TimeOut Business-Lunch, 26.02.2019

Cybersecurity-Erhebung bei kleinen und mittleren Elektrizitätsversorgungsunternehmen 2018

Wir machen Infrastrukturen digital sicher
www.electrosuisse.ch/cybersecurity

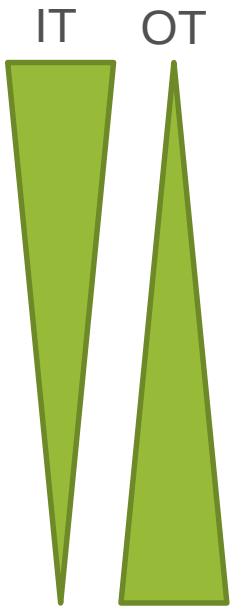
Electrosuisse

- 1889 gegründet als Schweizerischer Elektrotechnischer Verein (SEV).
- 2002 Neupositionierung als Electrosuisse.
- Hauptsitz in Fehraltorf, 230 Mitarbeitende.
- Mitglieder: 5000 Fachleute und mehr als 2000 Firmen.
- Akkreditierte und neutrale Fachstelle mit Angeboten zu Inspektion, Beratung, Prüfung, Zertifizierung, Normung und Weiterbildung.
- Seit 130 Jahren engagiert für elektrische Sicherheit.
- Seit 2018 auch engagiert für digitale Sicherheit.

Cybersecurity

3 Voraussetzungen und Schutzziele

- **Vertraulichkeit** (**C**onfidentiality)
  Zugriff nur für Berechtigte
  → *Zugriffskontrolle, Verschlüsselung*
- **Integrität** (**I**ntegrity)
  Korrektheit, Unverfälschtheit und Nachvollziehbarkeit
  → *Inhaltsauthentifizierung, Protokollierung (Audit Log)*
- **Verfügbarkeit** (**A**vailability)
  Wahrscheinlichkeit der Erfüllung der Anforderungen
  → *Redundanz, Backup*



Cybersecurity Konzept

Ein ganzheitliches Sicherheitskonzept basiert auf 3 Säulen:

1. Prävention & Verhinderung (vorher)
2. Monitoring & Entdeckung (während)
3. Reaktion, Wiederherstellung & Forensische Analyse (nachher)

Alle drei Säulen beinhalten sowohl technische als auch organisatorische und rechtliche Massnahmen.

Cybersecurity ist Chef-Sache!

NIST Cybersecurity Framework

5 prozessorientierte Funktionen:

1. **Identify** Was ist warum und wie gut zu schützen?
2. **Protect** Wie wird es geschützt?
3. **Detect** Wie wird eine Sicherheitsverletzung erkannt?
4. **Respond** Wie wird auf einen Vorfall reagiert?
5. **Recover** Wie wird die Sicherheit nach einem Vorfall wiederhergestellt?

vorher

während

nachher

Cybersecurity-Erhebung 2018

- 30 Elektrizitätsversorgungsunternehmen mit 4 bis 600 Mitarbeitern.
- Ziele:
  a) Rasche Standortbestimmung und Vergleich mit anderen.
  b) Zu adressierende Handlungsfelder aufzeigen.
- Unscharfe Messung:
  - Menschen: Kompetenz-Niveau
  - Prozesse/Methoden: Maturitäts-Niveau (Rating nach NIST-CSF)
  - Technologie: Security Level
- Fragen zu 23 Schlüsselelementen der Cybersecurity.
- Quick Assessment: Interview ca. 2 h vor Ort ohne Nachweise.

NIST-CSF Maturitätsstufen

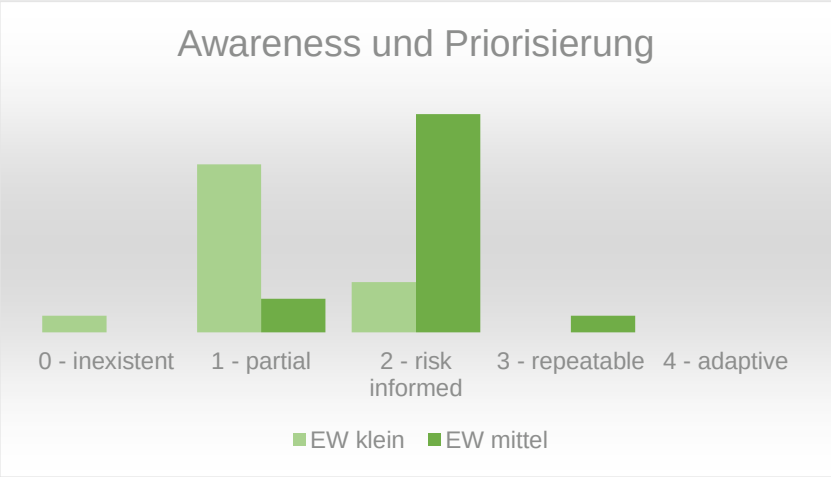
Stufe	Beschreibung
0 – Inexistent	▪ Thema/Risiko ist nicht adressiert.
1 – Partial	▪ Risiken sind nur teilweise bekannt und Massnahmen werden nur partiell umgesetzt. ▪ Risikomanagement ist nicht definiert, ad-hoc, oft nur reaktiv und nicht priorisiert.
2 – Risk Informed	▪ Risiken sind bekannt, Massnahmen werden priorisiert, aber nicht systematisch umgesetzt. ▪ Risikomanagement und Massnahmen sind definiert, aber noch nicht in der Organisation verankert.
3 – Repeatable	▪ Risikomanagement ist in Standards und Richtlinien vollständig definiert und in der Organisation verankert. ▪ Massnahmen sind auch als Prozesse beschrieben und werden systematisch umgesetzt.
4 – Adaptive	▪ Risikomanagement wird auf Basis von Erfahrungen und Kennzahlen/Indikatoren regelmässig angepasst. ▪ Massnahmen werden den Risiken und der Bedrohungslage laufend angepasst.

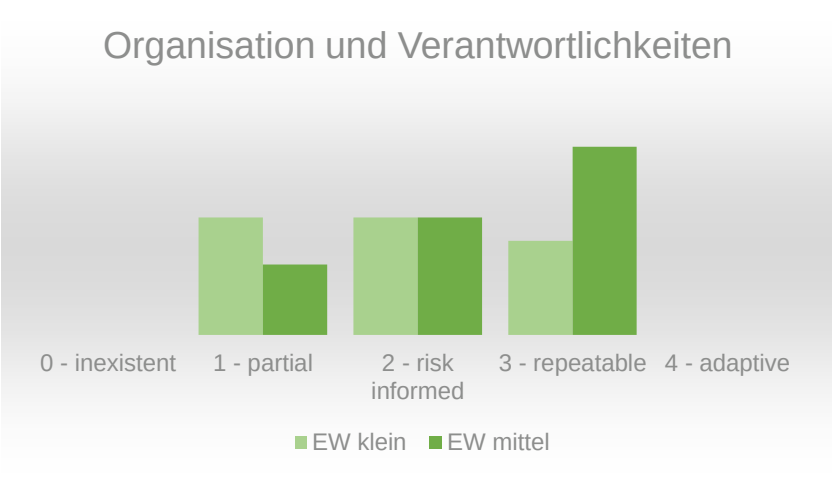
Durchschnittliche Cybersecurity Maturität

Hauptbefunde Gesamterhebung

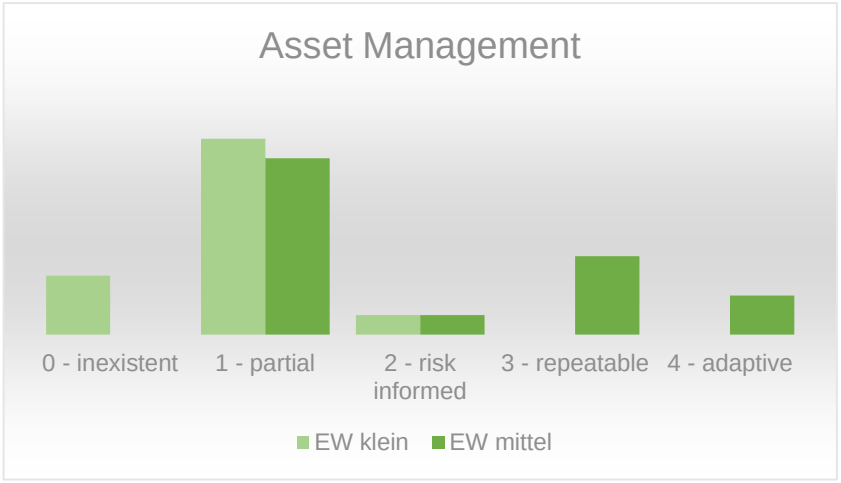
- Fehlendes vollständiges Asset Management.
- Zu wenig Risikobasiertheit.
- Fokus primär auf Schutzmassnahmen.
- Cybersecurity als Blindflug.
- Reaktionsbereitschaft ungenügend.
- Notfallvorbereitung und -übung ungenügend.
- Lieferantenrisiken unbekannt und vernachlässigt.
- Mensch als grösste Schwachstelle zu wenig behandelt.
- Fehlende Fachkompetenz und Ressourcen.
- Cybersecurity kein geführter Prozess.

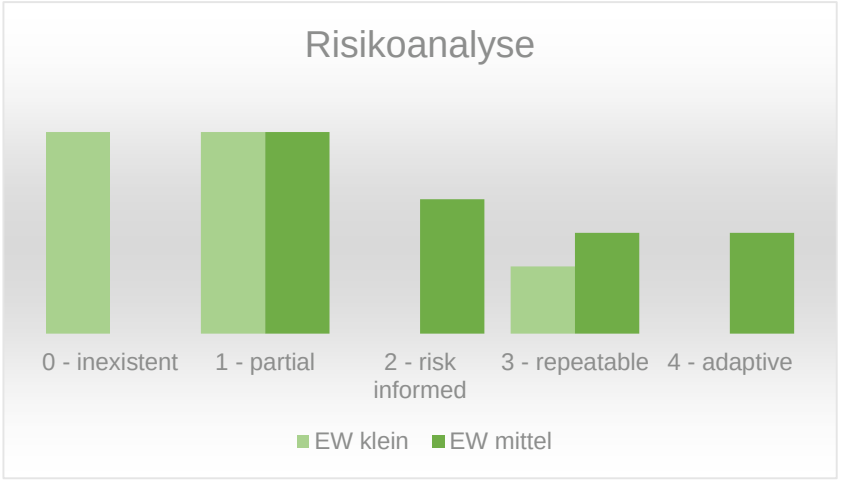
Organisatorische Verankerung



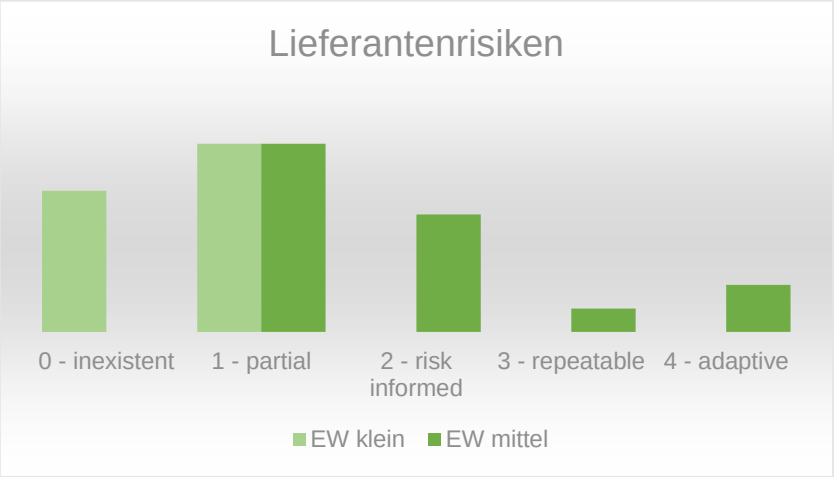


Grundlagen für Risikobasiertheit

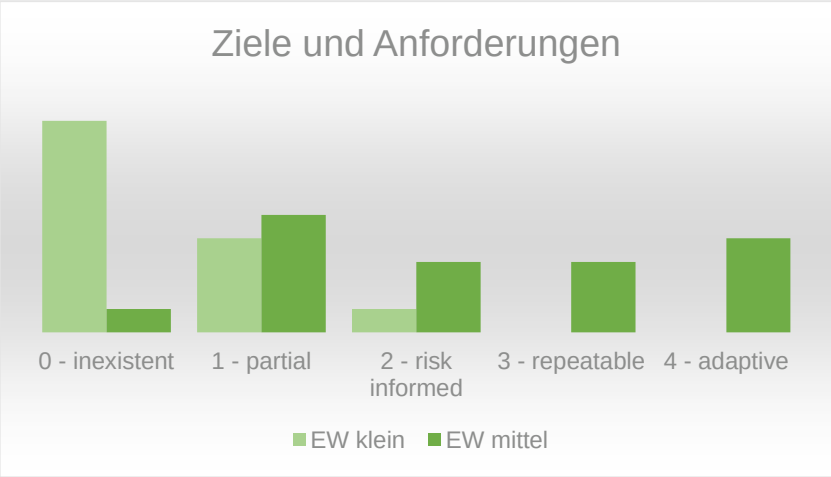


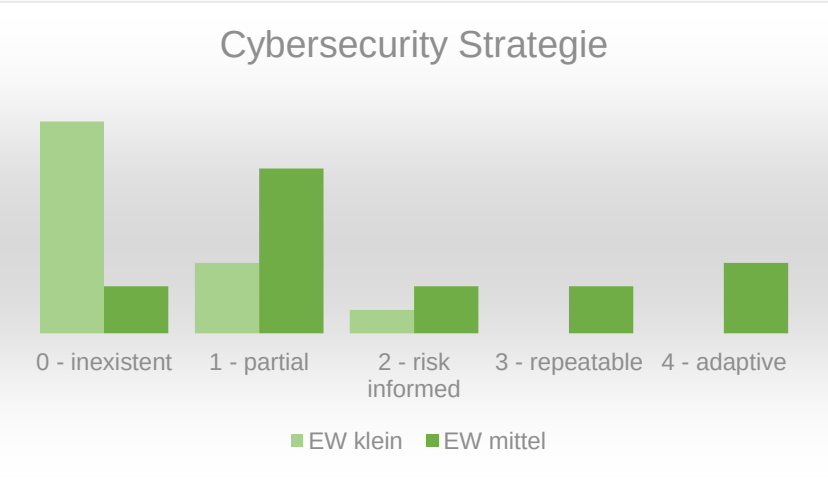


Importierte Risiken

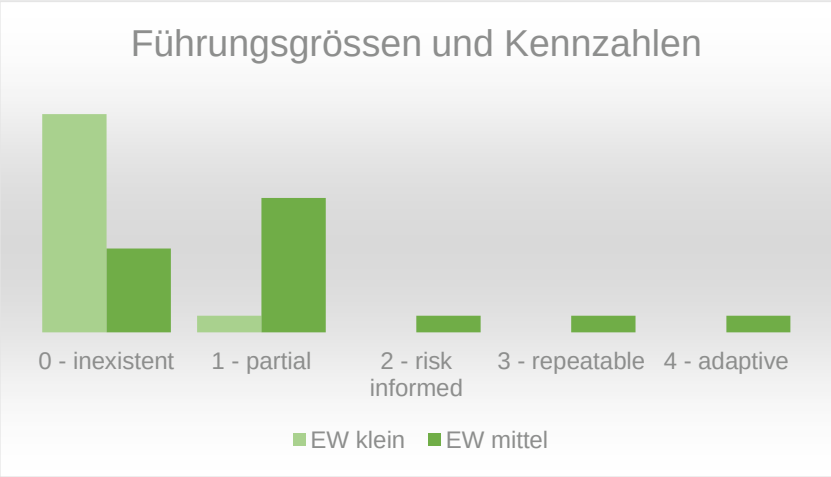


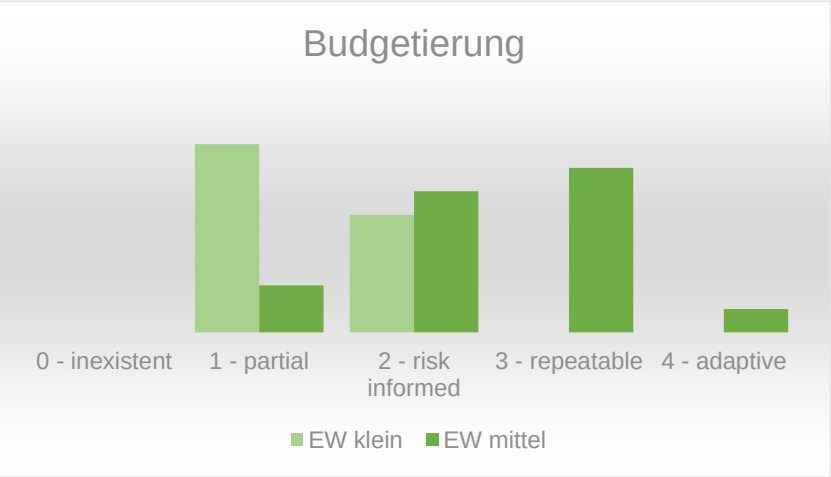
Zielorientierung



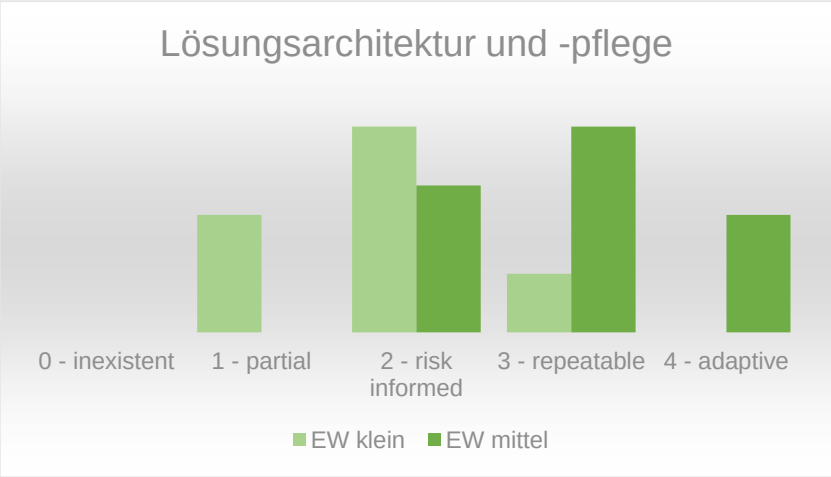


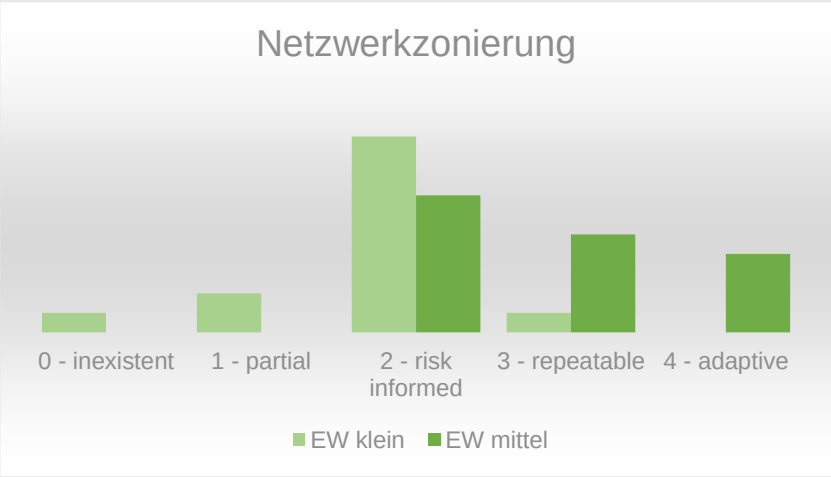
Führung und Budgetierung



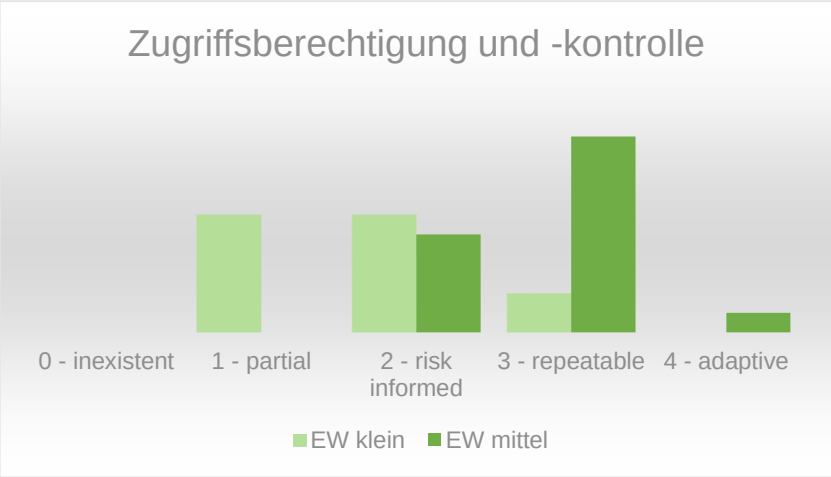


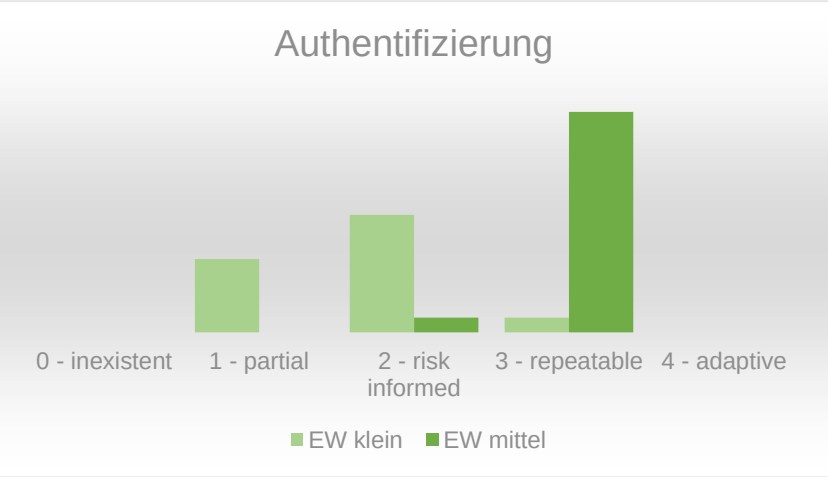
Technische Sicherheitslösung



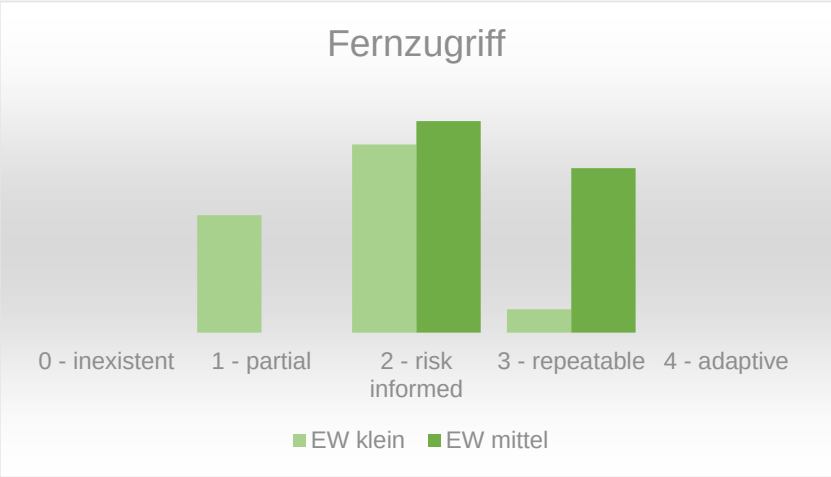


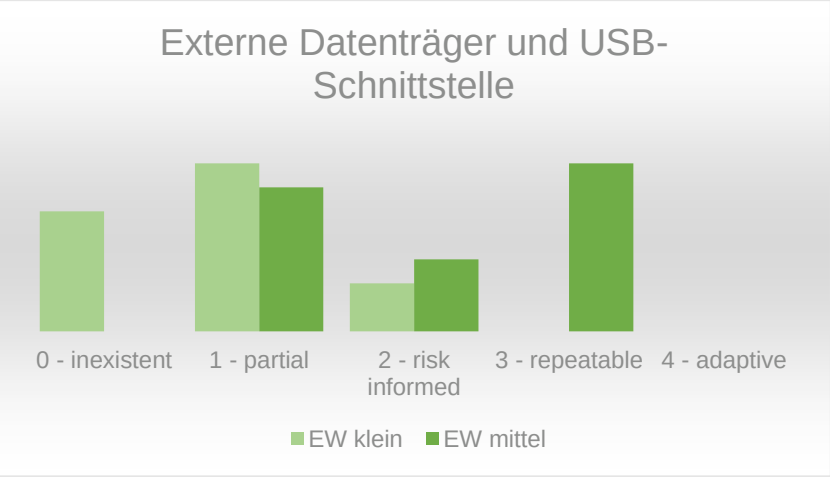
Identitäts- und Zugangsmanagement



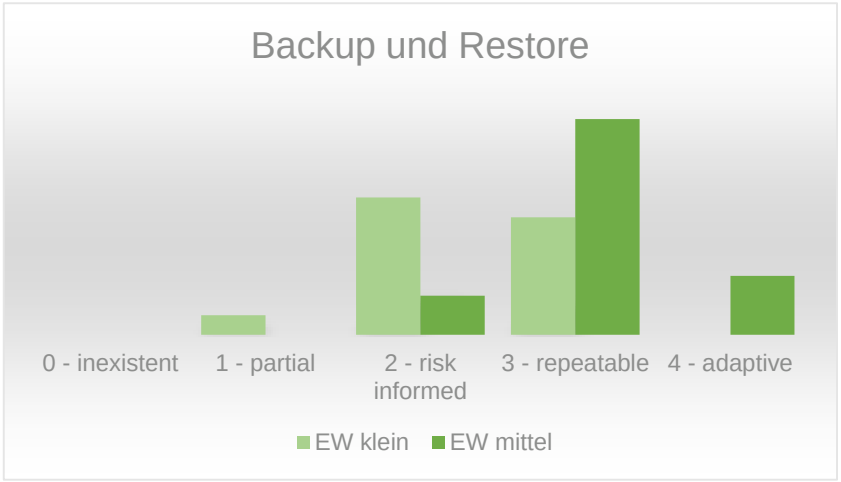


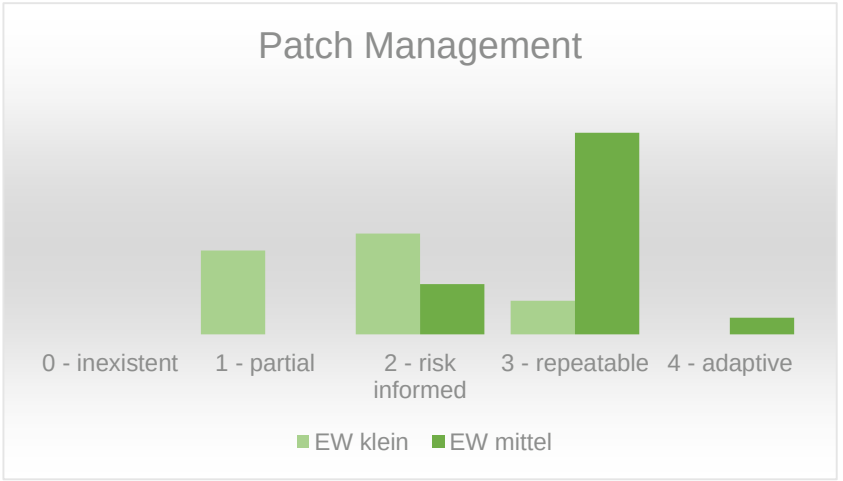
Schnittstellenrisiken



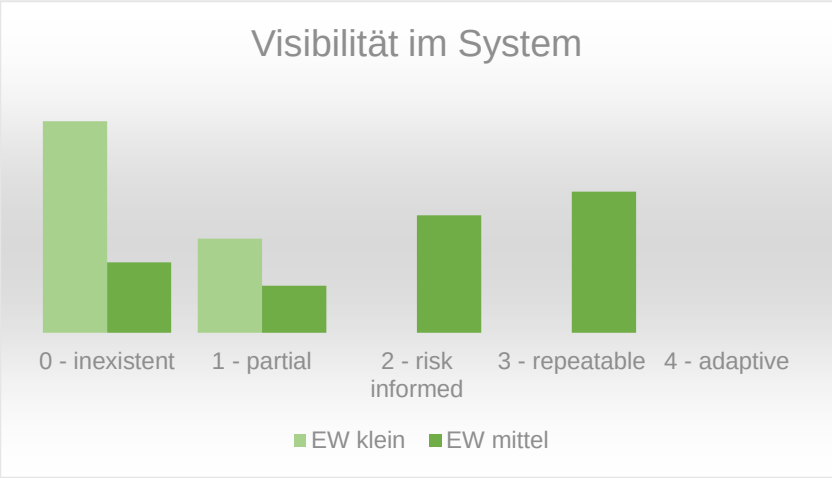


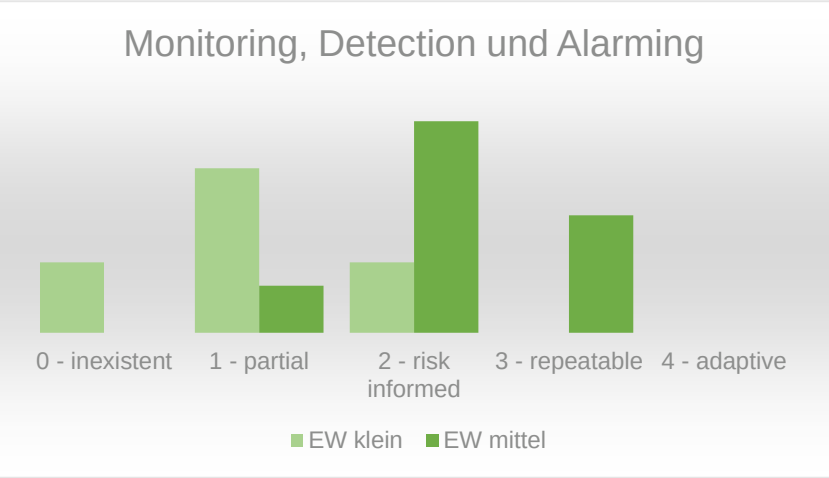
Klassische System Administration



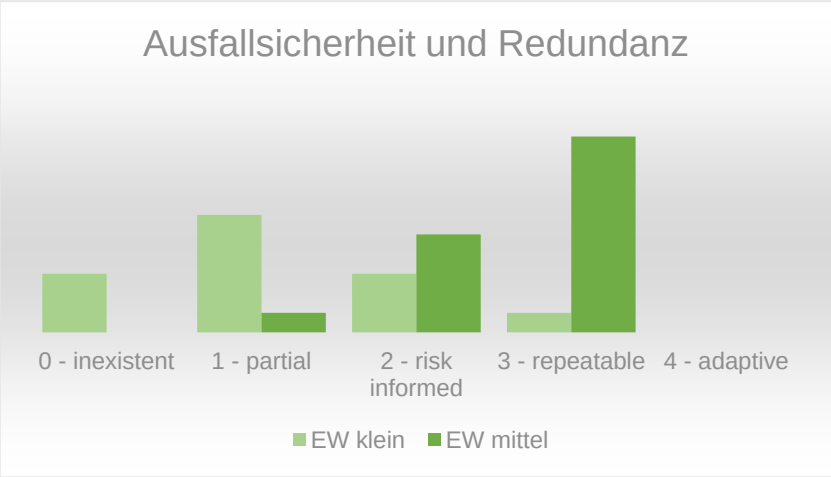


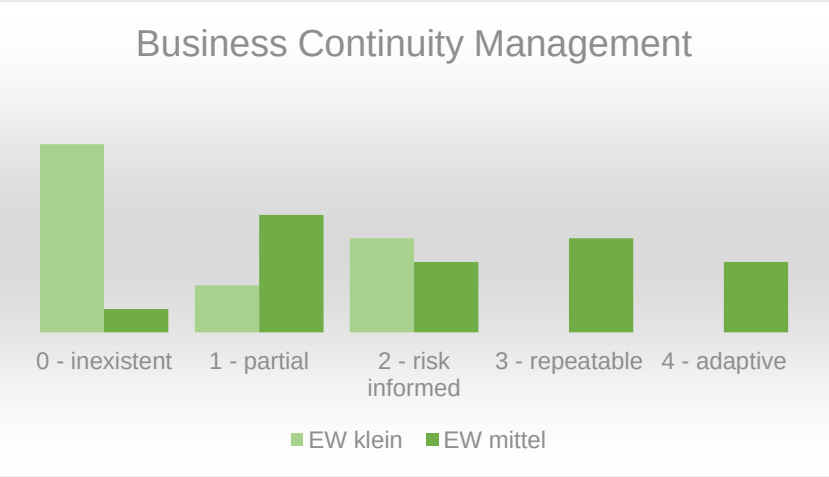
Sehen, erkennen und alarmieren



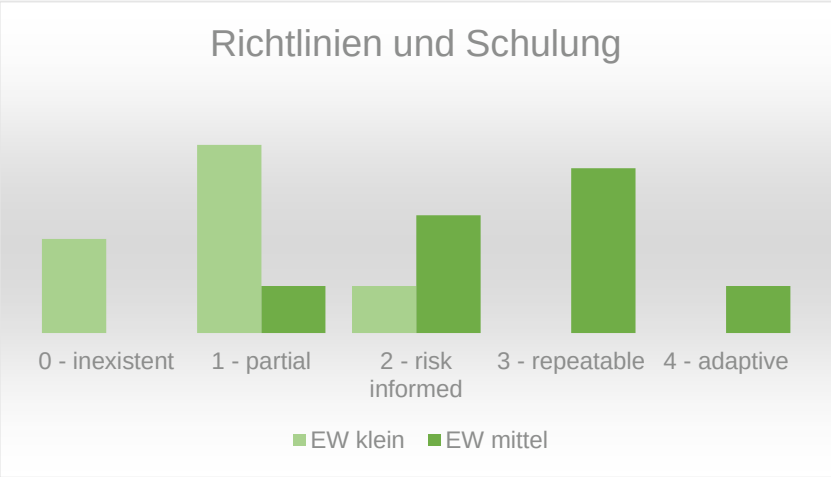


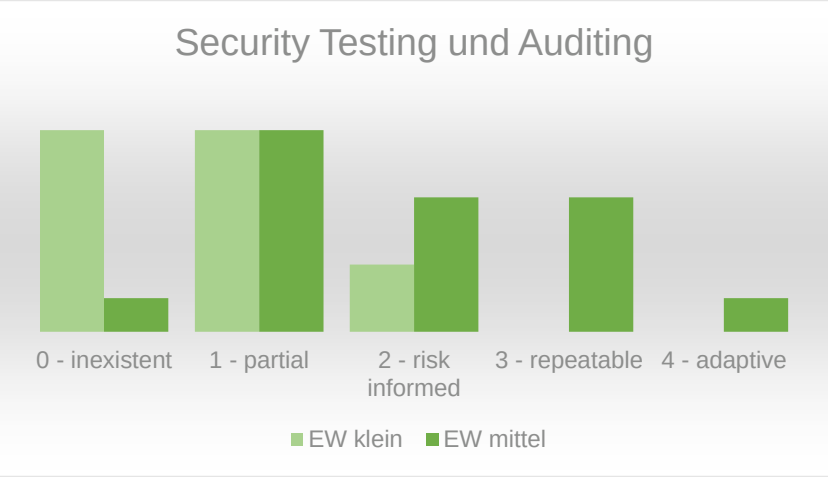
Notfallvorsorge





Faktor Mensch und Sicherheitsprüfung





Electrosuisse Cybersecurity Angebote

Beratung und Coaching	Schulung
Cybersecurity Foundations & Partner Care ▪ Schutzbedarfsermittlung ▪ Cybersecurity Gap-Analyse ▪ Massnahmendefinition und -planung ▪ Lieferantenmanagement	**Schulung für Betriebsleiter und IT/OT-Verantwortliche** ▪ Risiken ▪ Schlüsselelemente ▪ Vorgehen
Sparringpartner ▪ Periodische Cybersecurity-Beurteilung und Optimierung	**Awareness Training** ▪ Regelmässige Sensibilisierung und Schulung vor Ort