Schweizerischer Brunnenmeister-Verband

Cyber-Crime für kritische Infrastrukturen

Chestonag Automation AG
Remo Bruder

GWF AG
Joel Bossi

Rittmeyer AG
Patrick Erni

Schweizerischer Brunnenmeister-Verband

IKT-Minimalstandard

Empfehlungen für Cybersicherheit durch BWL (Bundesamt für wirtschaftliche Landesversorgung)
Der Bundesrat hat im **April 2018** die nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) für die Jahre 2018 bis 2022 verabschiedet. Im Rahmen dieser Strategie hat das BWL den Minimalstandard zur Cybersicherheit veröffentlicht. Der Standard ist als Richtlinie für die Basissicherheit für Anbieter und Betreiber von kritischer und nicht-kritischer Infrastruktur konzipiert. Er hat **Empfehlungscharakter** und basiert auf international anerkannten Standards, anhand derer die Cybersicherheit eines Unternehmens bewertet werden kann.

Cyber-Security erklärt mit Hilfe vom IKT-Minimalstandard

Bedrohung + **Schwachstelle** = **Gefahr (Auswirkung)**

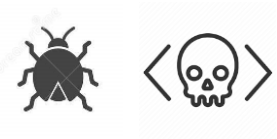
- E-Mail → Manipulation
- USB-Speicher → Diebstahl
- Internet → Erpressung
- Netzwerk → Ausfall
- Mitarbeiter → Zerstörung, Verlust

An der Bedrohung können wir nichts ändern - Schwachstellen können jedoch vermieden werden

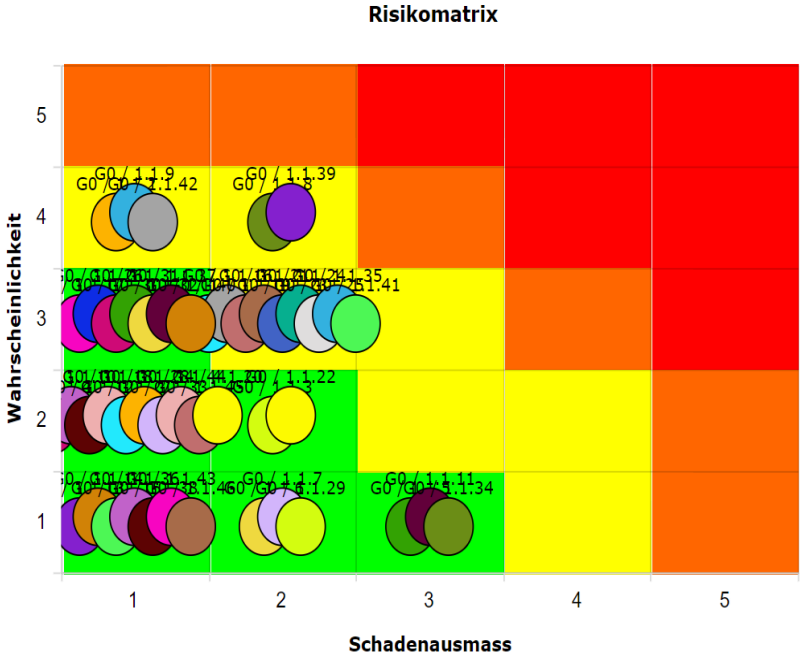
Wer bedroht mich?

Mensch

Software



Traditionelle



Schweizerischer Brunnenmeister-Verband

Was habe ich?

Identifizieren

Inventar

- Hardware
- Software
- Netzwerk
- SCADA / SPS
- User
- Rechte

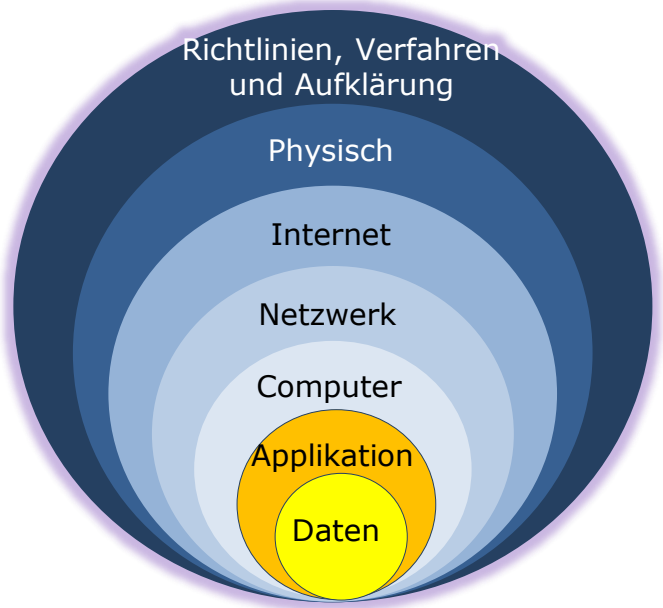
Schwachstellen

- Mensch (Social Engineering)
- Physisch
- Internet
- E-Mail
- Netzwerk
- WLAN
- Software
- Hardware
- USB-Schnittstelle

Wie schütze ich mich?

Massnahmen = Hindernisse einbauen mit defence in depth (mehrschichtiger Ansatz)

Normen
Schulung / Aufklärung
Abschliessen
Firewall
Passwort / 2FA
Zonierung
Netzwerküberwachung
Services
Systeme Härten
Software Update
Antivirus
Backup



Gefahr erkannt – Gefahr gebannt?

Erkennen

Gefahr

Angreifer

ERKENNEN

1. Auffälligkeiten und Vorfälle
2. Überwachung
3. Detektionsprozess

Angriffsvektor

Schwachstelle Mensch

Schwachstelle Software

Traditionelle Schwachstellen

Massnahme

Awareness

IT Sicherheit

Physische Sicherheit

Information

Information

Was tun, wenn der Angriff stattfindet?

Reagieren

Attack

Präventive Phase: Wie wir Informationsangriffe verhindern.

Reaktive Phase: Was wir tun können, wenn ein Angriff stattfindet

Erste Verteidigungslinie

- Awareness
- IT Sicherheit
- Physische Sicherheit

Zweite Verteidigungslinie

- Know-How Cyber-Abwehr
- IT-Notfallsicherheit
- Notfallmassnahmen

Dritte Verteidigungslinie

Business Continuity Management:

1. Reaktionsplanung inkl. AKV
2. Kommunikation und Unterstützung
3. Analyse: Vorbereitung ist die beste Verteidigung
4. Schadensminderung: Schnelles und effektives Verhalten mindert den Schaden
5. Verbesserungen: PDCA, denn aus Fehlern lernt man.

Information

Idee: Live-Szenario durchspielen um die theoretischen und eher abstrakten Vorgaben mit einem Praxisbeispiel zu vertiefen. Gerne können dazu aus dem Publikum Vorschläge zu einem Szenation gemacht werden.

Wiederherstellungsplanung

- Vor dem Ereignis bereits planen!
  - Was muss sofort wieder laufen?
  - Prozesse definieren, laufend anpassen und validieren
  - Prozesse und Verfahren vorher testen.
    - Beispiel Backup
    - Wo liegt nochmal der Wiederherstellungsplan?

- Checkliste
- Es dauert länger als man denkt.
- Zurück zur Normalität

Verbesserungen

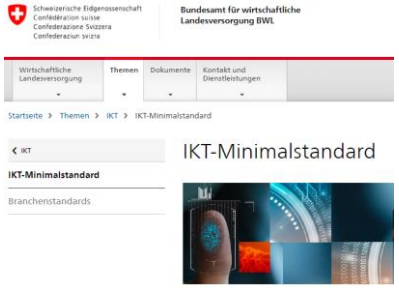
- Aus einem Ereignis lernen (auch aus Fehlern anderer)
  - Konnte das Kern/Tagesgeschäft aufrecht erhalten werden?
  - Was muss verbessert werden?
- Prozesse/Verfahren anpassen.

- Cybersecurity ist ein Prozess

Kommunikation

- Interne und Externe Partner informieren
  - Behörden, Kunden, Lieferanten, Mitarbeiter, Familie,…
- Reputation erhalten bzw. wiederherstellen
  - Offene, ehrliche, rasche Kommunikation
- Detaillierte Kommunikation der ausgeführten Wiederherstellungs-Schritte

https://www.ncsc.admin.ch



https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Schweizerischer Brunnenmeister-Verband

Zusammenfassung

Identifizieren	Schützen	Erkennen	Reagieren	Wieder-herstellen	
Inventar Management	Zugriffsmanagement und -steuerung	Vorfälle	Response Planning	Wiederherstellungs-planung	5
Geschäftsumfeld	Awareness und Training	Überwachung	Kommunikation	Verbesserungen	
Governance	Datensicherheit	Detektions-Prozess	Analyse	Kommunikation	
Risikomanagement	Schutz von Daten		Mitigation		23
Risikomanagement Strategie	Maintenance		Verbesserungen		
Lieferketten-management	Protective Technology				

Der IKT-Minimalstandard hilft mir mit den 106 Fragen meine Cyber-Security zu analysieren und einen bestmöglichen Schutz zu erstellen.