Information Security Society Switzerland
> vormals FGSec

Informationssicherheit für Juristen: vernachlässigter Prozess?

Liliane Mollet
ISSS Vorstand, Ergonomics AG
Master of Law
CAS Information Security

Agenda

- “Gerüchte-Küche”
- Definition Informationssicherheit
- Rechtliche Grundlagen
- Aktuelle Bedrohungen / Trends
- Konkrete Beispiele
- Kritische Würdigung
- Fragen / Diskussion

Information Security Society Switzerland
> vormals FGSec

“Gerüchte-Küche”

„Gerüchte-Küche“

- „IT-Security geht nur Informatiker etwas an“
- „Datenschutz ist eine rein rechtliche Angelegenheit“
- „Verantwortung der PCs liegt bei der IT“
- „Ich habe nichts zu verbergen“

Wirklich?

Foto: http://www.denkmalvonhinten.de/

Geheim, vertraulich oder „privacy“?

Information Security Society Switzerland
> vormals FGSec

Definition Informationssicherheit

Definition Informationssicherheit (1)

- **Was sind Informationen?**
  - Ideen im Kopf, ausformuliert auf Papier oder elektronisch abgespeichert
  - gesprochenes Wort

Definition Informationssicherheit (2)

- **Was soll genau „gesichert“ bzw. geschützt werden?**
  - Vertraulichkeit (confidentiality)
  - Verfügbarkeit (availability)
  - Integrität (integrity)
  - Verbindlichkeit/Nichtabstreitbarkeit (non-repudiation)

  ⇨ **Wichtigste Schutzziele der Informationssicherheit**

NZZ Online

Nachrichten | Finanzen | Magazin | Hintergrund | Blogs | Marktplätze | Shops | Abos &

Startseite · **International** · Wirtschaft · Schweiz · Kultur · Sport · Panorama · Wissensch

Dienstag, 23. Juni 2009, 15:23:22 Uhr

Nachrichten › International

9. April 2009, 11:03, NZZ Online

Oberster britischer Terrorfahnder tritt nach Panne zurück

Geheime Papiere offen lesbar herumgetragen

Sitz der britischen Terrorfahndung: Scotland Yard. (Bild: Reuters)

Der Anti-Terror-Chef von Scotland Yard hat seinen Rücktritt eingereicht. Er war von Presseleuten fotografiert worden, wie er geheime Papiere über eine laufende Anti-Terror-Überwachung gut lesbar unter dem Arm trug. Wegen der Panne mussten Razzien vorgezogen werden.

(sda/dpa) Nach einer Sicherheitspanne ist Grossbritanniens oberster Terrorfahnder, Bob Quick, zurückgetreten. Das teilte der Londoner Bürgermeister Boris Johnson am Donnerstag mit.

Er habe den Rücktritt des Anti-Terror-Chefs von

Vertraulichkeit? Verantwortung? Interessen?

Definition Informationssicherheit (3)

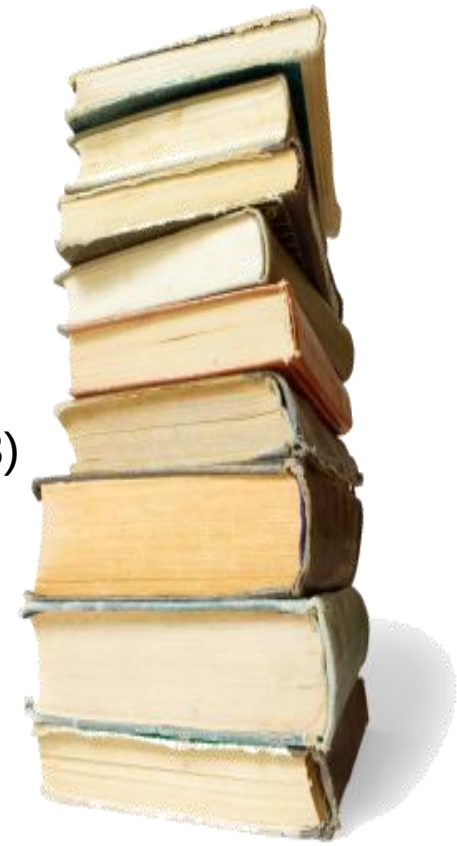
- **Definition nach ISO 27002 (17799:2005)**
  „Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.“

- „Informationssicherheit ist der Schutz von Informationen vor einer Vielzahl von Bedrohungen, die Aufrechterhaltung des Geschäftsbetriebs sicher zu stellen, Geschäftsrisiken zu minimieren und die Rendite und Geschäftschancen zu maximieren.“
  (inoffizielle deutsche Übersetzung)

Rechtliche Grundlagen

Rechtliche Grundlagen (1)

- **Schweizer Gesetze**
  - **Art. 7 DSG:** „Datensicherheit“
  - **Art. 8-11 VDSG:** „technische und organisatorische Massnahmen“
  - **Weitere Erlasse:**
    - Bundesinformatikverordnung (BinfV; SR 172.010.58)
    - Informationsschutzverordnung (ISchV; SR 510.411)
    - Obligationenrecht (z.B. Aufbewahrungspflichten, IKS)
    - Strafgesetzbuch (Cybercrime)
    - BG über die elektronische Signatur (ZertES; SR 943.03)
    - BG über Urheberrecht (URG; SR 231.1)
- **Internationale Standards**
  - ISO 27001/27002, BSI, COBIT, SOX, Basel II, OECD Guidelines, Information Security Forum (ISF)



Rechtliche Grundlagen (2)

- **Konkrete Verantwortlichkeiten im Bereich Informationsschutz?**

  - **Anwälte**
    Anwaltsgeheimnis (StGB 321)

  - **Bundesangestellte**
    Berufs-, Geschäfts- und Amtsgeheimnis (BPG 22)

  - **Unternehmensjuristen**
    Fabrikations- und Geschäftsgeheimnis;
    vertragliche Schweigepflichten

Rechtliche Grundlagen (3)

- **Beispiel „Münchner Anwaltsbüro“**

  Ein Münchner Anwaltsbüro führte eine elektronische Fristenkontrolle. Infolge mangelnder Datensicherung gingen **bei einem Systemabsturz Daten verloren.** Dadurch wurde die Frist für das Einreichen eines Rechtsbegehrens versäumt. Auf das verspätet eingereichte Rechtsmittel trat das Gericht nicht ein. Ein Antrag des Anwaltsbüros auf „Wiedereinsetzung der Frist“ wurde abgelehnt.

  (OLG München, 21U 2463/89, Beschl. Vom 02.05.1989, DuD, 102/90, S. 101/02)

- **In der Schweiz**
  - Schutzziele „Verfügbarkeit“ und „Integrität“ verletzt
  - Anwaltsbüro ist für elektronische Systeme zur Abwicklung seiner Geschäfte verantwortlich
  - Wiedereinsetzung einer versäumten Frist nur bei Umständen, die betreffende Partei nicht zu vertreten hat (Krankheit, Streik, usw.)

Information Security Society Switzerland
> vormals FGSec

Abgrenzung
Datenschutz / Informationssicherheit

Abgrenzung Datenschutz / Informationssicherheit

<u>Frage</u>: Handelt es sich um Daten einer natürlichen od. juristischen Person?

Datenschutz
schützt Personen(-daten)
und deren **Privatsphäre**

<u>Frage:</u> Handelt es sich um wichtige, geschäftskritische Informationen?

Informationssicherheit
schützt **alle Informationen** (auch Personendaten!): Papier, Wort, elektronische Daten, IT-Systeme, Programme, Prozessabläufe, Info.systeme, Datenbanken

Aktuelle Bedrohungen / Trends

Aktuelle Bedrohungen

- **Top 10 der Bedrohungen 2008:**
  - Drive-by Downloads
  - Eigene Mitarbeitende
  - Externe Mitarbeitende
  - Malware (Viren, Würmer)
  - Trojanische Pferde
  - Botnetzwerke
  - Software-Mängel
  - Hacking
  - Physische Bedrohungen
  - Neue Bedrohungen

Information Security Society Switzerland
> vormals FGSec

Konkrete Beispiele

1. Der Mitarbeitende

- **Gefahren**
  - Verlust oder Weitergabe von Informationen durch Unwissen, Unachtsamkeit, illegale Handlungen; Social Engineering!

- **Massnahmen**
  - Schulung der Mitarbeitenden (Sensibilisierung / Awareness)
  - Klare Richtlinien
  - Vertraulichkeitserklärungen: MA speziell verpflichten!

- **Folgen bei Nichtbeachtung**
  - Vertragsverletzungen ggn. Klienten
  - Haftung: Schadenersatz, Verlieren des Prozesses

2. Social Engineering

- **Gefahren**
  - Verlust von Personendaten, Geschäftsinformationen und Zugangsdaten an Dritte durch einfachen Trick (Telefon, E-Mail, Besucher, Internet-Foren, Soziale Netzwerke), Zutritt verschaffen an Unberechtigte

- **Massnahmen**
  - Sensibilisierung der Mitarbeitenden
  - Zwei-Faktoren-Authentifizierung
  - Passwörter nie doppelt verwenden
  - Besucher nie alleine lassen
  - Geschäftskritische oder vertrauliche Informationen nie per E-Mail
  - Datensparsamkeit im Internet!

„Dumb people hack systems, smart people hack persons.“

Bruce Schneier, Security Specialist

3. E-Mail

- **Gefahren**
  - Offen wie eine Postkarte, da unverschlüsselt; Aufbewahrungsdauer und –ort ungewiss; schnell!

- **Massnahmen**
  - Wichtige, geschäftskritische oder vertrauliche Daten verschlüsseln (PGP, WinZip 128/256bit)
  - elektronische Signatur (Authentizität und Integrität)
  - Briefpost oder Telefon

- **Folgen bei Nichtbeachtung**
  - Datenschutzrecht: Bekanntgabe an nicht berechtigte Dritte
  - Verletzung Anwaltsgeheimnis

A propos…

4. Soziale Netzwerke

- **Gefahren**
  - Weltweite Vernetzung, auf Ewigkeit gespeichert, Durchsetzung von Rechten schwierig, Menge, Türöffner für Social Engineering und Spam-Mails

- **Massnahmen**
  - Erst überlegen, dann handeln (Datensparsamkeit)
  - Datenschutz- und IS-Angebote des Anbieters nutzen

- **Folgen bei Nichtbeachtung**
  - Reputationsschaden der Firma oder der eigenen Person
  - Verletzung Geschäftsgeheimnis

Kritische Würdigung

Kritische Würdigung

- Datensparsamkeit
- Eigenverantwortung
- Vertrauen ist gut, Kontrolle ist besser. Hinterfragen Sie!
- Neuste Technik – beste Technik? Muss man immer und überall zu jeder Zeit alles zur Hand haben?
- Weniger ist manchmal mehr…

Information Security Society Switzerland
> vormals FGSec

Nützliche Links

Nützliche Links

IS für Unternehmen

- ISB: http://www.isb.admin.ch
- BSI: http://www.bsi.bund.de/
- ISSS: http://www.isss.ch

Bundesamt für Sicherheit in der Informationstechnik

IS für KMU und private Benutzer

- MELANI: http://www.melani.admin.ch/
- BSI für Bürger: http://www.bsi-fuer-buerger.de/
- Checkliste Bruce Schneier: http://www.schneier.com/essay-078.html

IT-Recht

- Deutsch Wyss & Partner: http://www.advobern.ch/

Fragen / Diskussion


THANK
YOU