# #24 Cyber Security

ZUKUNFTVERTEILNETZ

Firma: Datum:

**Anleitung:** Diskutieren Sie das Arbeitsblatt Cyber Security.
Beantworten Sie diese Fragen: Erfüllen wir die Anforderungen der ElCom an Cyber Security? Stellen wir den Schutz gegen Cyber-Angriffe umfassend sicher? Ermitteln Sie gemeinsam in einem ersten Schritt mögliche Sicherheitslücken und definieren Sie die nächsten Schritte.

## 1. Schritt: Bestandsaufnahme

### Risikolandschaft

Schaffen Sie sich einen Überblick über potentielle Angriffspunkte. Für einen detaillierteren Test:
https://digitalswitzerland.com/de/kmu-schnell-check/

**Energieerzeugungs- und Verteilnetz und Gebäude-Infrastruktur**

- Wird der Zutritt zu Gebäuden und Anlagen geregelt und dokumentiert?
- Sind Ihre Anlagen gegen bösartige Software geschützt?

**Organisation, Mitarbeitende und Prozesse**

- Ist in Ihrem Betrieb die Verantwortung für Cyber Security und für IT-Vorfälle definiert?
- Sind die Sofortmassnahmen im Falle eines IT-Vorfalls definiert?
- Haben Sie Passwortrichtlinien?

**ICT-Systemlandschaft / Operational Technology**

- Sind die Daten auf Ihren Systemen verschlüsselt?
- Werden Ihre Systeme automatisch aktualisiert?
- Verwenden Sie gesicherte und verschlüsselte Kommunikationsverbindungen?

### Wo sind Sie potentiell angreifbar? Wo sind Ihre Schwachstellen, wo haben Sie blinde Flecken?

### Wo stehen Sie im Bereich Cyber Security?

- ☐ Wir haben an einer Umfrage (BFE, ElCom, Electrosuisse) zu Cyber Security teilgenommen
- ☐ Wir haben die Studien der Electrosuisse und der ElCom gelesen und erkannt, dass Handlungsbedarf besteht
- ☐ Wir haben den „Cyber Security"-Schnelltest für KMU durchgeführt
- ☐ Wir sind uns bewusst, dass uns das Thema Cyber Security direkt betrifft.
- ☐ Wir haben unsere Infrastruktur, Organisation, Prozesse und die ICT-Systemlandschaft durch einen externen Spezialisten in einem „Cyber Security"-Assessment auf Sicherheitslücken überprüft
- ☐ Wir setzen Massnahmen um, um die Sicherheit umfassend zu gewährleisten
- ☐ Wir überprüfen unsere Infrastruktur, Organisation und Prozesse regelmässig

### Welche Massnahmensetzen wir bereits um?

- ☐ Wir schulen unsere Angestellten regelmässig im Umgang mit Cyber Sicherheit
- ☐ Unsere Mitarbeitenden wissen, worauf sie in ihrem Arbeitsalltag mit Bezug auf Cyber Sicherheit achten müssen
- ☐ Wir haben klare Zutrittsregelungen für alle Gebäude, Anlagen und Räume und setzen diese konsequent durch
- ☐ Wir haben IT-Sicherheitssysteme im Einsatz
- ☐ An unsere Lieferanten (beispielweise Head End System, Smartmeter, Gebäudeschliess-Systeme etc.) stellen wir konkrete und klare Sicherheitsanforderungen
- ☐ Wir haben mittels Penetration-Tests einige Sicherheitslücken entdeckt
- ☐ Weitere:

Falls Sie viele Kästchen markiert haben, sind Sie auf gutem Weg. Eine umfassende Überprüfung ist wichtig.

**2. Schritt: Massnahmen definieren**
Ziel: Schliessen der Sicherheitslücken planen

**3. Schritt: Sicherheitslücken beheben**
Ziel: Massnahmen umsetzen

**4. Schritt: Schutz testen**
Ziel: Wirkung der Massnahmen prüfen

**5. Schritt: Regelmässig überprüfen**
Ziel: Nächste Bestandsaufnahme planen

**Erkenntnisse und Massnahmen**
Unterstützung durch externen Spezialisten zur Finalisierung der Bestandsaufnahme und zur Definition von individuellen Massnahmen?