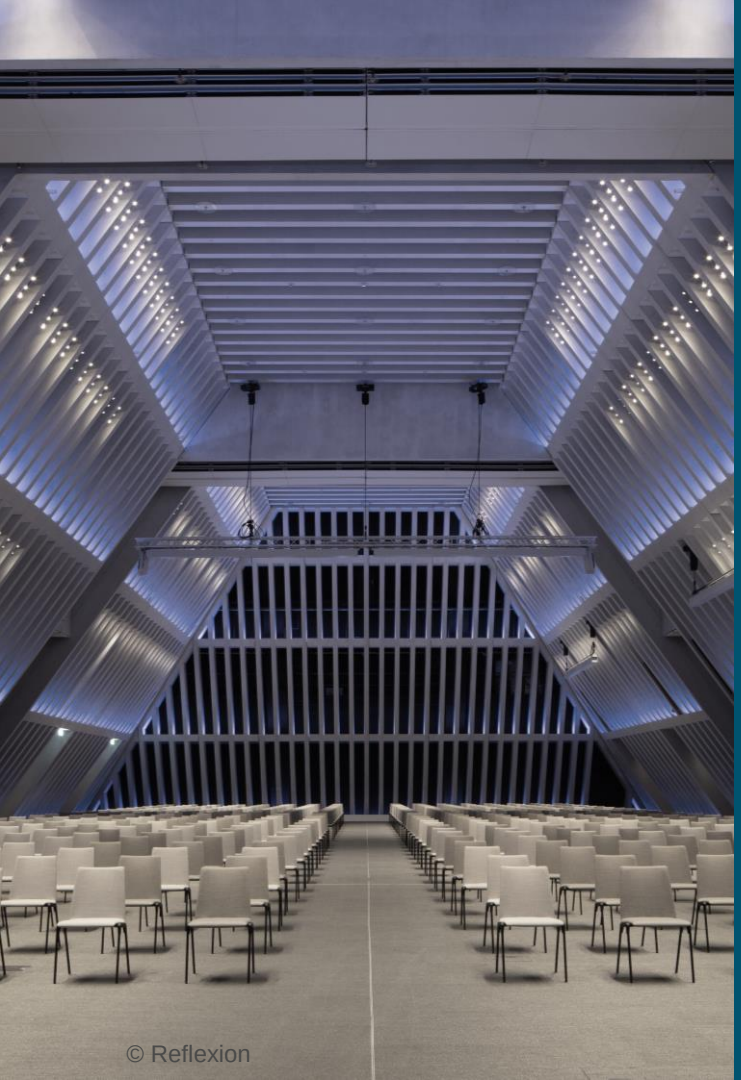
AMSTEIN + WALTHERT

Michael Noack & Marc Naumann

Digitalisierung - Cyber Security



Vorstellung Referenten

AMSTEIN + WALTHERT

Michael Noack

ICT Consultant

Amstein +
Walthert Progress

Marc Naumann

ICT Consultant

Amstein +
Walthert Progress

Daniel Imgrüth

Stv.
Geschäftsführer /
Energieberater

Schnyder
Ingenieure

Agenda

1. Einführung

2. Grundlagen

3. Selbstanalyse

4. Erste Massnahmen

5. Weiterführende Massnahmen

6. Fragerunde

7. Zusammenfassung

Sicht: Cyberkriminelle

- Automatisierte Attacken rund um die Uhr
- Selbst spezifische Angriffe können kostengünstig ausgeführt werden
- **Ein Erfolg reicht oft**, um die Kosten wieder hereinzuholen

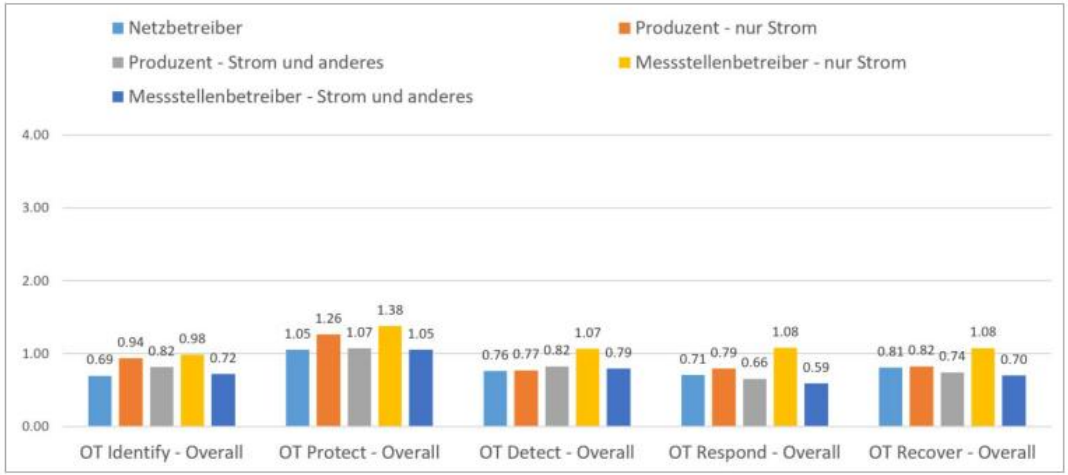
➢ **EVU sind trotz beschränkter Grösse ein interessantes Ziel**

Sicht: EVU

- Vorstellung:
- «Wir sind zu klein, um ein Ziel zu sein»
- «Wir reagieren dann, wenn etwas passiert»
- «In der Schweiz passiert uns sowieso nichts»

Sicht: EVU

- Realität (Bericht vom 28. Juni 2021 des BFE zu Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung:



https://www.globalsign.com/en/blog/cyber-autopsy-series-ukranian-power-grid-attack-makes-history, Aug 2021

AMSTEIN+WALTHERT

Beispiele

Die Stadt Bülach kämpft mit den Folgen eines Hackerangriffs. bild: watson

Bülach ist das neuste Opfer einer Cyberattacke – Mitarbeitende nicht per E-Mail erreichbar

Ransomware-Attacke auf Swissport

Hackerangriff stört zeitweise Flugbetrieb in der Schweiz

Swissport ist Opfer eines Cyberangriffs geworden. Die Attacke auf die Servicegesellschaft für Airlines und Flughäfen sorgte zeitweise für Verzögerungen im Flugbetrieb – und reiht sich ein in eine ganze Serie.

04.02.2022, 13.10 Uhr

IT-Security · Thought Leadership · speicherguide.de · Do

Newsticker · it-sa 2022 · Metaverse · Managed Service · Studien · Suc

Cybersicherheitsvorfälle könnten reale Welt treffen, auch in Deutschland

18. Juni, 2022 · 08:22

Hacker attackieren Arztpraxis und veröffentlichen Patientendaten

Die Ransomware-Bande mit dem Namen «Lockbit» hat erneut eine Arztpraxis in der Schweiz angegriffen. Im Darknet sind nun Diagnosen, Labortests, Daten zu Operationen und mehr aufgetaucht.

von Philipp Anz, 9. Mai 2022 um 17:07

Schwachstellen

- Phishing: Versuch an Logindaten / Passwörter zu kommen
- DDoS-Angriffe (Distributed Denial of Service): Versuch Netzwerk oder Webserver zu überlasten
- Schadsoftware/Malware: Netzwerke mit Schadsoftware infizieren
- Ransomware: Verschlüsselung von Daten

Agenda

1. Einführung
2. **Grundlagen**
3. Selbstanalyse
4. Erste Massnahmen
5. Weiterführende Massnahmen
6. Fragerunde
7. Zusammenfassung

Grundlagen - NIST Framework

- Kategorien des NIST[1] Cyber Security Frameworks:
  - Identify (Identifizieren)
  - Protect (Schützen)
  - Detect (Erkennen)
  - Respond (Reagieren)
  - Recover (Wiederherstellen)

1: NIST - US National Institute for Standards and Technology

Grundlagen - NIST Framework

- Identify
  - Inventar Management
  - Geschäftsumfeld
  - Governance
  - Risikomanagement
  - Risikomanagement Strategie
  - Lieferketten Risikomanagement

Grundlagen - NIST Framework

- Protect
  - Zugriffsmanagement und –steuerung
  - Awareness und Training
  - Datensicherheit
  - Schutz von Daten
  - Maintenance
  - Protective Technology

Grundlagen - NIST Framework

- Detect
  - Vorfälle
  - Überwachung
  - Detection Processes

Grundlagen - NIST Framework

- Respond
  - Response Planning
  - Kommunikation
  - Analyse
  - Mitigation
  - Verbesserungen

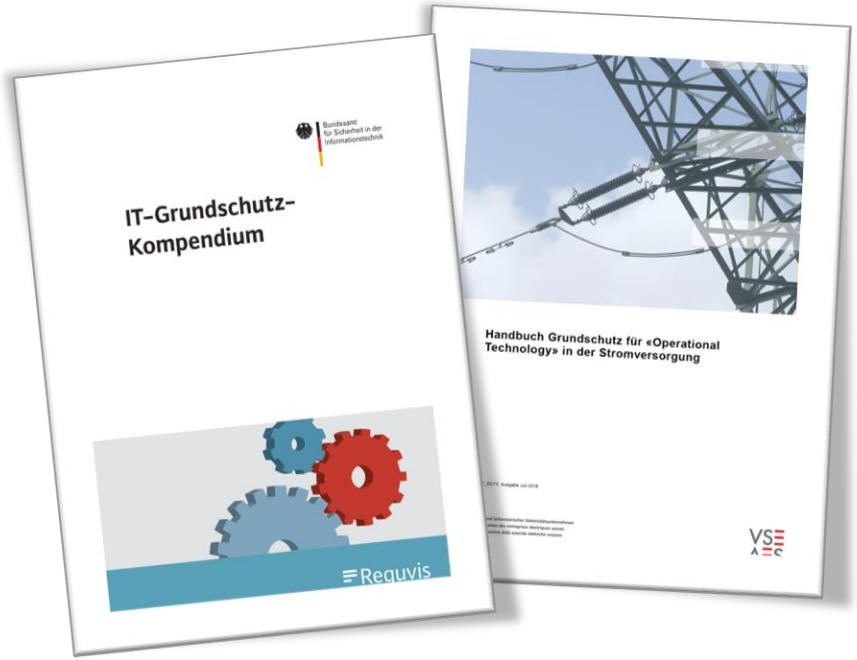
Grundlagen - NIST Framework

- Recover
  - Wiederherstellungsplanung
  - Verbesserungen
  - Kommunikation

Grundlagen – Alternative Richtlinien

- BSI Cybersecurity Richtlinie

- VSE Grundschutz
  in der Stromversorgung

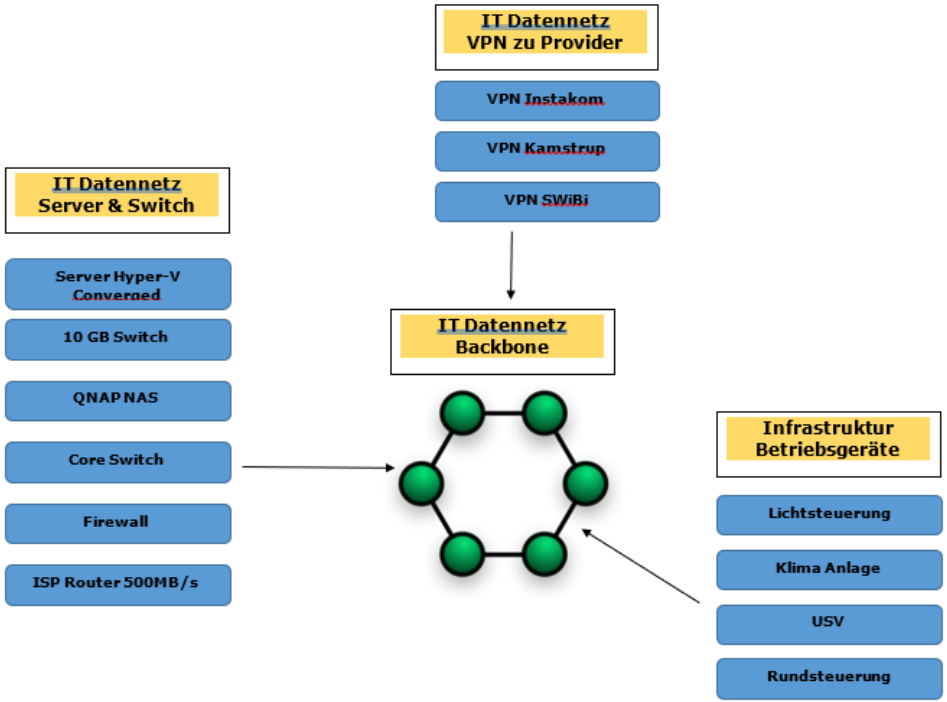


Grundlagen – OT Sicherheit

- Wichtige Unterscheidung zwischen IT und OT
- Zunehmende Vermischung (immer mehr IT in der OT)
- Dadurch auch veränderter Sicherheitsbedarf

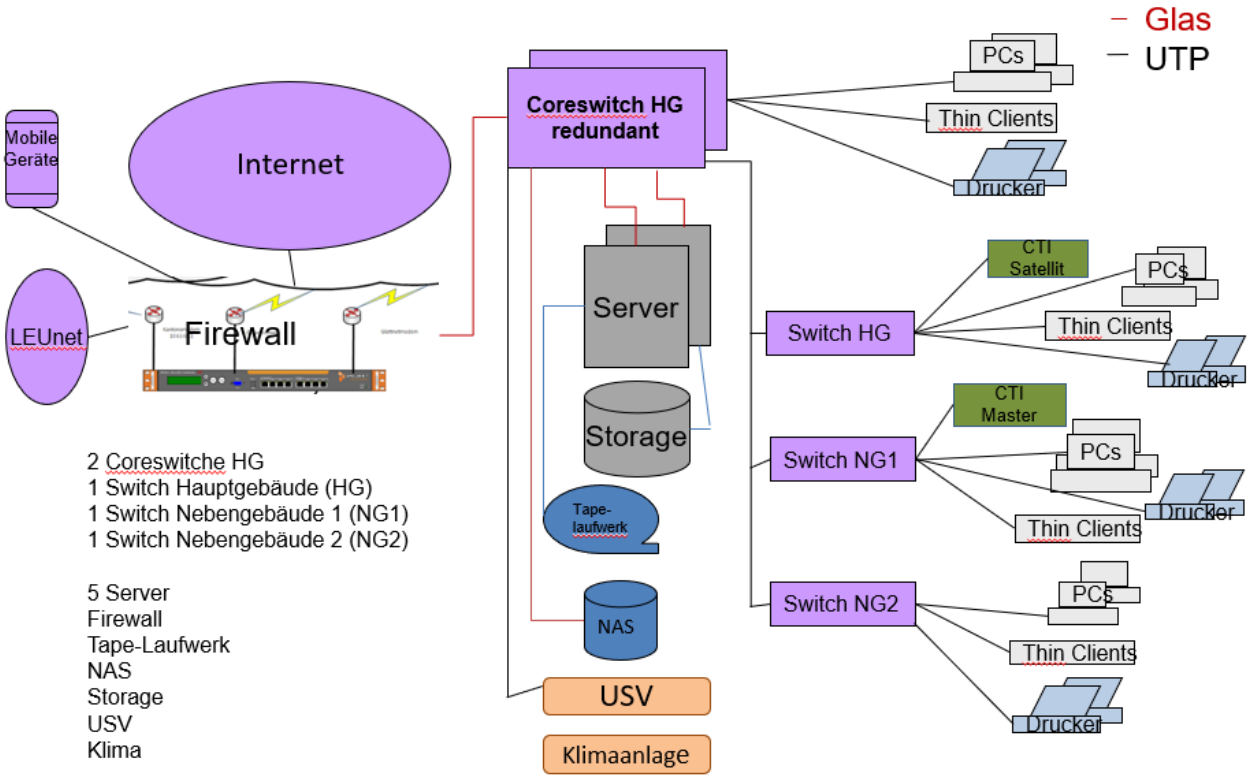
- ➢ Verdient besonderes Augenmerk
- ➢ Miteinander reden: Kompetenzen im Unternehmen nutzen

Grundlagen – typische IT-Landschaft EVU



AMSTEIN+WALTHERT

Grundlagen – typische IT-Landschaft EVU

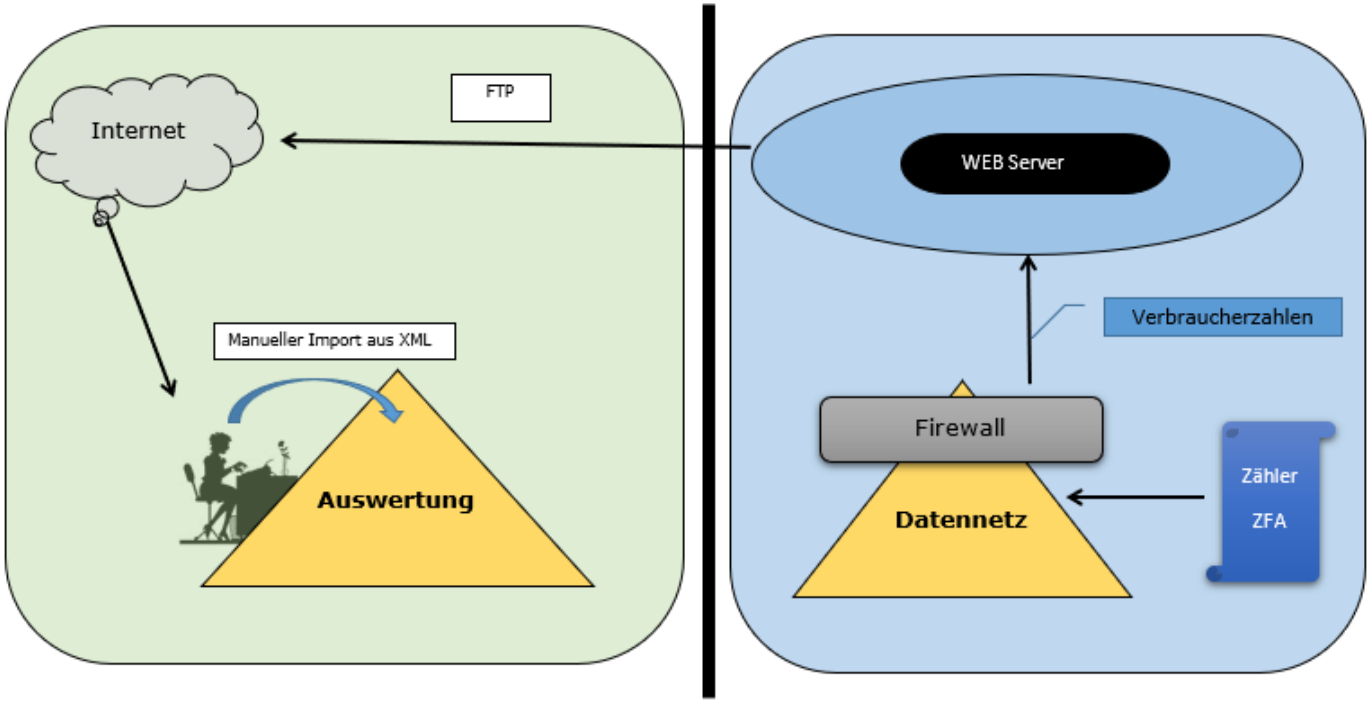


2 Coreswitche HG
1 Switch Hauptgebäude (HG)
1 Switch Nebengebäude 1 (NG1)
1 Switch Nebengebäude 2 (NG2)

5 Server
Firewall
Tape-Laufwerk
NAS
Storage
USV
Klima

AMSTEIN + WALTHERT

Grundlagen – typische IT-Landschaft EVU



Agenda

1. Einführung
2. Grundlagen
3. **Selbstanalyse**
4. Erste Massnahmen
5. Weiterführende Massnahmen
6. Fragerunde
7. Zusammenfassung

Selbstanalyse

- Gibt es einen Verantwortlichen für Cybersecurity?
- Führen wir ein gründliches Inventar?
- Wird Risikomanagement betrieben?
- (Wie) Sind meine MA ausgebildet?
  - Wurden Übungen/Tests durchgeführt?
- Gibt es Richtlinien und Konzepte?
- (Wie) Werden Vorfälle erkannt?
- Überwachen wir das ICT System?
- Gibt es Reaktions-, Kommunikations- und Analysepläne?
- Wurden Assessments oder Penetration Tests durchgeführt?

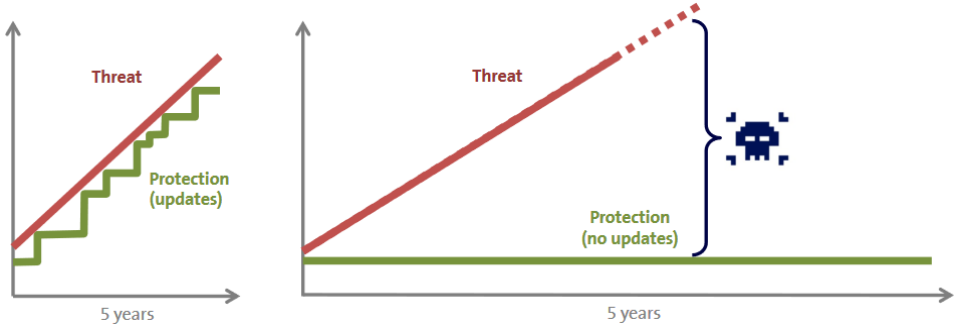
Agenda

1. Einführung
2. Grundlagen
3. Selbstanalyse
4. **Erste Massnahmen**
5. Weiterführende Massnahmen
6. Fragerunde
7. Zusammenfassung

Erste Massnahmen

- Verantwortlichkeit zuweisen, Grundlegender Entwurf zu Risikomanagement, Vollständiges Inventar erstellen
- Schulungen organisieren, Grundlegende Konzepte erstellen
- Software zur Erkennung und Überwachung installieren
- Reaktionspläne erstellen
- Kontinuierliche Prozess

Verbesserungen



Agenda

1. Einführung
2. Grundlagen
3. Selbstanalyse
4. Erste Massnahmen
5. **Weiterführende Massnahmen**
6. Fragerunde
7. Zusammenfassung

Zusätzliche Dienstleistungen speziell für EVU

- Amstein + Walthert Progress AG
  - Cyber Security Assessment
  - Prüfung der physischen Sicherheit der IT-Anlagen und Assets, inkl. Data Center
- Schnyder Ingenieure
  - Geschäftsführung | Sekretariat Verwaltungsrat
  - Infrastruktur- und Industrieautomation - Steuerungen von Kraftwerksanlagen, Wasserversorgungen und ARA
  - Energiewirtschaft - Energiebeschaffung im Markt, Portfolio- und Risikomanagement, Wirtschaftlichkeitsberechnungen, Bewertungen, strategische Ausrichtung, Beteiligungen
  - Netzwirtschaft - Regulatorisches Management, Tarifierung, Anlagebuchhaltung und Assetmanagement, Bewertungen
  - Elektrotechnik - Potenzialanalysen und Engineering von Produktions- und Verteilanlagen | Netzplanung
  - Energieeffizienz | Erneuerbar Energie - Aufbau Energieberatungsdienstleistung, Beratung für KMU, Grossverbraucher (Zielvereinbarung), energetische Betriebsoptimierung, Energiedatenmonitoring
- Ext. Partner
  - Datenschutz-Audits / System- und Applikationskontrollen / Penetration Tests

AMSTEIN + WALTHERT

Agenda

1. Einführung
2. Grundlagen
3. Selbstanalyse
4. Erste Massnahmen
5. Weiterführende Massnahmen
6. **Fragerunde**
7. Zusammenfassung

Fragerunde

- Fragen?

Agenda

1. Einführung
2. Grundlagen
3. Selbstanalyse
4. Erste Massnahmen
5. Weiterführende Massnahmen
6. Fragerunde
7. **Zusammenfassung**

Zusammenfassung

- An Cybersecurity Frameworks und Richtlinien orientieren (z.B. NIST)
- Assessments / Übungen mit MA und für gesamte Organisation durchführen
- Lieber präventiv Massnahmen ergreifen, als Opfer werden

AMSTEIN + WALTHERT

„Sicherheit ist kein Zustand und kein Produkt – Sicherheit ist ein Prozess.“