Cyber Security in der Praxis

Aufbau und Weiterentwicklung eines ISMS

Agenda

Vorstellung

Dr. Bettina Thurnher

Cyber Security in der Praxis

Wie kann man sich als Unternehmen schützen?

Aufbau eines ISMS

3 Faktoren für die Informationssicherheit

Kernelement der Informationssicherheit

Was wollen wir erreichen?

Und nach der Erstzertifizierung?

Weiterentwicklung des ISMS

Austausch mit PwC

Chinese Walls und andere Herausforderungen in der ISMS Prüfung und Security-Beratung

Wie kann ich Ihnen helfen?

Informationssicherheit bei GW

Bettina Thurnher

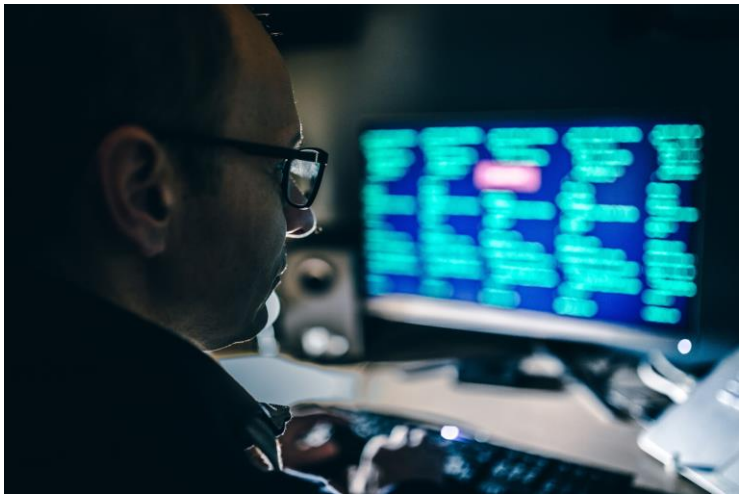
Information Security Manager bei Gebrüder Weiss GmbH

bettina.thurnher@gw-world.com

- Studium im Projekt- und Prozessmanagement, Promotion in Informatik
- Ausbildung zur ISO 27001 Lead Auditorin, geprüfte Datenschutz Managerin
- Mehrjährige Berufserfahrung in der Telekommunikationsbranche
- Informationssicherheit bei GW
  - Aufbau des Informations Sicherheits Management Systems (ISMS) und des Data Protection Management Systems (DPMS)
  - ISO 27001 Zertifizierung und Rezertifizierungen der Corporate IT

Cyber Security in der Praxis

Wie kann man sich als Unternehmen schützen?



- Absolute Sicherheit existiert nicht!
- Aber: als Unternehmen kann man viele Maßnahmen ergreifen um Risiken zu minimieren
  → **risikobasierter Ansatz**
- Informationssicherheit behandelt diese Themen: Normen ISO 27001, ISO 27002 schlagen eine Reihe von Good Practices vor
- ISO 27001 Zertifikat bringt Vorteile
  - ✓ Kundenanforderungen hinsichtlich Cyber Security sind erfüllt
  - ✓ Wettbewerbsvorteil: bei Ausschreibungen oft notwendig
  - ✓ Dauerhafte Sicherung von Marktanteilen durch Schutz vor Angriffen

Aufbau eines Informations Sicherheits Management Systems (ISMS)

3 Faktoren für die Informationssicherheit

Ausreichend Know-How muss zur Verfügung stehen:
Begleitung durch externe Beratung

Menschen

Prozesse

Technologie

Aufbau eines Informations Sicherheits Management Systems (ISMS)

3 Faktoren für die Informationssicherheit

Menschen

Prozesse

Technologie

- Einbeziehung der Mitarbeitenden
- Bewusstseinsbildung: Schulungen: Face-to-face, E-Learnings
- Erläuterungen und Dokumentation für Mitarbeitende: Richtlinien
- Etablierung Information Security Agents zur Unterstützung der Mitarbeitenden
- Unterstützung der Geschäftsleitung
    - Ressourcenbereitstellung
    - Vorbildwirkung

Aufbau eines Informations Sicherheits Management Systems (ISMS)

3 Faktoren für die Informationssicherheit

Menschen

Prozesse

Technologie

- Dokumentation der Prozesse Z.B.:
  - Risikomanagement
  - Projektmanagement
  - Änderungsmanagement
  - Eintritt, Wechsel oder Austritt von Mitarbeitenden
  - Notfallmanagement
  - IT-Lebenszyklus: Asset Management: Installation bis Deinstallation

Aufbau eines Informations Sicherheits Management Systems (ISMS)

3 Faktoren für die Informationssicherheit

Menschen

Prozesse

Technologie

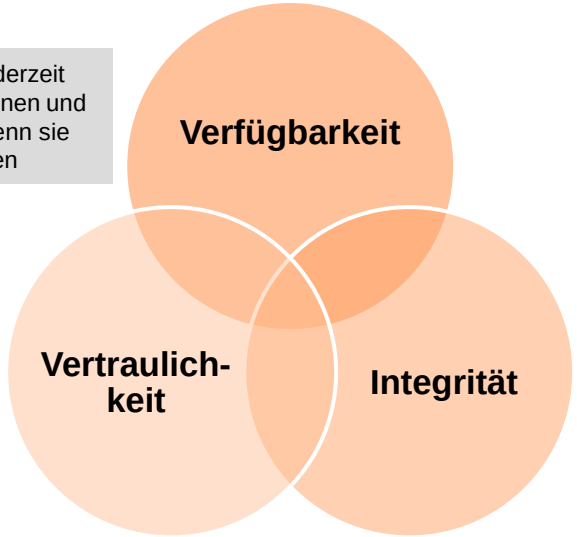
- IT-Sicherheit ist nur ein Teil von Informationssicherheit!
- Z.B.:
  - Applikationen: Pentests
  - Betriebssysteme: Virenschutz
  - Netzwerk, Firewall, NAC
  - Server Hardware: Härtung
  - Mobile Endgeräte: MDM
  - Zutrittskontrolle

Kernelement der Informationssicherheit

Was wollen wir erreichen?

Für GW steht die Verfügbarkeit an erster Stelle, da Kundendaten hoch verfügbar sein müssen und nicht verloren gehen dürfen!

Benutzer sollen jederzeit Zugriff auf Informationen und Systeme haben, wenn sie diese benötigen



Zugriff auf Informationen darf nur erfolgen, wenn die Notwendigkeit und die Berechtigung dafür besteht

Vollständigkeit und Richtigkeit von Informationen und deren Verarbeitung

Und nach einer Erstzertifizierung

→ Weiterentwicklung des ISMS

Wichtiger Bestandteil der ISO 27001 Norm:
Kontinuierlicher Verbesserungsprozess

Menschen

- Motiviation zum kritischen Nachdenken
- Themenspezifische Schulungen (Secure Coding, Secure Testing, Requirements Engineering)

Prozesse

- Weiterentwicklung von Dokumentationen hinsichtlich Praxistauglichkeit
- Strategische Weiterentwicklung: Stabiler IT Betrieb und Informationssicherheit

Technologie

- Kontinuierliches Anpassen auf aktuelle State-of-the-art Good Practices
- Informationssicherheit in neuen Technologien: Stichwort Cloud Services

Und jetzt:

- Fragen?
- Anschließender Austausch mit langjährigem Berater PwC

Gebrüder Weiss
Transport and Logistics