



IT-Sicherheitsgesetz - Konsequenzen für die Lieferketten der KRITIS- Dienstleister

Matias Krempel
stv. Leiter Arbeitskreis „Audits und Standards“

20.02.2019

- Versorgung der Bevölkerung, Sicherstellung von kritischen Prozessen, innere und äußere Sicherheit
- „All-Hazards“-Ansatz
- Komplexität moderner Gesellschaften

Worum geht es?

- Produkte, Services, Prozesse
- Maßnahmen (präventiv, detektiv, reaktiv)
- Zusammenspiel der Handelnden
- Kontinuierliches Nachsteuern

Woher kommen wir?

- Quality und Safety
- Security in Management- und Produktbezogenen-Standards
- Nachweis- / Zertifizierungsverfahren und –organisationen

Wo stehen wir aktuell?

- Cybersecurity-Fokus in Europa auf „Essential Services“
- Umsetzung (national und supranational)
- Zertifizierungsbedarf für die „Lieferketten“
- Befürchtungen und Wünsche der Betroffenen

Was wird uns nun beschäftigen?

- Erweiterter Fokus auf Security in der Lieferkette (Produkte, Services, Prozesse)
- Neue rechtliche Regelung „Cyber-Security-Act“
 - Zertifizierungsverfahren und –organisationen
 - Zertifizierungsdienstleister
- Wettbewerbsfaktor vs. Verbindlichkeit

Wie können wir uns organisieren?

- Standards (mit-)gestalten
- Integration in bestehende Prozesse
- Branchenspezifische Security-Toolkits
- „Schicksalsgemeinschaften“ von Herstellern und (KRITIS)-Dienstleistern organisieren

*Tu erst das Notwendige, dann das Mögliche
und plötzlich schaffst du das Unmögliche.*

FRANZ VON ASSISI

Kleine Bibliographie

- EU-Dokumente (insbesondere NIS-Richtlinie Directive (EU) 1148/2016 und Vorschlag "Cybersecurity Act", (COM/2017/0477 final - 2017/0225 (COD) abrufbar unter <https://eur-lex.europa.eu/>)
- Dokumente der Bundesrepublik Deutschland zum Schutz kritischer Infrastrukturen (incl. IT-Sicherheitsgesetz) https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/Strategie/strategie_node.html
- Sachstand der Umsetzung der NIS-Direktive in Europa <https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive>
- Katalog der IT-Security Gesetze und Standards (IT-Security Navigator) <https://www.itsecuritynavigator.de/>
- ENISA Unterlagen zur Cybersecurity Standardisierung https://www.enisa.europa.eu/events/cybersecurity_standardisation/
- Unterlagen der Bundesnetzagentur zu Kritischen Infrastrukturvorgaben für die Sektoren „Energie- und Telekommunikation“

Bilder sämtlich aus [commons.wikipedia.org](https://commons.wikimedia.org)
und gemäß Creative Commons nutzbar (creativecommons.org)
Einzelnachweise sind in den Notizen zu dieser Seite vermerkt