it.sec
security for your information

Gemeinsamkeiten & Probleme beim Management von Informationssicherheit & Datenschutz

Gemeinsame Sitzung von AK 1 & 5 am 02.04.2013

Bernhard C. Witt (it.sec GmbH & Co. KG)

Bernhard C. Witt

- Berater für Datenschutz und Informationssicherheit bei der it.sec GmbH & Co. KG
  verantwortlich für die Geschäftsfelder
  ° Datenschutz (→ externer Datenschutzbeauftragter)
  ° IT Governance, Risk & Compliance Management
- Industriekaufmann, Diplom-Informatiker
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- zertifizierter ISO/IEC 27001 Lead Auditor (BSi)
- CRISC (ISACA)
- Lehrbeauftragter an der Universität Ulm (seit 2005)
- Autor der Bücher „IT-Sicherheit kompakt und verständlich“ (2006) und „Datenschutz kompakt und verständlich“ (2008 & 2010)
- Sprecher der GI-Fachgruppe Management von Informationssicherheit (seit 2009)
- Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit (seit 2009)
- Mitglied im Leitungsgremium der GI-Fachgruppe Datenschutzfördernde Technik (seit 2012)
- Mitglied im DIN-Arbeitsausschuss „IT-Sicherheitsverfahren“ AK 1 & 4 (seit 2011)

it.sec
security for your information

Blickwinkel

IKT:

- Technik (Hardware, Software, Netzwerkkomponenten, etc.)
- Überschaubarer Wert (absolut bestimmt!)

→ **Supporting Assets**

→ Wechsel von IKT-Sicherheit zur Informationssicherheit

Informationen:

- Daten (inkl. personenbezogener Daten), Prozessbeschreibungen (inkl. notwendiger Compliance-Prozesse)
- Wert abhängig von Geschäftszweck / Aufgabe (relativer Wert!)

→ **Primary Assets**

→ Supporting Assets erhalten ihren Wert anhand der von ihnen unterstützten Primary Assets

Vorgehensmodell ISO/IEC 27005

1) Bestimmung **Kontext** (insb. rechtliche Anforderungen, SLAs, interne Festlegungen)
2) Festlegung **Risikoanalyse Methodologie** (in Abhängigkeit zum Kontext m. Festlegung der Sicherheitsziele)
3) Festlegung **Risikoappetit** des Asset Owners
4) Durchführung **Risk Assessment** zur Steuerung des ISMS (unter Betrachtung der Supporting Assets!)

→ Risk Assessment anhand der Interessen der durchführenden Stelle

→ Datenschutz dagegen geht von Interessen der Betroffenen aus

→ weitere Sicherheitsziele: Transparenz, Intervenierbarkeit, Datensparsamkeit & Einhaltung der Zweckbindung

Praxis-Probleme (1): Im Binnenverhältnis

- **Daten über Kunden / Patienten / Mandanten / Versicherte / kritische Infrastrukturen** etc.
  → **wesentliches Schutzgut**
  → i.d.R. große Anzahl Betroffener
  → dann Datenschutz maßgeblich für ISMS!
- **Daten über Mitarbeiter** dagegen häufig (international) **kein ausdrückliches Schutzgut**
  → i.d.R. (vergleichsweise) kleine Anzahl Betroffener
  → hier Datenschutz faktisch nur unter Compliance betrachtet

→ Unterschiedliche Wertschätzung innerhalb der Einrichtung für jeweilige Teil-Informationen

→ Unterschiedliche Wichtigkeit für ISMS-Steuerung!

Praxis-Probleme (2): Im Binnenverhältnis

- **Daten für Wertschöpfungskette** (z.B. Konstruktionsdaten, Rezeptdaten → Betriebs- & Geschäftsgeheimnis; personenbezogene Daten über Kunden / Patienten / Mandanten / Versicherte → Datengeheimnis):
  → grundlegend für Einrichtung, da Erfolg davon abhängt
  → **hoher Schutzbedarf** (gleich bei mehreren Sicherheitszielen!)
- **Daten für Support Assets** (z.B. IT, Mitarbeiter, Räume) dagegen nur von nachrangigem Interesse
  → **maximal mittlerer Schutzbedarf** (und das auch nur bei wenigen Sicherheitszielen)

→ Erweiterung der Sicherheitsziele bei ISMS zugunsten des Datenschutzes aus Steuerungssicht eher unwahrscheinlich (stattdessen: Prozesse zur Compliance!)

Praxis-Probleme (3): Im Außenverhältnis

- Auftragnehmer hat u.U. **anderen Risikoappetit** als ihre Auftraggeber (Pönale i.d.R. weit geringer als potenzieller Schaden bei Eintritt des Risikos!)
- Auftragnehmer verwendet oft **andere Risikoanalyse Methodologie** als ihre Auftraggeber (Geschäftsmodell!)
- Auftragnehmer hat **andere Vorstellung hinsichtlich meldepflichtiger Security Incidents** als Auftraggeber, wenn dies nicht ausdrücklich festgelegt wurde (ist aber nur bedingt möglich)
- Für Auftragnehmer ist es i.d.R. von **nachrangigem Interesse**, **welche Datenkategorien** im Auftrag verarbeitet werden, für Auftraggeber sind dagegen die überlassenen Daten u.U. grundlegend

→ jeweilige ISMS stark voneinander abweichend!

Vielen Dank für Ihre Aufmerksamkeit!

it.sec GmbH & Co. KG
Einsteinstr. 55
D-89077 Ulm

USt Id Nr.: DE 225547544
Steuernummer: 88012/53709
Amtsgericht Ulm: HRA 3129

vertreten durch den **Geschäftsführer Dipl. Ing. (FH) Holger Heimann**

Haftender Komplementär:
it.sec Verwaltungs GmbH
Amtsgericht Ulm: HRB 4593
Einsteinstr. 55
D-89077 Ulm