Resiliente Betriebsführung und IKT-Sicherheit

Breakout-Session TV 2.2 (ResIKT)

Tom Petersen, Joshua Stock
Sicherheit in verteilten Systemen (SVS)
https://svs.informatik.uni-hamburg.de

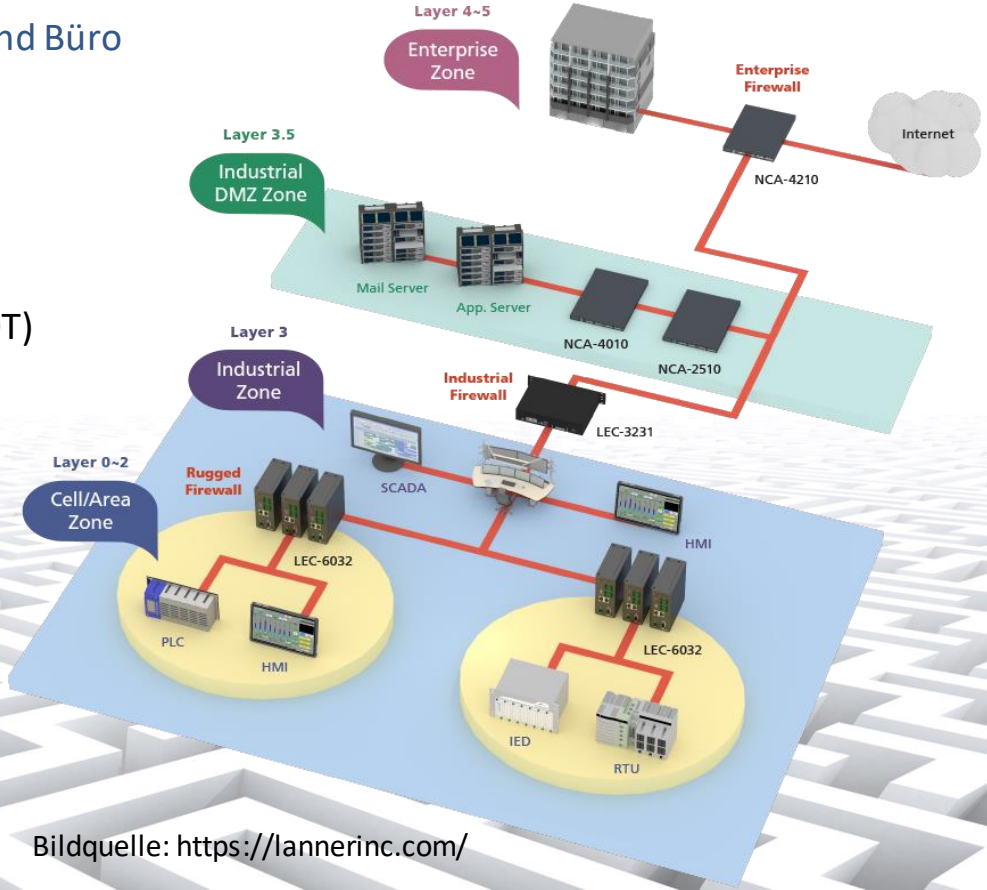
Bildquelle: Canada.ca

Einstieg

- Zunehmend digitale Prozesse
  - Sektorenkopplung: auch über Unternehmensgrenzen hinweg
- TV 2.2: IKT-Sicherheit im Energiesektor
  - Sinnvolle und bedarfsgerechte Bausteine
- Immer häufiger: Spezialisierte Angriffe auf Unternehmen, öffentliche Einrichtungen, Hochschulen,…
- Agenda heute:
  - Übersicht IT-/OT-Netze
  - Angriffe auf Energieinfrastruktur
  - Ergebnisse Interviews im NRL-Konsortium
  - Zusammenfassung von Bedrohungen und Maßnahmen
  - Diskussion

Abstrakte Übersicht: IT-/OT-Infrastruktur

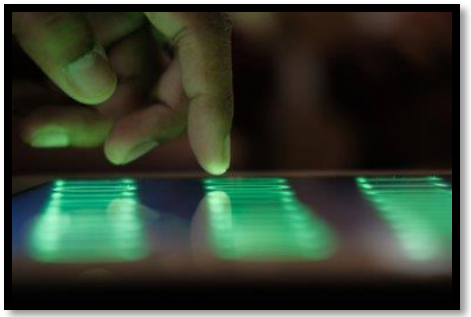
- Energieunternehmen mit Anlagen, Leitstelle und Büro
- Größtes Einfallstor: Internet
- Zwei Netzbereiche
  - Digitale Anlagensteuerung mit Leitstelle (OT)
  - Davon getrennt: Büro mit IT und Internet



Bildquelle: https://lannerinc.com/

Angriffe

- 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.

Angriffe

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

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 Authentifiezierungsmaßnahmen 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.

Über das Internet erreichbare Steuersysteme

Bowman dam (2013)

Angreifer nehmen Industriesteuerungen im Internet aufs Korn

Das US-CERT warnt davor, dass Angreifer die spezielle Suchmaschine Shodan zum Aufspüren verwundbarer Überwachungssysteme (SCADA) für Industriesteuerungen benutzen.

03.11.2010 11:45 Uhr | Security

Über das Internet erreichbare Steuersysteme

Bowman dam (2013)

Angreifer nehmen Industriesteuerungen im Internet aufs Korn

Das US-CER
zum Aufspü
Industrieste

03.11.2010 1

VNC-Roulette – was wollen Sie fernsteuern?

Ein Sicherheitsproblem, das es eigentlich nicht geben sollte und trotzdem: Industrielle Steurungssysteme, Linux-Desktops, Spammer auf Facebook – es gibt fast nichts, was man nicht entdecken kann, wenn man einfach nach offenen VNC-Servern sucht.

01.04.2016 07:00 Uhr | Security

Über das Internet erreichbare Steuersysteme

Bowman dam (2013)

Angreifer nehmen Industriesteuerungen im Internet aufs Korn

Das US-CER
zum Aufspü
Industrieste

03.11.2010 1

VNC-Roulette – was wollen Sie fernsteuern?

Ein Sicherheitsproblem, das es eigentlich nicht geben sollte und trotzdem:
Industrielle Steu
fast nichts, was
Servern sucht.

01.04.2016 07:00 U

IT-Security-Anfängerfehler gefährden Stromver- und Abwasserentsorgung

Angreifer könnten unter anderem Steuerungssysteme in kritischen Infrastrukturen mit Schadcode attackieren.

21.06.2022 10:20 Uhr | Security

Über das Internet erreichbare Steuersysteme

Bowman dam (2013)

Angreifer nehmen Industriesteuerungen im Internet aufs Korn

Das US-CER
zum Aufspü
Industrieste

03.11.2010 1

VNC-Roulette – was wollen Sie fernsteuern?

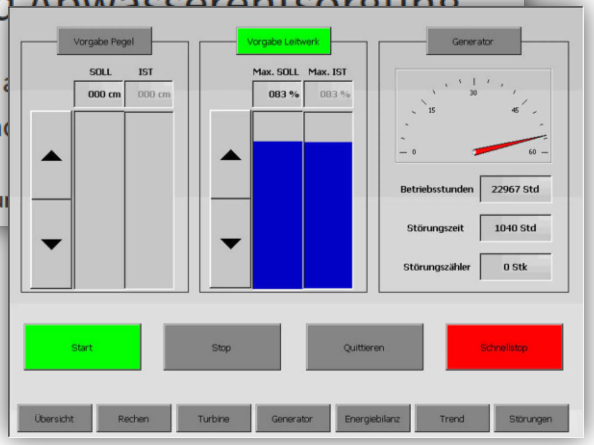
Ein Sicherheitsproblem, das es eigentlich nicht geben sollte und trotzdem:
Industrielle Steu
fast nichts, was
Servern sucht.

01.04.2016 07:00 U

IT-Security-Anfängerfehler gefährden Stromver- und Abwasserentsorgung

Angreifer könnten unter a
Infrastrukturen mit Schad

21.06.2022 10:20 Uhr | Secu



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.

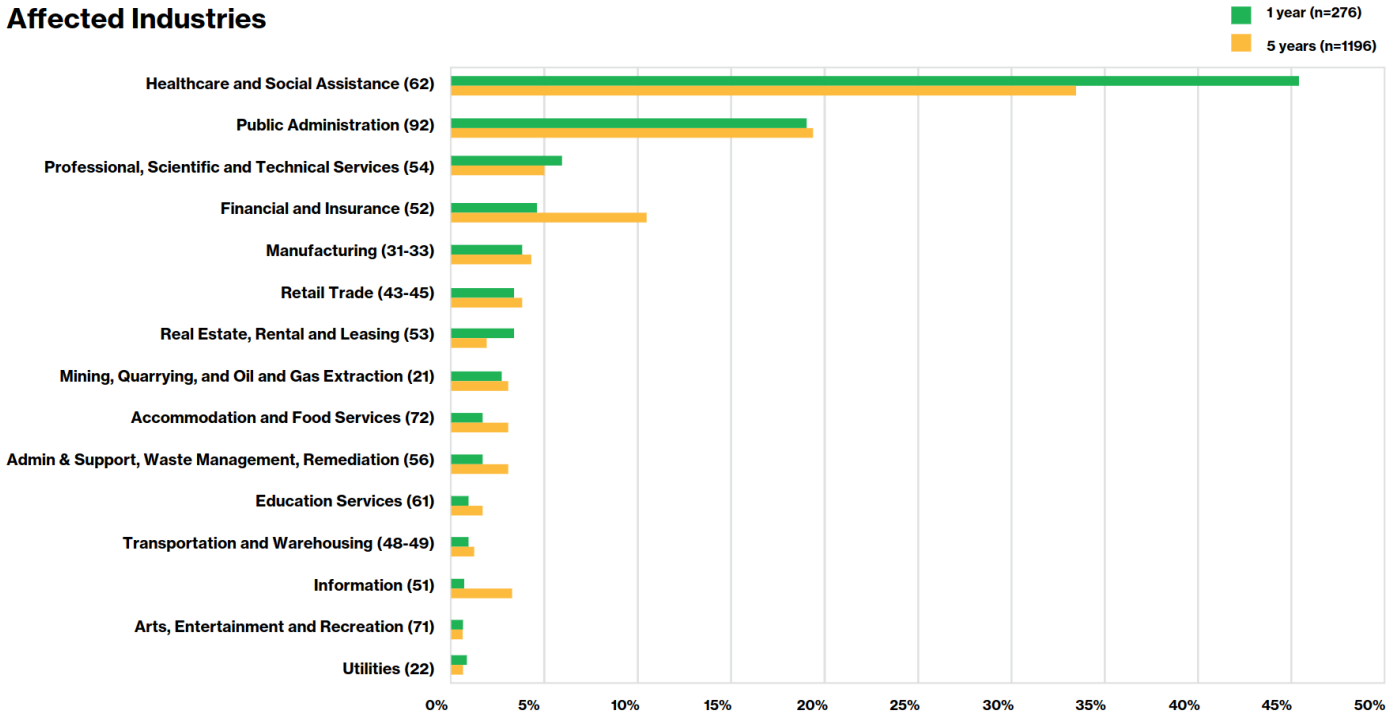
- 2009 nutzte ein **entlassener Angestellter** eines texanischen Energieunternehmens nicht entzogene Zugriffsrechte dazu, sensible Unternehmensdaten zu extrahieren und und andere Daten zu verändern oder zu löschen.
- Einige der gelöschten Dateien waren für Betriebsabläufe in der Verwaltung zentral, deren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

Insiderangriffe

Kalifornischer Netzbetreiber (2007)

Texanisches Energieunternehmen (2009)

Kalifornisches Öl- und Gasunternehmen (2009)



Verizon: Insider Threat Report (2019) [https://www.verizon.com/business/resources/reports/insider-threat-report.pdf]

Interviews mit Partnern aus dem NRL-Konsortium

- Fünf Interviews im Sommer/Herbst 2022

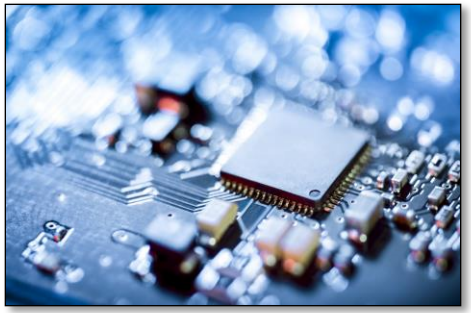
- Ziel: Überblick
  - IT- und OT-Infrastruktur
  - IKT-Sicherheitsherausforderungen
  - Organisationsübergreifende Kommunikation (Sektorenkopplung)

- Diverses Unternehmensspektrum
  - Anlagentypen
  - Unternehmensgröße
  - Erfahrungen: von kürzlich erfolgtem Ransomware-Angriff bis wenig Berührungspunkte

Erkenntnisse aus Interviews I

- Trennung von Netzen
  - IT-Netz/Büroinfrastruktur mit Internet verbunden
  - Davon unabhängig: OT-Netz mit sicherheitskritischen Anlagen
- Fernsteuerungsmöglichkeiten von Anlagen
  - Potenziell (ggf. unnötiges) Einfallstor für Angriffe
  - Maximale Schutzmaßnahmen erforderlich
    - VPN, 2-Faktor-Authentifizierung, sichere Passwörter, 4-Augen-Prinzip, …
- Physische Sicherheit: Konsequente Umsetzung von Sicherheitsrichtlinien
  - Auch mit Verkleidung (Blaumann, Leiter, Werkzeugkoffer, …)
  - Social Engineering

Erkenntnisse aus Interviews II



- Awareness-Schulungen von Mitarbeitenden
  - Schutznotwendigkeit
  - Vielfalt von Angriffsmöglichkeiten

- Aktuelle Softwareversionen: konsequentes Patchmanagement
  - Austausch von veralteten, nicht-updatebaren OT-Komponenten
  - Herstellerbezogene Leistung, kein Zugriff vs. eigenhändiges Einspielen von Updates

- Authentifizierung anderer Organisationen
  - über „an der Stimme erkennen“ am Telefon hinaus

Erkenntnisse aus Interviews III

- Redundante Kommunikationswege
  - Kommunikation auch bei Ausfall von/Angriff auf primäre Infrastruktur
    - Mit Anlagen und anderen relevanten Akteuren
    - Innerhalb und außerhalb eigenen Unternehmens

- Vorsicht bei Lieferketten
  - Aufträge an Dritte mit Zugriff auf IT-/OT-Netze
  - Übersicht über IKT-Sicherheitsmaßnahmen?
  - Potenzielles Einfallstor für Angriffe

- Informationen über Schwachstellen
  - Austausch ist essenziell
  - Sehr unterschiedliche Handhabung

Ergebnisse Literaturrecherche

- NESCOR: **Electric Sector Failure Scenarios and Impact Analyses** (2015)
  - 129 konkrete Bedrohungsszenarien in 8 Kategorien (u. a. Energieerzeugung)
- Dax et al.: **Stand zur IT-Sicherheit deutscher Stromnetzbetreiber** (2016)
  - Befragung deutscher Stromnetzbetreiber zum Stand der IT-Sicherheit
- Fischer et al.: **Evaluation of risks of cyber-incidents and on costs of preventing cyber-incidents in the energy sector** (2018)
  - Bedrohungen, Maßnahmen, Wirtschaftlichkeit für IT/OT-Sicherheit im europäischen Raum
- Canadian Centre for Cyber Security: **Cyber threat bulletin: The cyber threat to Canada's electricity sector** (2020)
  - Untersuchung von Bedrohungen für den kanadischen Energie-Sektor
- BSI: **Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen** (2022)

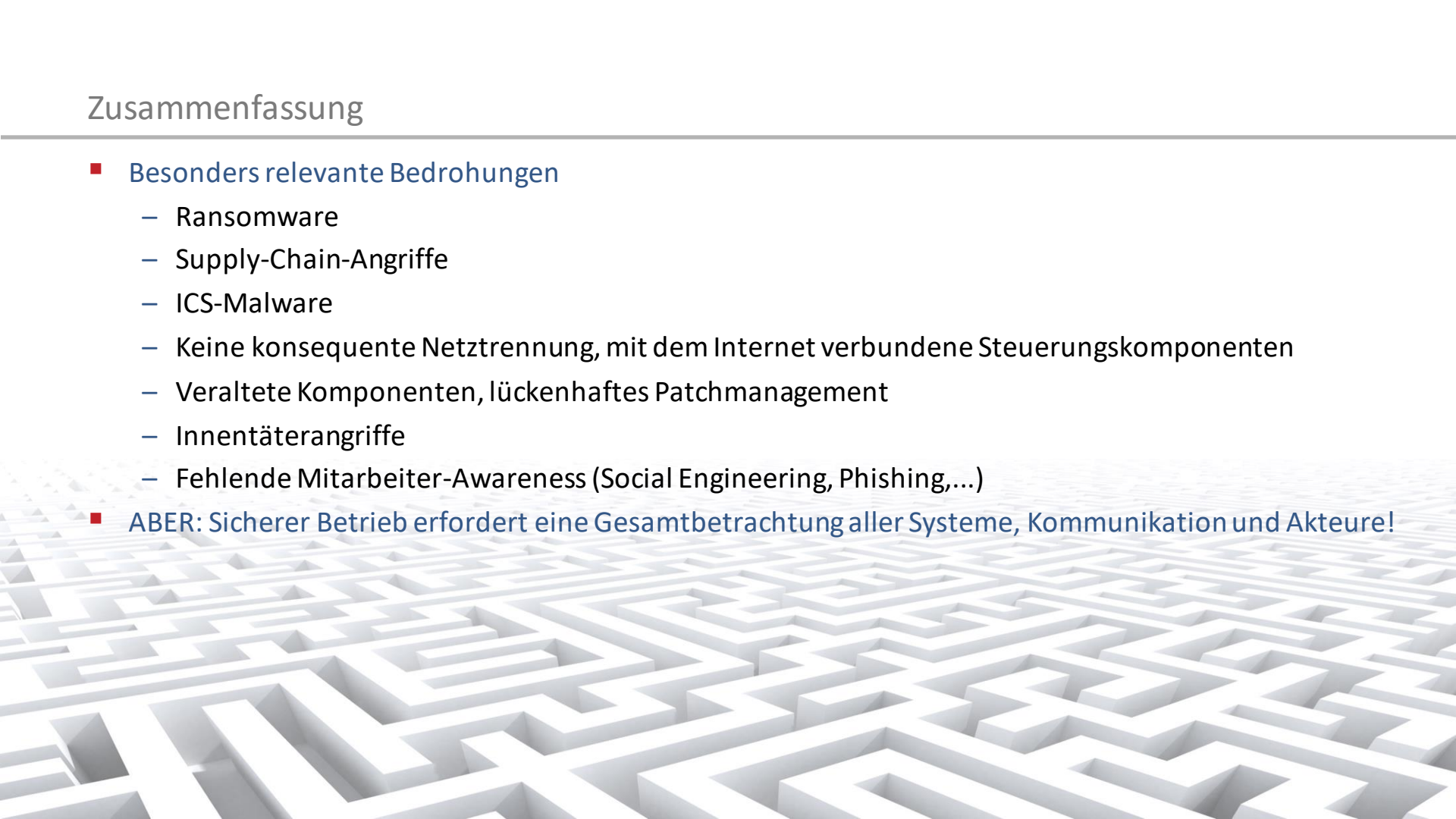
Ergebnisse Literaturrecherche

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]

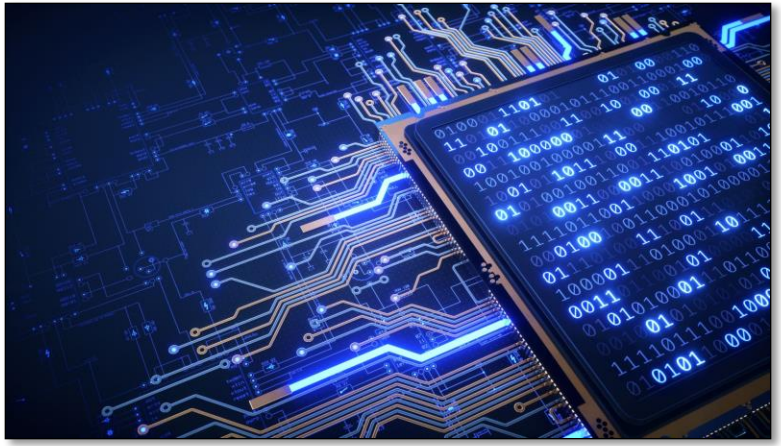
Zusammenfassung

- 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!



Werbung in eigener Sache

- Das BMWK etabliert mit der dena (Deutsche Energie-Agentur) eine "**Branchenplattform Cybersicherheit für die Stromwirtschaft**".
- TN der Branchenplattform sind **Akteure der Strom- und Digitalwirtschaft**. Besonderes, aber nicht ausschließliches Augenmerk liegt auf Akteuren, die nicht unter die KRITIS-Verordnung fallen.
- Die Plattform soll diesbezüglich wichtige **Bedarfe der Akteure** an die Politik adressieren.



- Dazu sollen in einem ersten Schritt relevante Themen unter den verschiedenen Teilnehmergruppen identifiziert werden. Grundlage dafür ist eine **Umfrage**, an der sich möglichst viele Akteure der Strom- und Digitalwirtschaft beteiligen sollen. Sie wird voraussichtlich **Mitte Mai** verschickt.
- Die Umfrage besteht aus **Thesen zur Cybersicherheit in der Stromwirtschaft**, die die Teilnehmenden bewerten sollen.

Thesen & Diskussion

- Wie findet Vernetzung über IKT-Sicherheit statt?
  - z.B. UP KRITIS (*Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen in Deutschland*)

- Welche Trends sind im Energiesektor zu beobachten und wie wirkt sich das aus ihrer Sicht auf die Bedrohungslage aus?

- Eigene Erfahrungen, Ergänzungen, Fragen?