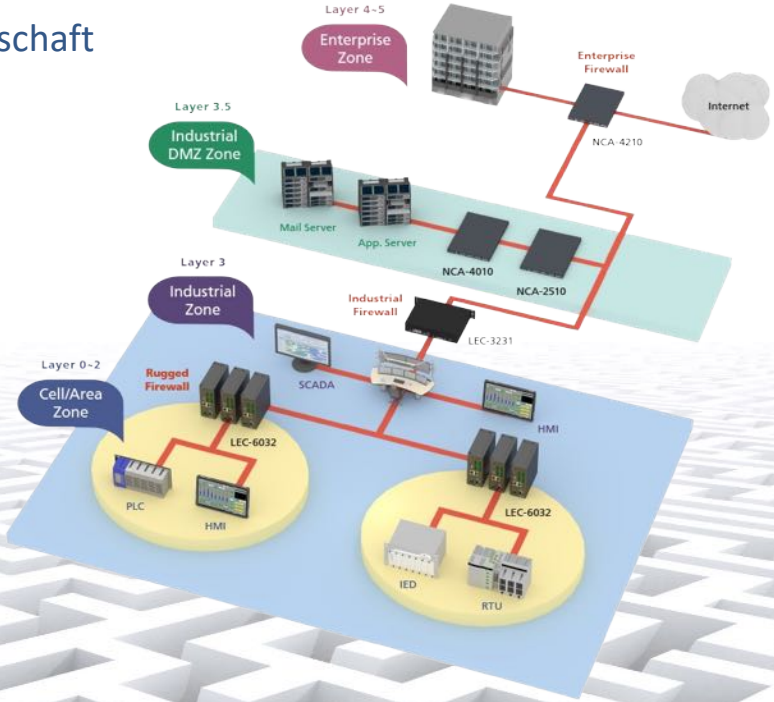
Die Vielfalt der aktuellen EU-Regulierung zur Cybersicherheit

Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
https://svs.informatik.uni-hamburg.de

Die Vielfalt der aktuellen EU-Regulierung zur Cybersicherheit

- Beispielhafte Bedrohungen aus dem Bereich Energiewirtschaft
- Aktuelle EU-Regulierungsansätze zur Cybersicherheit

Bildquelle: Canada.ca



Bildquelle: https://lannerinc.com/

Beispiel Energiewirtschaft: Bedrohungen in der Literatur

Bedrohung	Trend
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	unverändert
Infektion mit Schadsoftware über Internet und Intranet	stark gestiegen
Menschliches Fehlverhalten und Sabotage	unverändert
Kompromittierung von Extranet und Cloud-Komponenten	leicht gestiegen
Social Engineering und Phishing	unverändert
(D)DoS Angriffe	unverändert
Internet-verbundene Steuerungskomponenten	leicht gestiegen
Einbruch über Fernwartungszugänge	leicht gestiegen
Technisches Fehlverhalten und höhere Gewalt	unverändert
Soft- und Hardwareschwachstellen in der Lieferkette	stark gestiegen

BSI: Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen (2022)
[https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html]

Beispielhafte Angriffe aus dem Bereich Energiewirtschaft

- Bekannt gewordene Angriffe auf Unternehmen des Energiesektors der letzten Jahre
- Laut Kaspersky werden zwei Drittel der (überhaupt entdeckten) Sicherheitsvorfälle nicht gemeldet
- Hier lediglich eine Auswahl, nicht immer trennscharf

ICS-Malware	Ransomware	Supply-Chain-Angriffe
Angriffe auf Kommunikationswege & DDoS	Über das Internet erreichbare Steuersysteme	Insiderangriffe

[https://www.kaspersky.com/about/press-releases/2019_two-thirds-of-industrial-organizations-dont-report-cybersecurity-incidents-to-regulators]

ICS-Malware

Stuxnet (2010)

Havex (2013)

BlackEnergy 3 (2015)

Crash Override (2016)

Triton (2017)

- Hierbei handelt es sich um Schadsoftware, die sich explizit gegen industrielle Steueranlagen richtet.
- Erfordert im Normalfall vertieftes Angreiferwissen und lange Vorbereitung.

- Im Dezember 2015 wurde die Malware gegen drei ukrainische Energieversorger eingesetzt.
- Von **mehrstündigen Stromausfällen** waren über 200.000 Kunden betroffen.
- Angreifer hatten sich im Vorwege mittels **Social Engineering** Zugriff verschafft und über einen längeren Zeitraum in den Unternehmensnetzen verbreitet.
- Der letztliche Ausfall wurde durch **angepasste Firmware** für Steuerkomponenten hervorgerufen, die in das OT-Netz geschleust worden war.

Ransomware

Israel Electricity Authority
unbekannt (2016)

Kritische Infrastrukturen
WannaCry (2017)

Elexon (GB)
unbekannt (2020)

EDP (Portugal)
Ragnar-Locker (2020)

Colonial Pipeline
DarkSide (2021)

Nordex
Conti (2022)

- Ransomware verschlüsselt verfügbare Dateien und fordert Lösegeldzahlungen für die Entschlüsselung der Daten.
- Sie kann sich selbst auf weitere Systeme verbreiten.
- Teilweise werden die Dateien auch vor der Verschlüsselung entwendet und es wird mit Veröffentlichung gedroht.
- Diverse Ransomware/RaaS: CryptoLocker, Petya, Hive, BlackCat, …

- 2021 war die Betreibergesellschaft der **Colonial Pipeline** von der Ransomware DarkSide betroffen.
- Auch wenn die eigentliche Infrastruktur unversehrt blieb, so erfolgte doch eine **Einstellung des Betriebs**, da das Rechnungswesen betroffen war.

Supply-Chain-Angriffe

Havex (2013)

SolarWind (2020)

Viasat (2022)

- Bei Supply-Chain-Angriffen wird nicht das Zielunternehmen direkt angegriffen, sondern Dienstleister oder Zulieferer (Hardware oder Software), mit dem Ziel, indirekten Zugriff auf das Zielunternehmen zu erhalten.
- Potentiell können so viele Ziele gleichzeitig angegriffen werden.

- 2020 gelang es Angreifern, ein Softwareupdate einer Netzwerkmonitoring- und -managementsoftware der Firma **SolarWind** zu kompromittieren und eine Hintertür einzubauen.
- Dieses Update wurde von etwa **18.000 SolarWind-Kunden** (u.a. Behörden, Technologieformen, kritische Infrastrukturen) in den USA, Europa und Asien installiert.
- Die Folgen des Angriffs sind **bis heute schwer zu bewerten**. Ebenso ist unklar, ob die Angreifer immer noch Zugriff auf eine Vielzahl betroffener Systeme haben.

Angriffe auf Kommunikationswege & DDoS

50Hertz (2012)

Enercon/Viasat (2022)

- Anstatt Systeme anzugreifen, können ebenso Angriffe auf die Kommunikation zwischen Systemen zu Ausfällen des Gesamtsystems führen.
- Vergleichbar sind auch Distributed-Denial-of-Service-Angriffe, die Systeme mit einer zu großen Anzahl an Anfragen überlasten.

- 2022 wurde das Satellitennetz KA-SAT des Kommunikationsanbieters **Viasat** angegriffen, indem Modems des Satellitennetzes mit einer Wiper-Malware unbrauchbar gemacht worden waren.
- Durch den Ausfall des Kommunikationsnetzes verlor das deutsche Energieunternehmen Enercon für mehrere Tage die **Verbindung zu 5800 Windrädern**, sodass Monitoring und Fernwartung nicht mehr möglich war.

Über das Internet erreichbare Steuersysteme

Bowman dam (2013)

- Problematisch sind Kontrollsysteme, die direkt oder nur durch schwache Authentifizierungsmaßnahmen geschützt über das Internet erreichbar sind.
- Ein iranischer Angreifer verschaffte sich 2013 auf diese Weise Zugriff auf die **Steuerungssysteme des Bowman Dam** in den USA.
- Der Angreifer konnte lediglich **keinen Schaden** verursachen, da die physikalischen Steuerungskomponenten des Damms gerade gewartet wurden und von dem System getrennt waren.

Insiderangriffe

Kalifornischer Netzbetreiber (2007)

Texanisches Energieunternehmen (2009)

Kalifornisches Öl- und Gasunternehmen (2009)

- Dies beschreibt die Gefahr von gewollten oder ungewollten Datenleaks, Industriespionage, Sabotage, … durch Innentäter, die häufig in Sicherheitskonzepten missachtet werden.

- 2009 nutzte ein **entlassener Angestellter** eines texanischen Energieunternehmens nicht entzogene Zugriffsrechte dazu, sensible Unternehmensdaten zu extrahieren und und andere Daten zu verändern oder zu löschen.
- Einige der gelöschten Dateien waren für Betriebsabläufe in der Verwaltung zentral, deren Fehlen dem Unternehmen **Verluste auf dem Strommarkt** einbrachten.

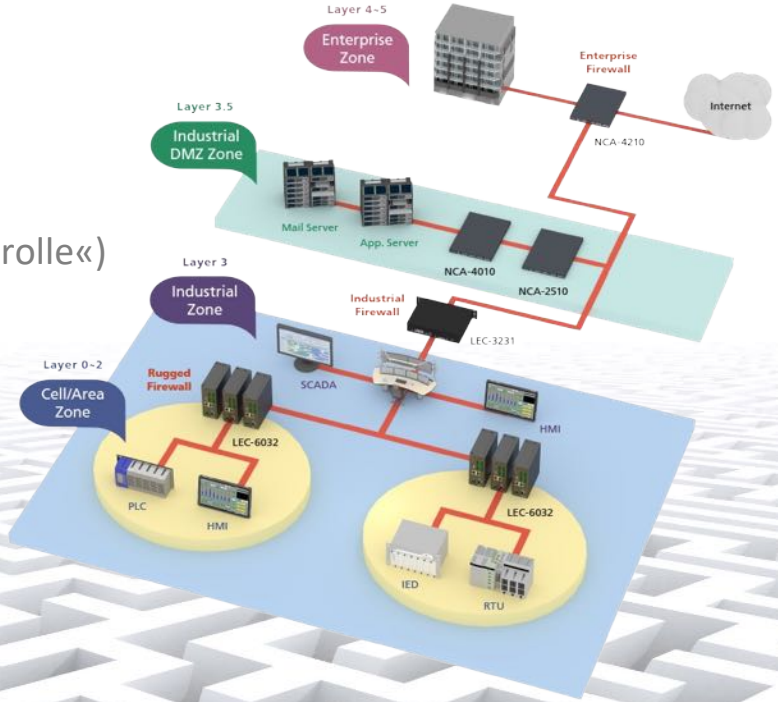
Zusammenfassung zu den wichtigsten Bedrohungen im Energiesektor

- Besonders relevante Bedrohungen
  - Ransomware
  - Supply-Chain-Angriffe
  - ICS-Malware
  - Keine konsequente Netztrennung, mit dem Internet verbundene Steuerungskomponenten
  - Veraltete Komponenten, lückenhaftes Patchmanagement
  - Innentäterangriffe
  - Fehlende Mitarbeiter-Awareness (Social Engineering, Phishing,...)
- ABER: Sicherer Betrieb erfordert eine Gesamtbetrachtung aller Systeme, Kommunikation und Akteure!

Aktuelle EU-Regulierungsansätze zur Cybersicherheit

Die Vielfalt der aktuellen EU-Regulierung zur Cybersicherheit

- Richtlinie zur Netz- und Informationssicherheit (NIS2)
- Cyber Solidarity Act
- Cyber Resilience Act (CRA)
- CER-Richtlinie (Critical Entities Resilience)
- …
- CSA (Prevent and Combat Child Sexual Abuse, »Chatkontrolle«)
- Artificial Intelligence Act (AI Act)
- Digital Services Act (DSA)



Bildquelle: https://lannerinc.com/

Richtlinie zur Netz- und Informationssicherheit (NIS2)

Vorschlag vom 14. Dezember 2022

- Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (EU 2022/2555) – aktualisiert die NIS-Richtlinie (2016/1148) aus 2016

NIS2
CSA
CRA
CER

- Ziel
  - Steigerung des allgemeinen Cybersicherheitsniveaus in der EU
  - Harmonisierung des Sicherheitsniveaus innerhalb der EU

- Adressaten
  - Unternehmen als Betreiber wesentlicher Dienste in den nachfolgend genannten Sektoren,
  - d.h. Betreiber kritischer Infrastrukturen,
  - aber auch Cloud-Dienste, Online-Shops, Suchmaschinen, Social Media

Richtlinie zur Netz- und Informationssicherheit (NIS2)

- Anwendungsbereich bisher:
  - Energiewirtschaft
  - Transportwesen
  - Bankwesen und Finanzmärkte
  - Gesundheit
  - Trinkwasserversorgung
  - Digitale Infrastruktur und Service Provider

- Erweiterter Anwendungsbereich: zusätzlich
  - Abwasserwirtschaft
  - Hersteller wichtiger Zwischenprodukte (z.B. chemische Substanzen für Medikamente)
  - Nahrungsmittelwirtschaft
  - Luft- und Raumfahrt
  - Post- und Telekommunikation
  - Öffentliche Verwaltung
  - Forschung

NIS2
CSA
CRA
CER

Richtlinie zur Netz- und Informationssicherheit (NIS2)

- Methoden
  - Definition von Schwellenwerten für die Sektoren
  - Ergreifen von geeigneten Sicherheitsmaßnahmen
  - Verpflichtung der Behörden zur Unterrichtung über schwerwiegende Vorkommnisse

- Maßnahmen
  - Aufbau von Computer Security Incident Response Teams (CSIRT)
  - Aufbau einer nationalen Netz- und Informationssystembehörde (NIS)
  - Aufbau einer Kooperationsplattform zum Informationsaustausch zwischen den EU-Mitgliedsländern
  - Aufbau einer sektorübergreifenden Sicherheitskultur

NIS2
CSA
CRA
CER

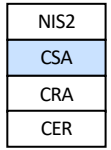
Cyber Solidarity Act

Vorschlag vom 18. April 2023

- Ziel
  - Prävention, Erkennung und Reaktion auf Cyber-Sicherheitsvorfälle verbessern

- Vorgehen
  - Aufbau von sog. Security Operations Centres (SOCs) innerhalb der EU-Mitgliedsländer
  - Zusammenfassung der SOCs in länderübergreifenden SOC-Plattformen

- Etabliert werden sollen
  - Cybersecurity Emergency Mechanism
  - Cybersecurity Incident Review Mechanism



Cyber Resilience Act (CRA)

Vorschlag vom 15. September 2022

- Ziel
  - Cybersicherheit für den gesamten Produktlebenszyklus
  - definiert Sicherheitsanforderungen für Produkte mit sog. digitalen Elementen
  - digitale Elemente: Hardware und Software

NIS2
CSA
CRA
CER

- Methoden
  - Schwachstellen-Management, Update-Management
  - Updates für die gesamte Laufzeit eines Produkts
- Fokus
  - private digitale Geräte wie Computer, Handys, Router, IoT-Devices, smarte Haushaltsgeräte, smartes Spielzeug, aber auch Industrial IoT

- Befürchtung: Entwicklung freier Software bedroht
  - Offener Brief der Open-Source-Community: «die Entwicklung und globale Bedeutung neuer Open-Source-Software stark eingeschränkt»

Cyber Resilience Act (CRA)

- Classification of Critical products with digital elements (CRA Art. 6, Annex III)
  - Critical Products with Digital Elements
    - CRA Art. 3: »a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(2) and whose core functionality is set out in Annex III«
  - Highly Critical Products with Digital Elements
    - CRA Art. 3: »a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(5)«

- Querbezüge zu NIS2 (Annex III) und High-Risk AI Systems (CRA Art. 8)

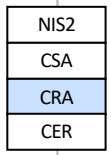
Class 1

- Identity management systems
- Password managers
- Mobile device management software
- Firewalls, Routers, Microcontrollers
- Field-programmable gate arrays (FPGA)
- Supervisory Control And Data Acquisition Systems (SCADA)
- …

Class 2

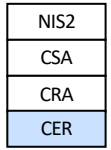
- Operating systems for servers, desktops, and mobile devices
- Hypervisors and container systems
- Public Key Infrastructure (PKI)
- Hardware Security Modules (HSMs)
- Secure Cryptoprocessors
- Smartcards
- Smart Meters
- …

Annex III



CER-Richtlinie (Critical Entities Resilience)

- löst die European Critical Infrastructures Direktive von 2008 ab
- Umsetzung in nationales Recht bis 2024 – geplant in einem KRITIS-Dachgesetz



- Ziel
  - bessere Resilienz bei kritischen Infrastrukturen
  - recht strenge Meldepflichten (innerhalb von 24 Stunden) nach einem Vorfall

- Critical Entities = unter RCE regulierte Unternehmen
  - RCE reguliert Critical Entities in elf Sektoren, die sog. Essential Services erbringen
  - mit Sektoren aus NIS 2 (Annex I) fast deckungsgleich
  - KRITIS-Sektoren aus BSI-Gesetz (BSI-KritisV) sind allerdings etwas umfassender

https://www.kritis.bund.de

Sieben Sektoren kritischer Infrastrukturen nach BSI-KritisV

- Energie:
  - Elektrizität (≥420 MW), Gas, Kraftstoff und Heizöl, Fernwärme (≥2300 GWh/Jahr)
- Gesundheit:
  - medizinische Versorgung/Krankenhäuser (≥30.000 vollstationäre Fälle/Jahr), unmittelbar lebenserhaltende Medizinprodukte, verschreibungspflichtige Arzneimittel und Blut- und Plasmakonzentrate, Laboriumsdiagnostik (≥1,5 Mio. Aufträge/Jahr)
- Informationstechnik und Telekommunikation:
  - Zugangs-, Übertragungsnetze (≥100.000 Anschlüsse), DNS-Resolver, Rechenzentren, Content Delivery Networks (≥75.000 TByte/Jahr), Certificate Authorities

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)

https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf

https://www.kritis.bund.de

Sieben Sektoren kritischer Infrastrukturen nach BSI-KritisV

- Transport und Verkehr:
  - Personen- und Güterverkehr, Luftverkehr, Schienenverkehr, Binnen- und Seeschifffahrt, Straßenverkehr, öffentlicher Personennahverkehr (≥125 Mio. Fahrgäste/Jahr), Logistik
- Wasser:
  - Trinkwasserversorgung, Abwasserbeseitigung
- Finanz- und Versicherungswesen:
  - Bargeldversorgung (≥15 Mio. Transaktionen/Jahr), kartengestützter (≥21,5 Mio. Transaktionen/Jahr) und konventioneller Zahlungsverkehr, Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften, Versicherungsdienstleistungen
- Ernährung:
  - Lebensmittelproduktion,-verarbeitung, -handel

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)

https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf

CER-Richtlinie (Critical Entities Resilience)

- Wesentliche Maßnahme: Erstellung eines sog. Resilienz-Plans
  - Risiko-Bewertung: Ausfallrisiken identifizieren und bewerten
  - Allgemeine Präventionsmaßnahmen gegen Sicherheitsvorfälle
  - Physische Sicherheitsmaßnahmen: Perimeterschutz, Zutrittskontrolle
  - Risiko- und Krisenmanagement
  - Business Continuity Management (BCM)
  - Personell Security
  - Awareness-Maßnahmen

NIS2
CSA
CRA
CER

- enge Bezüge zu ISO 27001/27002

2013

Security Policy
Organization of Information Security
Human Resources Security
Asset Management
Access Control
Cryptography
Physical and Environmental Security
Operations security
Communications Security
Information Systems Acquisition, Development, Maintenance
Supplier Relationships
Information Security Incident Management
Information Security Aspects of Business Continuity
Compliance

2022

Organizational controls (37 Maßnahmen)
People controls (8 Maßnahmen)
Physical controls (14 Maßnahmen)
Technological controls (34 Maßnahmen)

Fazit

- Unübersichtlichkeit der EU Gesetzgebung
- Wünschenswert: Systematik der Gesetzgebungsvorhaben

- Schutz
  - der Verbraucher
  - der Unternehmen
  - der kritischen Infrastruktur
  - des Staats

- Spannungsfelder
  - Technologische Souveränität vs. Kosten der Sicherheit
  - Schutz von Bürgerrechten vs. Terror- und Kriminalitätsbekämpfung
  - Cybersecurity (zwischenstaatliche Auseinandersetzungen)