Leitthemen WS 2: „Sichere Dienste und Prozesse im Internet“

1) Welche Richtung nimmt die Informationssicherheit in Unternehmen allgemein?
2) Welche Handlungsbedarfe ergeben sich daraus für Unternehmen?
3) Wie steht es mit der Haftung in den Unternehmen? Hilft diese die Sicherheit besser zu verankern (analog zu Financial Services Industry)?
4) Vor dem Hintergrund der Herausforderungen einer Cybersecurity-Strategie: Welches sind die Lessons Learnt aus dem Workshop und welchen Beitrag können die im Workshop genannten Aspekte hierzu leisten?

1. Welche Richtung nimmt die Informationssicherheit in Unternehmen allgemein?

- Internet ist grenzenlos, aber Gesetze sind national und europäisch.
- Perimeterschutz (z.B. Firewalls) reicht nicht mehr aus.
- Substitution von Passwörtern rhetorisch akzeptiert, aber nicht (konsequent) umgesetzt
- Business und private Kommunikation ändern sich (weniger E-Mail, mehr Messenger und Social Media)
- Schwachstellen Google und Facebook
  - Single-Sign-On
  - Always-Online

2. Welche Handlungsbedarfe ergeben sich daraus für Unternehmen?

- Vorbildfunktion des Managements muss stärker werden!
- Vermarktbarkeit von Sicherheit über Kundennutzen
- Social Media als Enabler für Akzeptanz
- Vereinheitlichung der E-Mail-Sicherheitslösungen
- Daten müssen “sich selber schützen”.
- Schwachstellen bei Webanwendungen (Google und Facebook)
  - Standardisierung besserer Web-Protokolle erforderlich
  - Einführung Business Browser?
- Device Management, BYOD/**BYOS**
  - Application Container und entspr. Policies erforderlich

3. Wie steht es mit der Haftung in den Unternehmen?
Hilft diese die Sicherheit besser zu verankern?

- Ist das für Haftung notwendige Rechts-verständnis für neue Anwendungen (etwa Cloud) gegeben?
- Finanzieller Druck über Haftung – auf wen?
- „Endnutzer“ von der Haftung freistellen oder nicht oder halb oder …?
- BYOD/BYOS kann zu Kollision mit Lizenzbedingungen der SW führen.
- Versicherbarkeit der Risiken erst durch hinreichendes Sicherheitsniveau ermöglicht.

4. Vor dem Hintergrund der Cybersecurity-Strategie: Lessons Learnt und Beiträge aus dem Workshop

- Abholung des Nutzers zwingend
- Unterschiedliche Bedarfe bei Nutzern akzeptieren
- Verschlüsselung besonders wichtig
- Bei Cloud ist speziell der Zugang zu schützen
  - Zur Authentifizierung nicht nur Passwörter
  - HTML5-Chaos muss beschnitten werden.
- Proaktive Sicherheit:
  - Analysetools erforderlich zur Identifizierung von Schwachstellen vor dem Schadfall
  - Aber Totalüberwachung hilft auch nicht.
- Virtualisierung der einzelnen Anwendungen kann pragmatisch helfen.
- Insgesamt hoher Forschungs- und Entwicklungsbedarf!