
- Authentisierung bei Zugang und Zugriff anhand Wissen/Besitz/Merkmal
- Schutz vor Viren, Würmer, Trojanische Pferde etc.
- Protokollierung (→ Überwachung der Technik & Datenströme; z.B. Netzwerkmonitoring, Intrusion Detection Systems)
- Änderung von Produktivsystemen erst nach Erfolg bei Testsystemen
- Dokumentation von Änderungen an Systemeinstellungen
- regelmäßige Kontrollen (z.B. durch Penetrationstests)
- Einrichtung eines Vulnerability Managements

→ **Hilfsmittel**: Sicherheitsleitlinie (security policy)

Sicherheitsarchitektur des ISO/OSI-Referenzmodells

- Sicherheitsdienste (nach ISO 7498-2):
  - ° Authentifizierung
  - ° Zugriffskontrolle
  - ° Gewährleistung der Vertraulichkeit
  - ° Gewährleistung der Integrität
  - ° Nachweis der Verursachung
- richtet sich nicht gegen Ausnutzung der Protokollfunktionalitäten (requests for comments)

Management der Netzwerksicherheit (1)

- Grundlage: ISO/IEC 18028-1
- Sicherheitsniveau abhängig von Schutzwürdigkeit & Stellung der Zugriffsberechtigten
- berücksichtigt die Verfügbarkeit, Integrität, Vertraulichkeit und Ausfallsicherheit der (Übertragungs-) Daten sowie die Authentizität, Zurechenbarkeit und Nichtabstreitbarkeit der Kommunikationspartner

Management der Netzwerksicherheit (2)

Maßnahmen:

- Erstellung eines aktuellen Netzwerkplans
- Einrichtung technischer Schutzzonen mittels Firewalls
- Erkennen & Blockieren verdächtigen Netzwerktraffics
- Einsatz eines aktuellen Antivirenschutzes
- dem Schutzgrad angemessen hohe Passwortgüte
- Härtung der Rechner durch Abschaltung unnötiger Dienste
- Gewährleistung technischer Redundanz
- Einsatz von Verschlüsselungstechniken bei der Datenübertragung
- Benutzung der Network Address Translation

Perimeterschutz mittels Firewalls

- Firewall = System aus Hard- und Software zur Separation eines Netzes von anderen Netzen
- nur autorisierter Datenverkehr soll Firewall (bei eingestellten Ports & IP-Adressen sowie einer definierten Durchlassrichtung) passieren dürfen (Achtung: Firewall kann umgangen werden!)
- Einsatz mehrerer Netzwerkkarten geboten
- Unterschied physischer Verbindungen & logischen Datenflusses
- Es gibt verschiedene Architekturen:
  - Paketfilter (Filterung von IP-Paketen); z.B. Screening Router
  - Application Level Gateways (auf Proxy-Server = Bastian Host); z.B. Dual Homed Host
  - Mischformen (Screened Host/Subnet)
- Demilitarisierte Zone (DMZ) als Pufferzone

Sicherheitsstrategien zur Gestaltung von Firewalls

nach Zwicky, Cooper & Chapman (2000):

- least privilege → Anwendung need-to-know-Prinzip
- defense in depth → Aufbau einer gestaffelten Abwehr
- choke point → Etablierung eines engen Kanals
- weakest link → Absicherung des schwächsten Glieds
- fail-safe stance → Anwendung des Erlaubnisprinzips
- universal participation → Beteiligung von Insidern
- diversity of defense → Verwendung von Komponenten unterschiedlicher Händler & Aufteilung der Administration
- simplicity → Anwendung des Prinzips der Einfachheit
- security through obscurity → Ausnutzung von Überraschungseffekten durch Reduzierung aktiver Mitteilungen

Maßnahmen physischer Sicherheit

ergriffene Maßnahmen	1998	2000	2002	2004	2006
Unterbrechungsfr. Stromvers.	76%	79%	97%	91%	90%
Klimatisierung	74%	74%	94%	83%	85%
Brandmeldesysteme	71%	71%	83%	83%	81%
Datensicherungsschränke	75%	78%	80%	85%	80%
Sicherheitstüren	62%	65%	76%	76%	68%
Einbruchmeldesysteme	52%	51%	70%	72%	67%
Löschanlagen	47%	48%	50%	57%	54%
Glasflächendurchbruchschutz	48%	43%	56%	55%	52%
Bewachung	40%	44%	46%	49%	47%
Video-Überwachung	23%	25%	28%	39%	38%
Schutz gg. komprom. Abstrahl.	11%	10%	13%	13%	13%

Quelle: <kes>-Sicherheitsstudien

Sicherung der Authentisierung

- Sicherung der Benutzeridentifikation anhand
  - Wissen → z.B. Password
  - Besitz → z.B. Chipkarte (= Prozessorkarte)
  - Merkmal → z.B. Unterschrift/Biometrie
- nur Feststellung, ob Benutzer berechtigt ist, nicht ob dessen Identität korrekt ist!

→ Zugangs-/Zugriffskontrolle mittels Rechteprüfung

Zum Password

- BIOS-/Boot-Password kann durch Jumper-Umsetzung, Ausbau der Festplatte oder mittels Software-Unterstützung umgangen werden
- Bildschirmschoner-Password kann durch Neustart (über trusted path) oder Original-Software im CD-ROM-Laufwerk umgangen werden
- jedes Password ist mit Brute Force (= Ausprobieren) knackbar: bei 26 Groß- und 26 Kleinbuchstaben, sowie 10 Zahlen (= 62 Zeichen) dauert Brute Force bei 6 Stellen ca. ¼ h (bei 1,4 GHz), erst ab 7. Stelle werden ein paar wenige Tage benötigt
- bei Verwendung sprechender Wörter ist das Password durch Dictionary Attack binnen weniger Sekunden geknackt
- Achtung: Ausspähen von Daten strafbar! (§ 202a StGB)

Zur Chipkarte

- Unterscheidung zwischen kontaktloser Karte (z.B. Uni-Chipkarte) und Kontaktkarte (z.B. Krankenversicherungskarte)
- Kennzeichen aller Chipkarten: Vorhandensein eines Prozessor-Chips (→ Speicher- und Verarbeitungsmedium im Sinne von § 6c BDSG)
- leichte Angreifbarkeit:
  → Durchdringung der Schutzschichten durch Abschleifen / Anätzen
  → Manipulierbarkeit gespeicherter Bits durch Beschuss mit elektromagnetischer Strahlung (z.B. Blitzlicht)
  → Messbarkeit des Energieverbrauchs („power analysis“) oder der benötigten Rechenzeit („timing attacks“)
- Schlüssel oder PIN auf EEPROM (nicht-flüchtiger Speicher), Verschlüsselung üblicherweise symmetrisch

Zur Biometrie

= Erfassung und (Ver-)Messung von Lebewesen und ihren Eigenschaften

- Unterscheidung in:
  - physiologische Merkmalsverfahren (Fingerabdruckverfahren, Iris-/Retinaerkennungsverfahren, Gesichtserkennungsverfahren)
  - verhaltensabhängige Merkmalsverfahren (Sprachmuster- / Schriftdynamikerkennungsverfahren, Tipprhythmusverfahren)
- Speicherung eines Referenzmusters und Abgleich hiermit (Probleme: falsche Akzeptanz → „false acceptance rate“, falsche Ablehung → „false rejection rate“; Genauigkeit unterschiedlich und größtenteils diametral zur gesellschaftlichen Akzeptanz → lediglich Fingerabdruck in beiden Kategorien gut)

Zugriffskontrolle

Matrizen:

- Subjekt (Benutzer & Prozesse) = Zeilen
- Objekt (Dateien & Datenträger) = Spalten
- Zugriffsart (lesen, schreiben, ausführen, löschen) = Zellen

→ Access Control List: wer darf auf gegebenes Objekt zugreifen

→ Capability List: auf welche Objekte darf ein gegebener Benutzer zugreifen

→ Grundsatz: need-to-know (nur benötigte Rechte einräumen)

→ Pflege erfordert z.T. hohen Aufwand (darum: Benutzerrollen!)

→ beachtenswert: spezifischere Regeln vor allgemeineren Regeln!

Beispiele zur Sicherheitsleitlinie (security policy)

Inhalte
(aus <kes> 5/2000, S. 55ff):

- Leitaussagen
- IT-Sicherheitspolitik (allgemein + für IT-Systeme & IT-Anwendungen)
- IT-Sicherheitsmanagement (Aufgabendefinition bis Projekt-Handbuch)
- Regelwerke der IT-Sicherheit (nach Verantwortlichkeiten)
- Anhänge mit Dienstanweisungen und Richtlinien

Anforderungen
(aus DuD 2/2002, S. 104ff):

- Stellenwert der Sicherheit (Priorisierungen)
- Sicherheitsziele/-strategie
- Sicherheitsprozess (Umsetzung im Unternehmen)
- Umfassender Anspruch (auch Produktsicherheit etc.)
- Relevanz (für alle Mitarbeiter)
- Ansprechpartner (Kontakt innerhalb des Unternehmens)
- Umfang (kurz, dafür Verweis auf umfangreichen Anhang)
- Formaler Rahmen (Integration in übliches Lay-Out)

Kennzeichen datenschutz-freundlicher Techniken

= Privacy Enhancing Technologies (PET; 1995)

- Ziel: weniger Risiken für die Privatsphäre der Betroffenen durch Ausgestaltung eingesetzter Informations- und Kommunikations-technik unter Reduktion des Personenbezugs (→ Anonymität)
- setzt bereits im Vorfeld der Verarbeitung personenbezogener Daten an → Datenvermeidung!
- wichtiges Hilfsmittel vorausschauender Technikgestaltung
- unabhängig von etwaigen Rechtsnormen
- Rückwirkung auf rechtliche Entwicklung („Stand der Technik“)

→ datenschutzgerecht & datenschutzfördernd

frühere Bezeichnung: „Systemdatenschutz“ (Podlech)
→ strukturelle, systemanalytische Ergänzung des individuellen Rechtsschutzes der Betroffenen

Prinzipien datenschutz-freundlicher Techniken (1)

Datensparsamkeit & Systemdatenschutz

- je weniger personenbezogene Daten herausgegeben werden (müssen), desto leichter lassen sich entsprechende Techniken anwenden

→ nur erforderliche Daten verarbeiten

→ frühestmögliche Anonymisierung

→ frühestmögliche Löschung

→ Verschlüsselung bei Kommunikation

→ Beispiel: prepaid-Chipkarten, Mix-Netz, Transaktionspseudonym (z.B. mit verdeckter Zufallszahl bei elektronischem Geld)

Prinzipien datenschutz-freundlicher Techniken (2)

Selbstdatenschutz & Transparenz

- Selbstbestimmung und –steuerung des Nutzers

→ Nutzer entscheidet selbst, wie anonym er Dienste in Anspruch nimmt

→ Verarbeitung wird verständlich offengelegt (Verfahrensverzeichnis) und ist nachprüfbar (→ Identitätsmanagement)

→ Formulierung eigener Schutzziele

→ Nutzung vertrauenswürdiger Institutionen (Trust Center)

→ Unterstützung durch Anwendung der Betroffenenrechte

→ Beispiel: Platform for Privacy Preferences (P3P auf www.w3org/P3P/)

Beispiel für datenschutzfreundliche Technik: DC-Netz (1)

Teilnehmer A	
Nachricht:	**1011**
Symm. Schlüssel mit B	1100
Symm. Schlüssel mit C	1001
Übertragung 1	**1110**

Teilnehmer B	
Nachricht:	**0000**
Symm. Schlüssel mit A	1100
Symm. Schlüssel mit C	0101
Übertragung 2	**1001**

Teilnehmer C	
Nachricht:	**0000**
Symm. Schlüssel mit A	1001
Symm. Schlüssel mit B	0101
Übertragung 3	**1100**

Übertragung 1	1110
Übertragung 2	1001
Übertragung 3	1100
Ergebnis:	**1011**

DC-Netz = Dining Cryptographers Network (David Chaum 1988)

- Verfahren zur Anonymität des Senders
- für jedes Nutzbit werden n Schlüsselbits bei n Teilnehmer über unsicheren Kanal gesandt und mittels Vernam-Chiffre (per XOR) summiert
- die Teilnehmer vereinbaren paarweise gemeinsame Schlüssel

Beispiel für datenschutzfreundliche Technik: DC-Netz (2)

Vorteile:

- Verfahren garantiert die Anonymität des Senders
- Vernam-Chiffre macht Verfahren mathematisch beweisbar sicher (nutzt one-time-pad-Eigenschaft)
- aktiver Angreifer kann aufgespürt werden, da der Sender den korrekten Wert der überlagerten Nachricht kennt und überprüfen kann

Nachteile:

- Austausch der paarweisen Schlüssel muss sicher erfolgen
- eignet sich nur für die Kommunikation einer beschränkten Gruppe, bei der alle Teilnehmer kommunizieren müssen
- Verfahren muss synchronisiert ablaufen

Andere datenschutz-freundliche Techniken

- **MIX-Netz**: Kommunikation wird über einen Nachrichtenvermittler (Zwischenknoten) abgewickelt, der genügend viele Datenpakete von genügend vielen Sendern sammelt und leitet diese so verändert weiter, dass außer Sender oder MIX-Station keiner die Pakete zuordnen kann. (Empfänger-Anonymität durch „anonyme Rückadressen“ realisierbar) → asynchrone Kommunikation
- anonymisierende Proxies (z.B. anonymizer.com, rewebber.com)
- Verfahren mit Berücksichtigung von Verkehrsanalysen (z.B. AN.ON/JAP = MIX-Netz unter JAP.inf.tu-dresden.de)
- Cookie-Austausch (z.B. CookieCooker.de) bzw. Cookie-Filter (z.B. webwasher.com)

Literaturhinweise

Im Semesterapparat verfügbar:

- Bernhard C. Witt: IT-Sicherheit kompakt und verständlich; Wiesbaden, Vieweg, 2006
- Claudia Eckert: IT-Sicherheit; München, Oldenbourg, 2006, 4. Auflage [im Semesterapparat noch die 3. Auflage von 2004]

Zum Hintergrund der Vorlesung empfehlenswert:

- Hans-Peter Königs: IT-Risiko-Management mit System; Wiesbaden, Vieweg, 2005
- Bruce Schneier: Secrets & Lies – IT-Sicherheit in einer vernetzten Welt; Heidelberg, dpunkt, 2001
- Günter Müller & Andreas Pfitzmann (Hrsg): Mehrseitige Sicherheit in der Kommunikationstechnik; Bonn, Addison Wesley, 1997
- Zeitschriften: <kes>, hakin9, IEEE security & privacy, IT-SICHERHEIT

Aufgabe: Prüfungsfragen

→ Formulieren Sie je eine Prüfungsfrage zu den

- Grundlagen des Datenschutzes
- Grundlagen der IT-Sicherheit

  soweit diese in Vorlesung oder Übung behandelt wurden!

→ Erstellen Sie zu einer Frage Ihre Musterlösung!

→ Geben Sie zur Musterlösung die Punktevergabe an!

Zeit: 15 Minuten! (pro Teilaufgabe ca. 5 min)

Ziel: Präsentierbare Lösung!