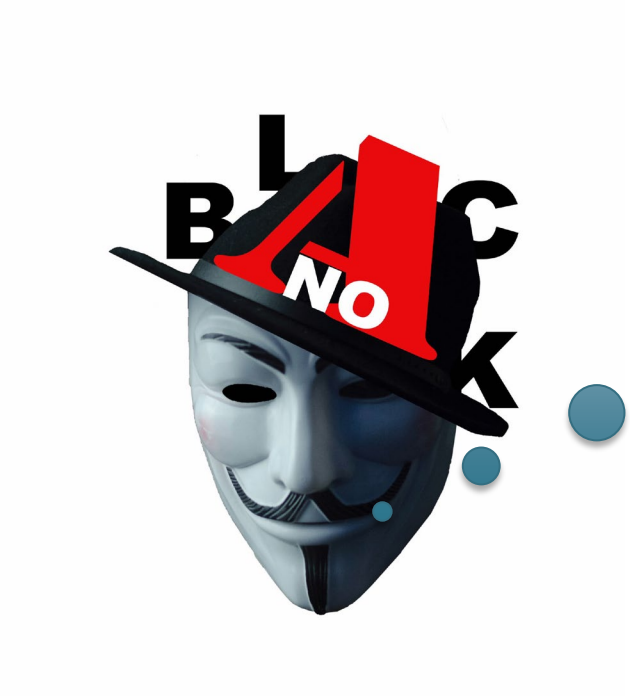
INFRA PROTECT

Cyber Security
als neue Herausforderung für die Versorgungssicherheit

Was man wissen sollte….



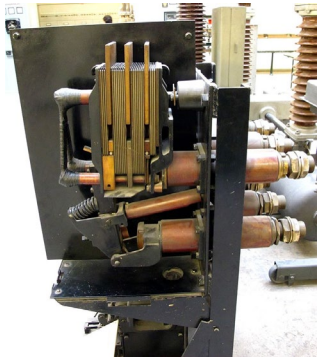
NEIN

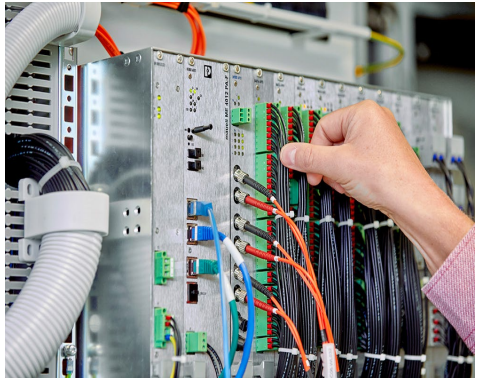
Agenda

1. **Status nascendi und die Genese in der E-Wirtschaft**
2. **Vorgehensmodell einmal anders**
3. **Angriffsformen bis hin zum APT**
4. **Heute die Zukunft denken**
5. **Viribus unitis**

RELEASE TO PUBLIC

Entwicklung der letzten Jahrzente





E-CONTROL

Y2K

2010: österreichweite Risikoanalyse Elektrizität

Update 1&2

Gas 2016

2020/21 Energiewirtschaft

2021 Energie + Telekommunikation

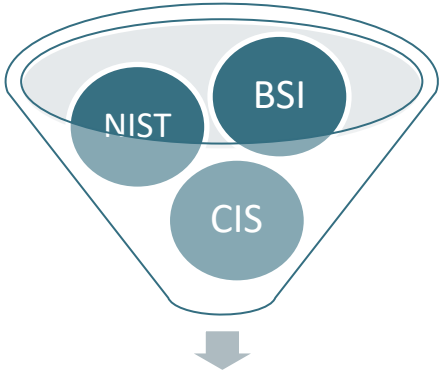
FGW FACHVERBAND GAS WÄRME

oesterreichs energie.

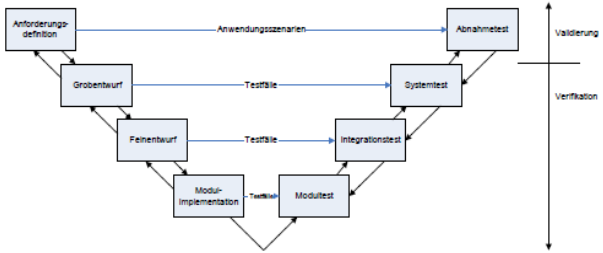
RELEASE TO PUBLIC

IT-V-Modell & Verwundbarkeit

Normatives Vorgehensmodell (Bundeswehr)



Gefahren & Bedrohungen relevant für die Energiewirtschaft



- DIN/ISO 31.000, Risk management (ONR 49.000ff)
- DIN/ISO ISO 31.010, Risk assessment techniques
- ISO 22.300, Business continuity management
- ISO 22.301, Societal security, business continuity management requirements
- ISO 22.313, Business continuity management, System Guidance
- ISO 27.002 Information security management systems
- ISO 27.019 Energiewirtschaft
- BDEW-White-Paper
- NETWORK-CODE

– ON S 2412, Security Management System: Begriffe und Definitionen
– ON S 2413, Security Management System: Grundlagen und Prozesse
– ON S 2414-1, Leitfaden für die Einbettung der Informationssicherheit in das Security Management System
– ON S 2414-2, Leitfaden für die Einbettung der Physischen Sicherheit in das Security Management System
– ON S 2414-3, Leitfaden für die Einbettung von Resilienz Management in das Security Management System
– ON S 2415-1, Anforderungen an ein Security Management System
– ON S 2415-2, Anforderungen an die Qualifikation eines Security Managers

413 spezifische Normen

IEC ……

DIN/EN

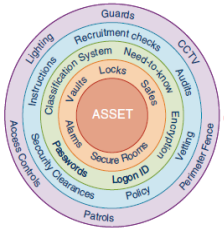
RELEASE TO PUBLIC

Was Sie/Wir akzeptieren müssen

Den ersten Schritt setzt IMMER der/die

ANGREIFER

physische Security Konzepte (

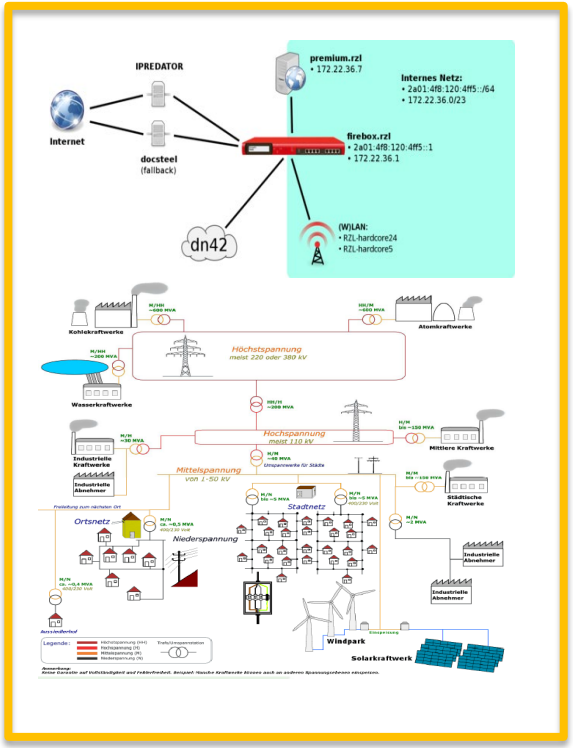


eifen zu kurz

Erkennen, Kanalisiern, Reagieren

Verwundbarkeitsanalyse 3-Schritte

» Angriffsziel



Machbarkeit

RELEASE TO PUBLIC

Auswirkung

Machbarkeit & Verwundbarkeit technisch – wer ?

» IEC 62443 Security Levels in Industrial Control Applications

Security Level	Target	Skills	Motivation	Means	Resources
SL1	Casual or coincidental violations	No Attack Skills	Mistakes	Non-intentional	Individual
SL2	Cybercrime, Hacker	Generic	Low	Simple	Low (Isolated Individual)
SL3	Hacktivist, Terrorist	ICS Specific	Moderate	Sophisticated (Attack)	Moderate (Hacker Group)
SL4	Nation State	ICS Specific	High	Sophisticated (Campaign)	Extended (Multi-disciplinary Teams)

Bewertungstabelle		
Machbarkeit Intentionale Gefahren		Bewertung Punkte
Verbale Beschreibung	Aufwand in Zeit und Know-how	
Sehr hoher Aufwand für die Tatausführung. Setzt Wissen voraus, das man sich durch sehr intensive Beschäftigung mit der Materie über einen längeren Zeitraum aneignen muss. Die Tat setzt auch voraus, dass man physische oder organisatorische IKT Barrieren unentdeckt überwinden kann. Eingesetze Hilfsmittel zur Überwindung (Angriffsmethoden/Vektoren) sind bis dato unbekannt.	Wochen - Monate der Vorbereitung / Expertenniveau vgl. auch State Actors inkl. gezielter Aufklärung	1
Hoher Aufwand für die Tatausführung. Setzt Wissen voraus, das man sich durch intensive Beschäftigung mit der Materie aneignen kann. Die Tat setzt voraus, dass man organisatorische IKT Barrieren (auch soziale Kenntnisse) unentdeckt überwindet. Es wird ein Mix aus bekannten und unbekannten Angriffsmethoden/Vektoren verwendet. Information über Infrastruktur und Zugriffsmöglichkeiten darauf. Angriffe auf die physische Infrastruktur Layer 1 (LWL, Koax, Cu, Funk).	Wochen der Vorbereitung - spezielle Fachkenntnisse werden vorausgesetzt z.B. APTs - auch in Kombination mit social Engineerung	2
Überschaubarer Aufwand für die Tatausführung. Das Ziel hat subjektiv eine gewisse Attraktivität. Die Tat setzt voraus, dass bekannte Schwachstellen in organisatorischen IKT Barrieren mit bekannten Hilfsmittel überwunden werden müssen. (Keine Automatisation der Angriffe/Vektoren)	Tage der Vorbereitung- Fachkenntnisse werden vorausgesetzt. Auch kriminelle Handlungen	3
Geringer Aufwand für die Tatausführung. Das Ziel hat eine subjektiv hohe Attraktivität. Die Tat setzt voraus, dass bekannte Schwachstellen in IKT-basierten Barrieren mit vorhandenen Werkzeugen automatisiert überwunden werden können.	Wenige Tage der Vorbereitung werden vorausgesetzt. Manipulationen durch Insider	4
Sehr geringer Aufwand für die Tatausführung notwendig. Es reicht bestehende Hilfsmittel/Werkzeuge für die Überwindung von IKT-Barrieren einzusetzen, um erfolgreich zu sein.	Es stehen bereits anpassbare Werkzeuge bzw. Werkzeugkisten zur Verfügung. Die Tat kann von interessierten Laien begangen werden. Hacktivisten	5
Aufwand wird auch finanziell verstanden		

Agenda

1. **Status nascendi und die Genese in der E-Wirtschaft**
2. **Vorgehensmodell einmal anders**
3. **Angriffsformen bis hin zum APT**
4. **[Heute die Zukunft denken]**
5. **Viribus unitis**

RELEASE TO PUBLIC

Heute die Zukunft denken
IKT-Risikoanalyse - Version 4.0 Stand März 2021

4.1 Domänenmodell.at-Strom

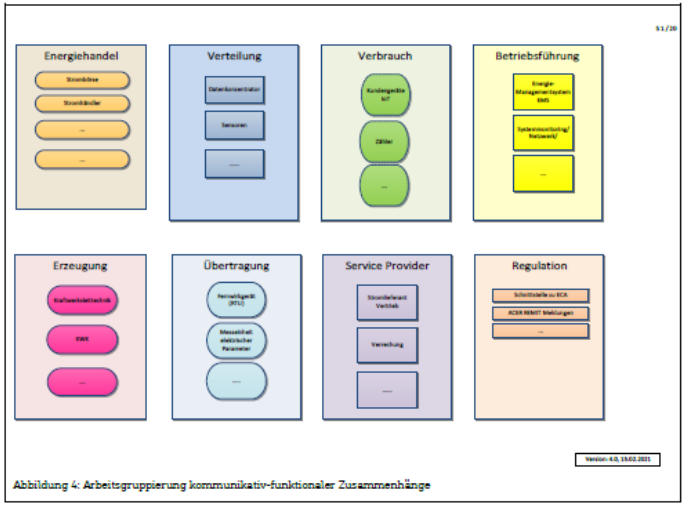


Abbildung 4: Arbeitsgruppierung kommunikativ-funktionaler Zusammenhänge

In Anlehnung bzw. abgeleitet aus dem NIST-Domänenmodell wurden in der Version 1.0 der IKT-Risikoanalyse Strom folgende Gruppen funktionaler Einheiten zusammengefasst:

- Erzeugung
- Verteilung
- Übertragung
- Betriebsführung
- Energiehandel
- Verbraucher
- Regulation

4.2 Domänenmodell.at-GAS

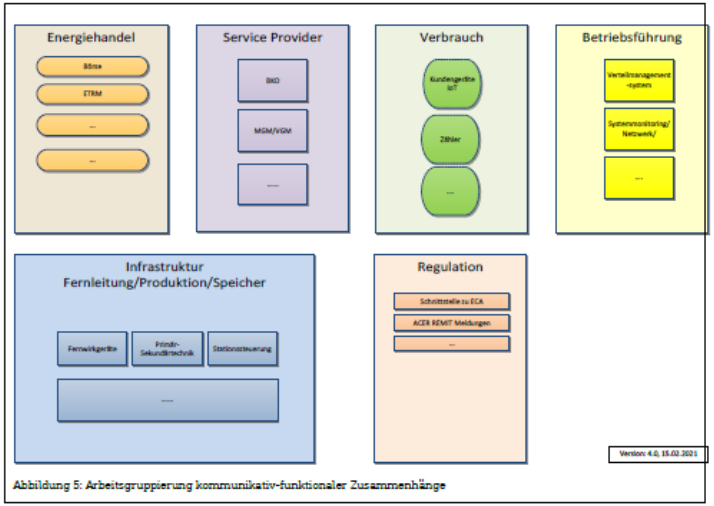


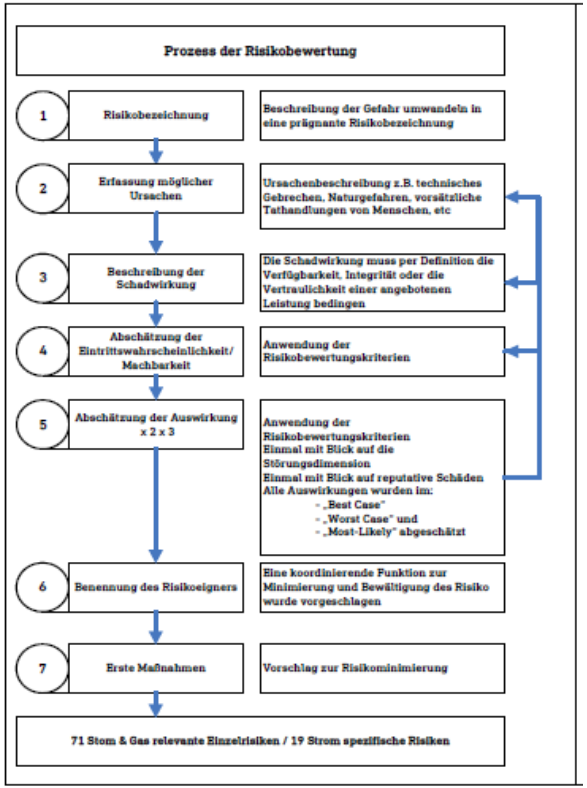
Abbildung 5: Arbeitsgruppierung kommunikativ-funktionaler Zusammenhänge

Das Domänenmodell fasst folgende Gruppen funktionaler Einheiten zusammen:

- Infrastruktureinrichtungen
- Entitäten in der Betriebsführung
- Entitäten des Energiehandels
- Entitäten aus Sicht von Service Providern
- Entitäten im Verbrauch
- Aspekte im regulierten Markt

RELEASE TO PUBLIC

Heute die Zukunft denken



- Dzt. und ex ante 226 tatsächlich relevante Gefahren (Hazard& Threats)
- 71 gemeinsame Risiken
  - Empfehlungen inkl. Monitoring
  - Mitigierende Maßnahmen
  - Umsetzungshorizonte

RELEASE TO PUBLIC

Heute die Zukunft denken

- » Einführung neuer Technologien
- » Expertise der Angriffe
- » Faktor Mensch
- » Technisch /organisatorische Unzulänglichkeiten

Energiewirtschaft und Telekombranche

Aggregationsrisiken, Vergleich zur Vorversion +1

17 Aggregationsrisiken:

- » Umgruppierung der Einzelrisiken
- » 1x Risiko höher
- » 1x geringer

15 Aggregationsrisiken:

- » Umgruppierungen
- » 5 geringer

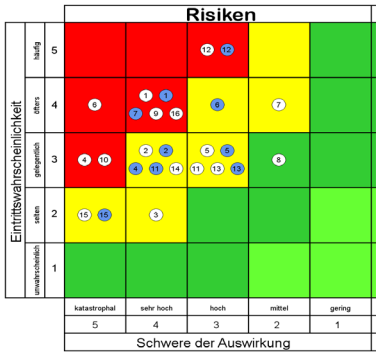


Abbildung 1: Aggregationsrisiken V3.0-2018

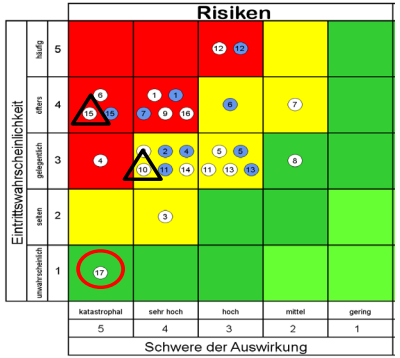


Abbildung 2: Aggregationsrisiken V4.0-2020

Neues Risiko Veränderte Risiken

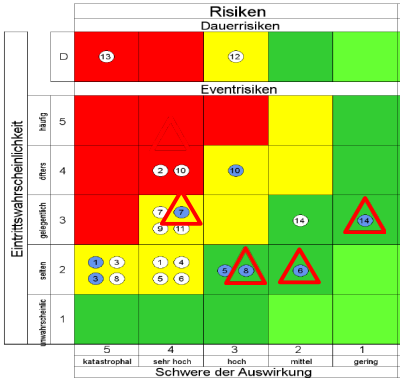


Abbildung 1: Aggregationsrisiken V2.0-2019

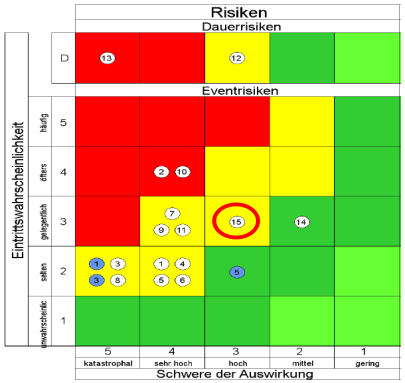


Abbildung 2: Aggregationsrisiken V3.0-2020

RELEASE TO PUBLIC

Agenda

1. **Status nascendi und die Genese in der E-Wirtschaft**
2. **Vorgehensmodell einmal anders**
3. **Angriffsformen bis hin zum APT**
4. **Heute die Zukunft denken**
5. **[Viribus unitis]**

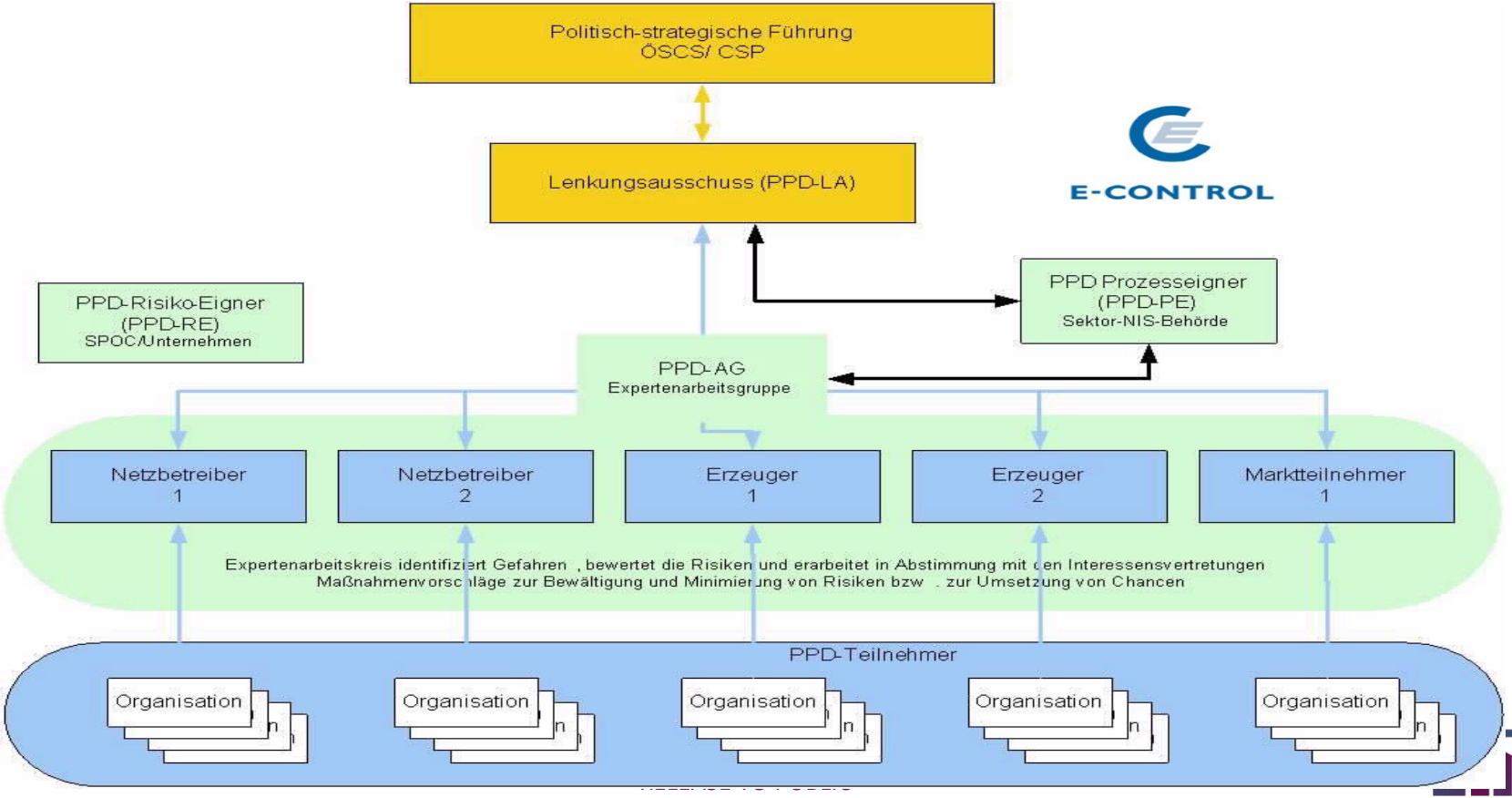
RELEASE TO PUBLIC

Vorzeigemodell PPP-Modell.at

- KI bzw. BWD-Betreiber der E-Wirtschaft (ALLE)
- SyS-relevante Betreiber
- Behörden
- Interessensvertretungen
- Hersteller, Lieferanten, Dienstleister

- Gemeinsam mit der Telekommunikationsbranche

PPP-Modell (e) Kommunikationsgeflecht(e)



Kernbotschaften

- 100 % gibt‘s nicht
- Wettrüsten
- ca. 50 wirklich Wissende E-Wirtschaft + Telekom
- Nat. / Int. Infoaustausch (AEC) + Hersteller
- Übungen / Simulationen
- Behörde Wirtschaft

Zusammenfassung

- Cybersicherheit ist eine der zukünftigen Herausforderungen
- Zusammenarbeit Behörde und Betreiber
- Internationale Vernetzung

Fragen ?