Cybersicherheit und Resilienz im Stromnetzbetrieb – Stand und Entwicklung aus Sicht eines Verteil- und Flächennetzbetreibers

VDE SYMPOSIUM Region Ost-Mitte

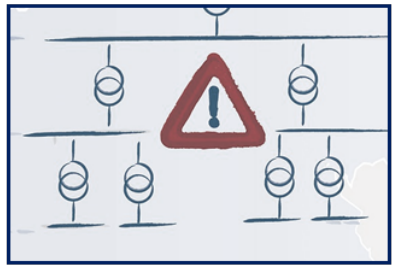
Erfurt, den 01. Dezember 2022

Dr.-Ing. Michael Agsten
Dr.-Ing. Christoph Brosinsky
Netzführung TEN Thüringer Energienetze GmbH & Co. KG

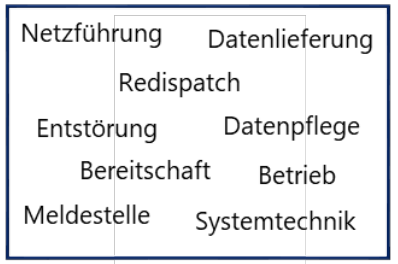
Thüringer Energienetze

Zielbild der OT Infrastruktur der TEN: dauerhaft / permanent verfügbare Beobachtbarkeit & Steuerbarkeit der Energienetze als Teil des Rückgrats der Energieversorgung Thüringens

4,3 GW Erzeugung in Thüringen



Kaskade & Redispatch



Dienstleistungen

Mehrspartensysteme

Intelligente digitale standardisierte Leitsystem- & Sekundärtechnik "DSO 2.0"

24/7

99,9 % Verfügbarkeit

ISMS, ITSK, 27019 TR

Skalierbarkeit

Verarbeitung Massendaten

Thüringer Energienetze

Krisenauswirkungen auf die Energieversorgungssicherheit sind **nicht** begrenzt auf die IT/OT Sicherheit

- **IT/OT Sicherheit**
  - erfolgreiche Hackerangriffe in der Business-IT, vorwiegend Ransomware (bspw. TÜV Thüringen, BTC AG, ENTEGA, KISTERS, Wilken, etc..)
  - → Prozess-IT (PIT) bisher nicht betroffen
  - → **aber:** mit Industroyer (2016 Ukraine), Stuxnet (2010 Iran) existieren Verfahren, um OT Systeme zu kompromittieren und PIT Systeme anzugreifen
  - **Beispiel 2022:** KA-SAT Störung, die sich auf ca. 5.800 Enercon Anlagen (in Summe ca. 10 GW) ausgewirkt hat

- **Physische Sicherheit**
  - Einbrüche und Angriffe auf KRITIS Infrastrukturen deutschlandweit
  - TEN verzeichnet ebenso einen Anstieg an erfolgreichen Einbrüchen in unbesetzte Standorte
    → jedes Mal zu bewerten: handelt es sich um Diebstahl oder Versuch Angriff auf IT Systeme aus dem UW heraus?
  - **Beispiel 2022:** 08. Oktober 2022 Sabotage Kommunikationskabeln der deutschen Bahn, Folge: großflächige Unterbrechung des Bahnverkehrs
  - **Beispiel 2022:** mehrere Einbrüche in Umspannwerke in der Uckermark

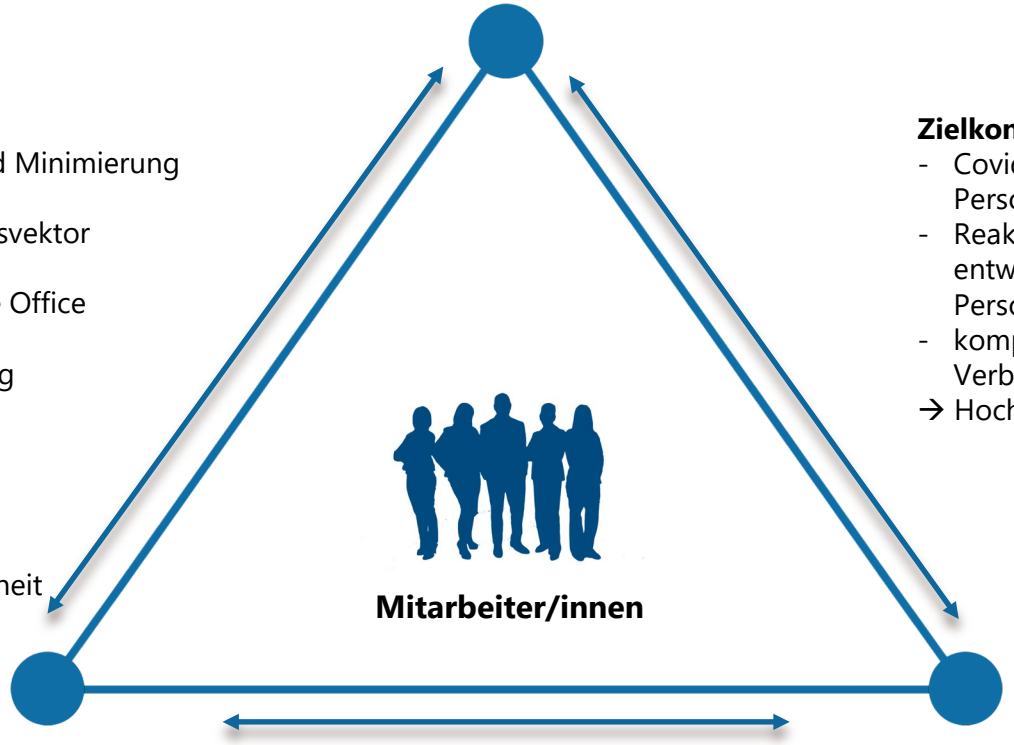
- **Personal**
  - Personalknappheit hat sich verschärft (Demographie + fehlender Nachwuchs) → Know-How Verlust
  - Erhöhte Anfälligkeit für Erkrankungen (Pandemie & derzeit stärker auftretende saisonale Erkrankungen bspw. Grippe)
  - Bewerbungssituation
    - nahezu keine Bewerbungen
    - fachlich selten geeignet
    - nicht greifbare Risiken bei Migrationshintergründen aus Krisengebieten bzw. Embargoländern
    - → die Grundlage für die Aufrechterhaltung der Informationssicherheit / IT Sicherheit wird auch im Recruitingprozess langfristig gelegt
  - aktives Recruiting anderer Unternehmen entzieht Know-How Träger → damit verschärft sich die Personalsituation / gerade auch im OT/IT Bereich

Thüringer Energienetze

Das Management der Krisen & die sich entwickelnden Bedrohungslagen verursachen Zielkonflikte, die tlw. tagesaktuell neu bewertet und priorisiert werden müssen.

Pandemie Covid19

Ziel: *Betriebsfähigkeit 24/7 Beobachtung und Steuerung aufrecht erhalten und ggf. mit Minimalbesetzung in Kasernierung tätig*



Zielkonflikt: Cybersecurity vs. Pandemie

- Home Office zur Beherrschung der Pandemie und Minimierung des gleichzeitigen Ausfalls vieler Mitarbeiter
- Home Office ist hingegen ein zusätzlicher Angriffsvektor für Cybersecuritybedrohungen
- bestimmte Tätigkeiten lassen sich aus dem Home Office nicht erledigen

→ Vielzahl kompensierender Maßnahmen notwendig

- weiterhin Maskenpflicht
- Mitarbeiterschulungen
- Derzeit max. 2d Home Office
- Abstandsreglungen
- Schulungen & Sensibilisierung zur
- Aufrechterhaltung der Informationssicherheit

Zielkonflikt: Energiemangelkrisen vs. Pandemie

- Covid19 Pandemie führt weiterhin zu fluktuierende Personalausfällen (Erkrankung od. Quarantänefestlegungen)
- Reaktionsschemen auf die seit dem 24.02.2022 sich damals **neu** entwickelnde Krise erforderten Priorisierung der verfügbaren Personalressourcen
- komplett neue Prozesse wurden durch den Gesetzgeber und die Verbände im Wochentakt organsiert

→ Hochdynamische Phase

Cybersecurity

Ziel: *Informationssicherheit, Handlungsfähigkeit, 24/7 Beobachtung und Steuerung aufrecht erhalten, Netzstabilität ist nur mit dem Leitsystem aufrecht zu erhalten*

Zielkonflikt: Cybersecurity vs. Energiemangellagen

- Mitarbeiteressourcen & Fokussierung
- beide Themen forderten und fordern weiterhin eine hohe Aufmerksamkeit und entwickeln sich hochdynamisch

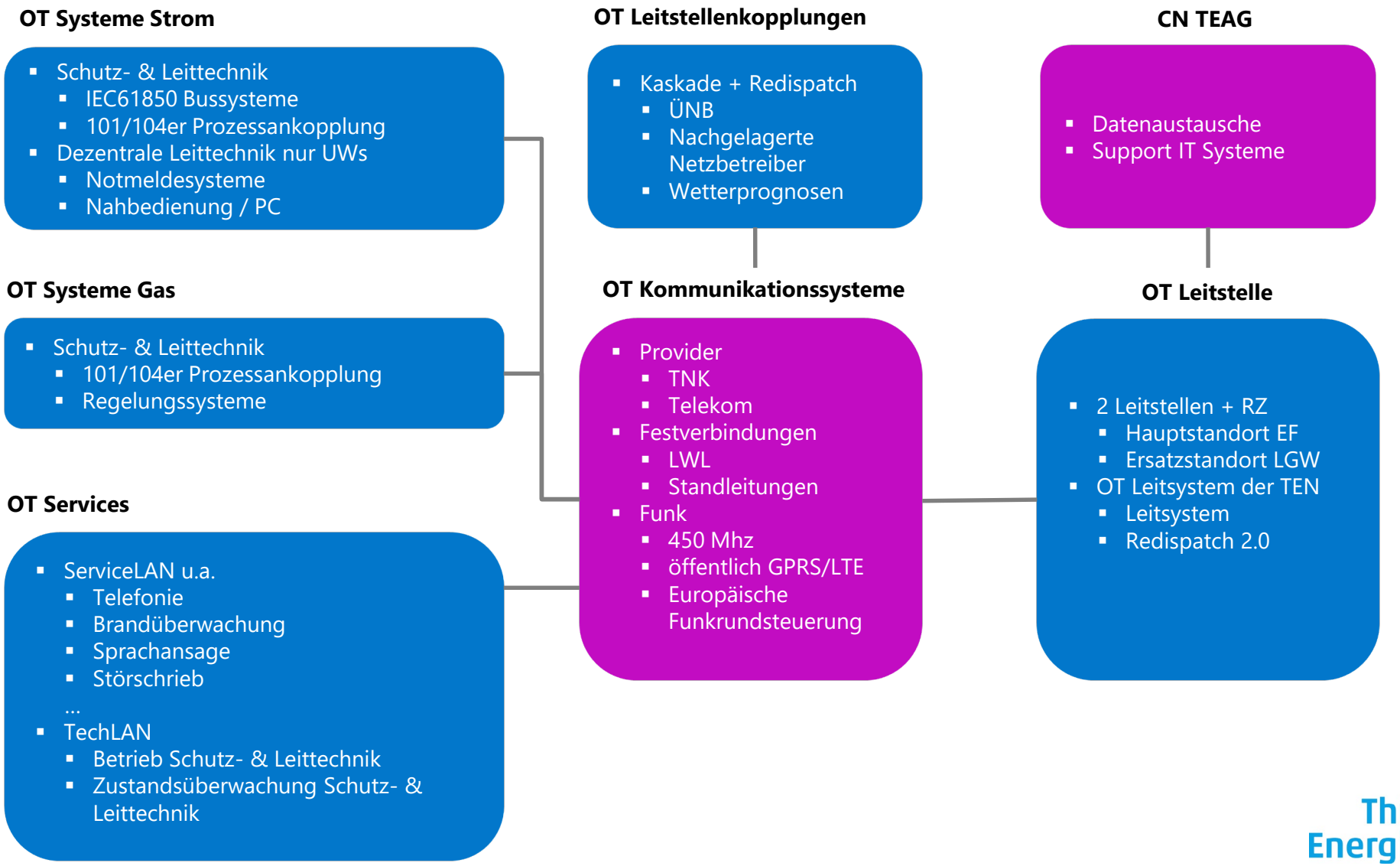
Energiemangellagen Gas & Strom

Ziel: *stabiler Systembetrieb bei Gas- und Strommangel*

→ *Krisenorganisation / in 2022 deutlicher Mehraufwand der MAK zur Beherrschung dieser Situation*

Thüringer Energienetze

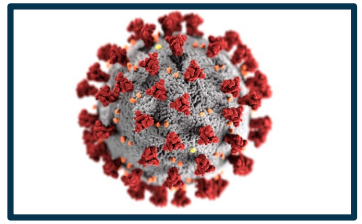
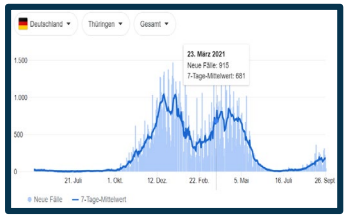
Auszug der Systeme der OT, die für einen sicheren Netzbetrieb notwendig sind



Tagesgeschäft Risikomanagement

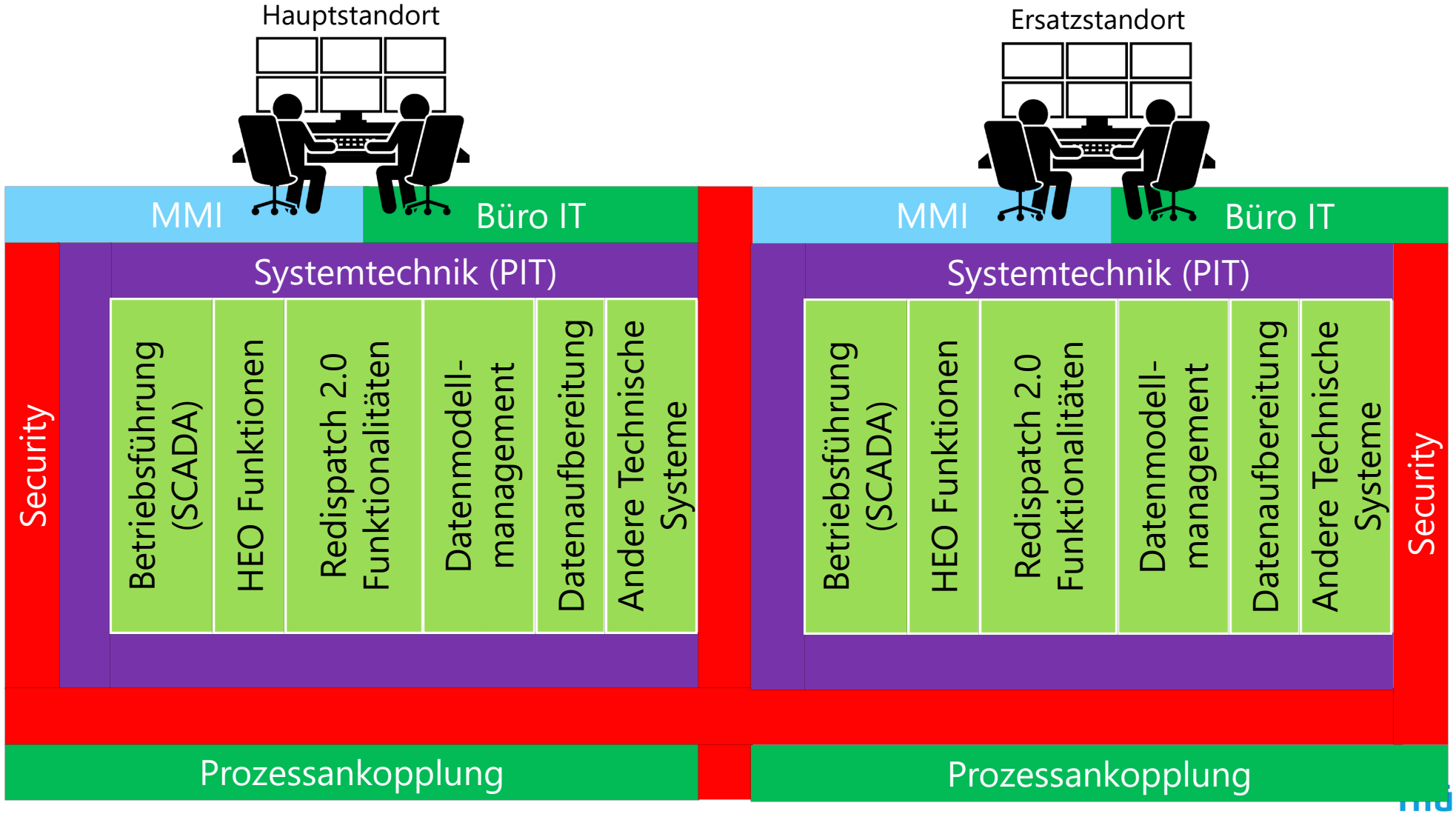
Nichts ist so stetig wie die Veränderung!!

Prozess des Risikomanagement

Bedrohung / Schwachstelle	Einschätzung Schaden & Ereigniswahrscheinlichkeit	Ableitung Risiko - rot - grün - gelb	Identifikation Maßnahmen - Vermeidung - Verminderung - Mitigation - Risiko tragen	Restrisiko
		hoch	▪ Impfung ▪ Maske tragen ▪ Home Office ▪ Zweileitstellenbetrieb ▪ dauerhaftes Hygiene- & Gesundheitsmanagement	mäßig
	▪ Assetregister ▪ Schwachstellen-management ▪ tagesaktuelle IT Bedrohungslage ▪ BSI Meldungen	hoch	▪ Patchen ▪ IT Security Regelwerke ▪ Schulungen ▪ Human Firewall	mäßig
	▪ Szenarioerstellung- und Management ▪ Regelmäßige Aktualisierung ▪ Bewertung Klimawandel ▪ Business Impact Analysen	kritisch	▪ Notfallpläne ▪ Redundanzen ▪ ggf. technische und organisatorische Anpassungen	mäßig
		kritisch		mäßig
		hoch		mäßig
		mäßig		mäßig
		mäßig		mäßig
		mäßig		mäßig
		mäßig		mäßig
		mäßig		mäßig
		mäßig		mäßig
		mäßig		mäßig

Thüringer Energienetze

Zwei-Standort Betrieb in gehärteten Rechenzentren



Strategische Maßnahmen Aufrechterhaltung der OT Sicherheit

Zero Trust Strategie OT in Umsetzung für alle OT Systeme

- Zugang, Zutritt und Zugriff je Anwendungsfall
  - minimalisiert
  - personalisiert
  - zeitlich begrenzt

- vorhandene Zero Trust Strategie gg. externen Schnittstellen
  - Fernwartung
  - Datenaustauschen im Rahmen Dienstleistungen & Projekten
  - Anwendung in der Netzführungsdienstleistung (bspw. abgesetzte Arbeitsplätze)

- Umsetzung Zero Trust Strategie gg. allen internen Schnittstellen in der TEAG Gruppe
  - innerhalb der TEN
  - Informations- und Datenaustauschen OT/IT
  - Informations- und Datenaustauschen OT/Kommunikationstechnik

Monitoring & Reaktionsmanagement OT in Umsetzung

- Security Information and Event Management (SIEM) / Security Operations Center (SOC)
- Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS) in Firewalls
- flächendeckende Anomalieerkennung
- spezialisierte Anomaliererkennung in neuen Umspannwerken

Thüringer Energienetze

Operative Maßnahmen zur Aufrechterhaltung der OT Sicherheit

OT Härtung

- Hardware / Software
  - wiederholende Penetrationtests & Tiefenanalysen
  - Schwachstellenmanagement im Rahmen DL Steuerung → Ziel schließen von Schwachstellen
- OT/IT spezialisiertes Schwachstellenmanagement
  - dauerhafte Überprüfung vorahnender und neuer Schwachstellen
  - tägliche Auswertung der BSI Lageberichte → mit anschließender Risikobeurteilung
  - eingeübte Reaktionen auf veränderte Bedrohungslagen

Vorfallsmanagement

- grundsätzlich werden bei Vorfällen (erkannten Anomalien | Einbrüchen in Anlagen) ad-hoc Maßnahmen eingeleitet
  - Befahrung / Begehung → physische & optische Kontrolle aller OT/IT Systeme
  - Netzwerkanalysen und ggf. sofortige Isolation (technisch | physisch) nicht mehr vertrauenswürdiger OT/IT Systeme
  - Ableitung von Maßnahmen und Verbesserungen für alle betroffenen Systeme

Business Continuity Management

- Backup- & Recovery Strategie aktualisieren & erproben
- Notfallpläne zur Absicherung des Netzbetriebs sind vorhanden und werden stets aktualisiert (bspw. Blackoutfall, manueller Netzbetrieb)
- Priorisierung der Weiterentwicklung von Verfahren zur **schnellen** Wiederherstellung der Beobachtbarkeit- und Steuerbarkeit der Energienetze

Thüringer Energienetze

Maßnahmen Personal

- **Sensibilisierung aller Mitarbeiter**
  - Regelmäßige E-Learning
  - Spezifische Weiterbildung
  - Informationssicherheit Bestandteil jeder Beratung

- **Aufrechterhaltung Kompetenz der ISB / Admins / Spezialisten / ISMS**
  - Aktualisierungen der ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27019
  - Foundation Schulung ISO/IEC 27001
  - TEAG Auditorenschulung ISO/IEC 27001
  - Schulungen der Fraunhofer Gesellschaft zur OT Sicherheit im Bereich der Schutz- und Leittechnik

- **Organisatorische Maßnahmen bei Abweichungen**
  - Ursachen- und Wirksamkeitsüberprüfung bei Abweichungen & ggf. disziplinarische Maßnahmen
  - Risikoanalyse und Behandlung im ISMS der TEN

Thüringer Energienetze

Zertifizierung der nach dem IT Sicherheitskatalog der BNetzA

- **TEN ist seit 2017 gemäß IT Sicherheitskatalog der BNetzA zertifiziert**
  - **Erstzertifizierung 2017 (TÜV Thüringen)**
    - Überwachungsaudit 2018
    - Überwachungsaudit 2019
  - **Rezertifizierung 2020 (TÜV Thüringen)**
    - Überwachungsaudit 2021
    - Überwachungsaudit 2022
  - **Rezertifizierung in 2023 anstehend**

- **Fazit**
  → Audits wesentlicher Bestandteil der Aufrechterhaltung der Informations- und IT Sicherheit der TEN

Thüringer Energienetze

Fazit

- Informationssicherheit ist eine Kombination aus IT/OT Sicherheit + Physische Sicherheit + Personal(-sicherheit) & deren Verhalten:
  - **IT/OT Sicherheit** schützt IT/OT + Informationen **reaktiv** (Abwehr des digitalen Angriffs auf Informationen + IT/OT Komponenten)
  - **Physische Sicherheit** schützt IT/OT **präventiv** (Abwehr von Angriffen auf IT/OT Systeme + Informationen) in den Bereichen Zutritt + Zugriff
  - **Personal(-sicherheit)** schützt IT/OT **präventiv** (Abwehr von Angriffen auf IT/OT + Informationen) in den Bereichen Verhalten, Reaktionen bei Auffälligkeiten, abnormalen Situationen, etc..

→ IT/OT + Informationssicherheit ist **nicht** ein ausschließliches IT Thema

- Angriff & Schutz
  - waren schon immer
  - sind heute aktueller denn je
  - und werden zukünftig verstärkt

  ein Wettbewerb zwischen
  - Politik/Mächten
  - bezahlten Organisationen
  - freien Hackerorganisationen
  - Erpressern (bspw. Ransomware) und
  - denjenigen, die sich schützen (bspw. die KRITIS Unternehmen)

→ es ist zwingend notwendig, sich **auf** die **Notfall- und Recoverykonzepte** zu **konzentrieren**

Thüringer Energienetze