AIG – @medialawcamp, Berlin 2016

Compliance im Zeitalter von Cyber-Risiken

CYBER-RISIKEN und Compliance
Herausforderungen bei der Kommunikation

Geschäftsführung

1. Die IT Sicherheit ist (ausschließlich) ein Thema der IT
2. Die IT ein reines Costcenter
3. Wir müssen Kosten sparen

IT Verantwortlicher:

1. Ich muss um mein IT-Budget und Aner-kennung unserer Arbeit kämpfen
2. Alle externen Ausgaben (auch die für Risikotransfers) gehen zu Lasten der ITBudgets

Rechtsabteilung

1. Oberste Priorität haben Schutz von Unternehmen und -sführung
2. Welche deutschen Normen / Urteile sind für die Risiko-beurteilung relevant?

Maker / Versicherer

1. IT-Sicherheit ist ein schwieriges Thema. Ich halte mich an meinen One-Pager (Datenschutz)
2. Ein paar “Buzz”-words aus der aktuellen Presse, passen immer.

AIG

Schadenbeispiele

Fall a)

Das Warenwirtschaftssystem eines produzierenden Unternehmens ist Ziel einer DDoS-Attacke und erleidet in Folge einen partiellen Produktionsausfall.

Fall b)

Eine Rechtsanwalts- und Steuerberaterkanzlei kann nicht mehr auf ihre Korrespondenzdaten zugreifen, da diese durch den Verschlüsselungsvirus Dorifel verschlüsselt wurden. Die nähere Untersuchung deutet darauf hin, dass weitere Schadcodes nachgeladen wurden. Unter anderem wurden wahrscheinlich Codes zum Stehlen von Bankdaten installiert, wie anhand gefundener Logfiles mit Namen, Kreditkarten- und Kartenprüfnummern gefolgert werden kann.

AIG

Schadenbeispiele

Fall c)

In einem Industrieunternehmen wurde festgestellt, dass auf einem Bediener-PC unzulässige Software installiert war, um urheberrechtlich geschützte Filme von Torrent-Servern herunterzuladen. Dadurch wurde eine mobile Datenanbindung des Bediener-PC zum zentralen Internetzugang überlastet und wichtige IT-gestützte Geschäftsprozesse beeinträchtigt.

Fall d)

Ein Dienstleistungsunternehmen erhält eine erpresserische Nachricht. Bei Nichtzahlung sollen „gestohlene“ Kundendaten im Internet veröffentlicht und die Presse informiert werden. Das Unternehmen hat Vertriebsstandorte im Ausland.

AIG

Schadenbeispiele

Fall e)

Nach Auspionieren der Server eines Zielunternehmens werden die dort gewonnenen Daten von Kriminellen für eine „Fake President“ – Attacke verwendet. (der Personalchef wird dazu gebrrcht sämtliche Mitarbeiterdaten per E-Mail zu versenden.

Fall f)

Es wurde bei einer Routineprüfung festgestellt, dass auf einem Server in einem für alle User frei zugänglichen Share über einen längeren Zeitraum vertrauliche Daten gespeichert werden.

AIG

Schadenbeispiele

Fall g)

Ein globales Unternehmen stellt fest, dass eine Webseite in Asien gehackt wurde. Bei der Ermittlung wird festgestellt, dass es neben diesem Angriff zu weiteren Angriffen gekommen ist, die auch Server in der DMZ in Deutschland kompromittiert haben. Es wurden alle Server angegriffen und User-Daten gestohlen. Zusätzlich kam es zu einer Kompromitierung auch von internen Servern.

Fall d)

„Services“ aus dem Darknet …

Compliance im Zeitalter von Cyber-Risiken

Wer ist für was verantwortlich?

- intra company
  - CEO
  - COO
  - CIO
  - CISO
- inter company
  - Dienstleister
  - Geschäftspartner
  - Endkunden
  - Lieferanten
  - Staat

Welche Unternehmen sind besonders betroffen?

- Finanzinstitute
- Telekommunikationsdienste
- Öffentlicher Sektor
- Produzenten
- Land/Region
- Einzelhandel
- Versorgungsunternehmen

Wo ist Compliance besonders relevant?

- Kundendaten
- Produktionssteuerung
- R&D
- Datenaustausch
- Outsourcing

Schäden?

- Betriebsunterbrechung
- Schadensersatzforderungen
- Reputationsverlust
- Strafen, Bußen

Welche Regeln gelten?

- Land/Region
- Gesetze
- Moral
- Normen
- Open Source
- Verträge
- Lieferanten
- PCI, etc.
- Dienstleister
- Kunden

AIG

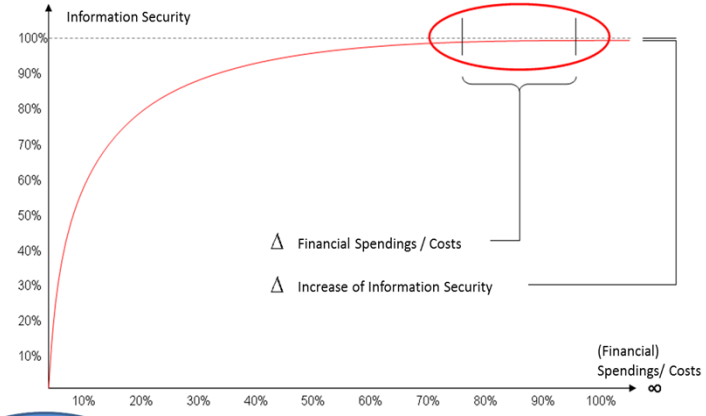
CYBER RISK

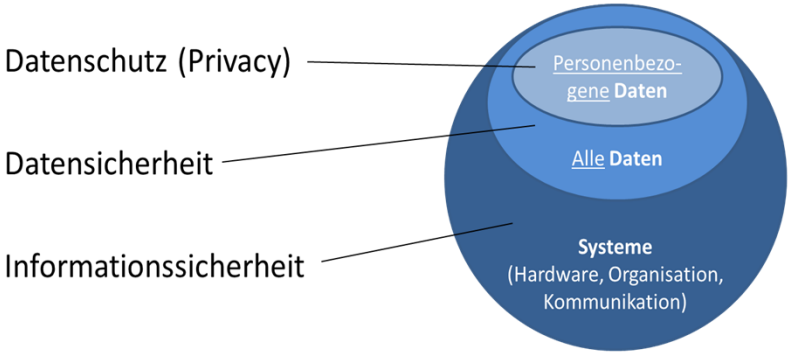
Schwerpunkte, Fallstricke, Erwartungen
Herausforderungen in der Kommunikation

§

Einfache Begriffe = „Sichere“ Begriffe:

- ✓ Schadprogramm
- ✓ Verletzung der
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit





AIG

Vielen Dank

Weitergehende Fragen richten Sie gerne an:

Thomas Pache
Dipl.-Ing., Dipl.-Wirtschaftsingenieur
Manager Professional Indemnity
Financial Lines

T +49 (0) 69 97113-288 Frankfurt
T +49 (0) 40 3604-503 Hamburg
M +49 (0) 151 16719100
E thomas.pache@aig.com