Swissgrid AG
Bleichemattstrasse 31
Postfach
5001 Aarau
Schweiz

T +41 58 580 21 11
info@swissgrid.ch
www.swissgrid.ch

Factsheet

Cybersicherheit bei kritischen Infrastrukturen

Datum Juni 2023

1 Digitale Transformation und Cybersicherheit: die Risiken verstehen

Unter Digitalisierung versteht man den Prozess der Nutzung digitaler Technologien, um Geschäftsabläufe und -prozesse zu transformieren und zu automatisieren. Dies kann unter anderem den Einsatz von Technologien wie Cloud-Computing, das Internet der Dinge (IoT), Big-Data-Analysen und maschinelles Lernen umfassen. Ziel dieser Digitalisierungsbemühungen ist es, die betriebliche Effizienz zu optimieren, die Planungsgenauigkeit zu verbessern und die betriebliche Zuverlässigkeit, Sicherheit und Widerstandsfähigkeit zu erhöhen.

Infolgedessen wird die Infrastruktur der Stromnetze zunehmend durch intelligente Informations- und Kommunikationstechnologien gesteuert. Die Verfügbarkeit, Integrität oder Vertraulichkeit von Daten und Systemen sind potenzielle Risikofaktoren: Im schlimmsten Fall können Cyberbedrohungen zu einem grossflächigen Netzzusammenbruch führen, sodass grosse Gebiete über einen längeren Zeitraum ohne Strom sind. Dies könnte zu erheblichen Unterbrechungen bei wichtigen Diensten und kritischer Infrastruktur sowie in der Gesellschaft und der Wirtschaft führen.

Für die Betreiberinnen und Betreiber kritischer Infrastruktur ist es daher von entscheidender Bedeutung, zuverlässige Cybersicherheitsmassnahmen zu ergreifen, um Cyberangriffe zu verhindern und die potenziellen Auswirkungen eines Angriffs abzumildern.

2 Cybersicherheit: höchste Priorität

Als Betreiberin kritischer Infrastruktur ist sich Swissgrid der Bedeutung der Cybersicherheit in der heutigen digitalen Landschaft bewusst. Wir legen grossen Wert darauf, verlässliche Sicherheitsmassnahmen umzusetzen, um unsere Systeme zu schützen und den sicheren Betrieb des Schweizer Übertragungsnetzes zu gewährleisten.

Das Cybersicherheitsprogramm von Swissgrid stützt sich auf die folgenden Säulen:

- Risikobewertung: Das Programm ermittelt und bewertet Cybersicherheitsrisiken für die Informationen und Systeme des Unternehmens.

- Governance: Das Programm definiert Rollen, Verantwortlichkeiten und Prozesse, um Cybersicherheitsrisiken zu verwalten und die Rechenschaftspflicht zu gewährleisten.

- Asset-Management: Das Programm ermittelt und verwaltet alle Vermögenswerte, einschliesslich Hardware, Software und Daten, um ihren Wert und ihre Wichtigkeit für das Unternehmen zu verstehen.

- Zugangskontrolle: Das Programm beschränkt den Zugang zu sensiblen Daten und Systemen auf befugtes Personal und verwendet eine Multi-Faktor-Authentifizierung, um den Zugang zu sichern.

- Reaktion auf Vorfälle: Das Programm erstellt einen Plan, um auf Cybersicherheitsvorfälle zu reagieren und ihre Auswirkungen auf die Organisation zu minimieren.

- Schulung des Sicherheitsbewusstseins: Das Programm bietet allen Mitarbeitenden kontinuierliche Schulungen zu bewährten Verfahren der Cybersicherheit und zu ihrer Rolle beim Schutz der Vermögenswerte des Unternehmens.

- Kontinuierliche Überwachung: Im Rahmen des Programms werden die Systeme und Netze des Unternehmens kontinuierlich auf potenzielle Sicherheitsbedrohungen hin überwacht. Zudem werden proaktiv Risiken ermittelt und vermindert.

- Betriebskontinuitätsmanagement (BKM): Das Programm umfasst BKM-Praktiken, um sicherzustellen, dass kritische Geschäftsprozesse im Falle eines Cybersicherheitsvorfalls oder einer anderen Störung weiterlaufen können.

- Notfallwiederherstellung: Das Programm erstellt einen Notfallwiederherstellungsplan, um kritische Systeme und Daten im Falle eines Cybersicherheitsvorfalls oder einer anderen Störung wiederherzustellen.

- Externe Zusammenarbeit: Das Programm arbeitet mit externen Partnern wie Industriepartnern, Anbietern und Regierungsbehörden zusammen, um Cybersicherheitsrisiken zu erkennen und zu mindern.

Die Bedrohungslandschaft entwickelt sich ständig weiter. Darüber hinaus sind Cyberangreifer immer auf der Suche nach neuen Schwachstellen sowie Techniken, um diese auszunutzen. Es reicht daher nicht, ein Cybersicherheitsprogramm einmalig umzusetzen, sondern es muss kontinuierlich verbessert werden.

Kontinuierlich verbessern bedeutet, das Cybersicherheitsprogramm regelmässig zu überprüfen und zu bewerten, Schwachstellen und verbesserungswürdige Bereiche zu ermitteln und die notwendigen Anpassungen vorzunehmen, um das Programm zu optimieren. Dieser Prozess sollte durch regelmässige Bedrohungsbewertungen und Anfälligkeitsprüfungen sowie durch laufende Schulungen für die Mitarbeitenden und die Zusammenarbeit mit externen Partnern unterstützt werden.

Durch die kontinuierliche Verbesserung unseres Cybersicherheitsprogramms wollen wir neuen Bedrohungen immer einen Schritt voraus sein, indem wir uns an veränderte Umstände anpassen und stets ein hohes Sicherheitsniveau aufrechterhalten.

Das Managementsystem für Informationssicherheit von Swissgrid ist nach ISO/IEC 27001 zertifiziert, einem der am meisten anerkannten und akzeptierten internationalen Standards für Informationssicherheit.

3 Zusammenfassung

Die Digitalisierung bringt auch die Nutzung von Netzwerken, Cloud-Computing und anderen digitalen Plattformen mit sich, die anfällig für Cyberangriffe sein können. Deshalb müssen Unternehmen zuverlässige Cybersicherheitsmassnahmen einführen, um ihre Systeme und Daten vor Störungen, Verstössen, Diebstahl und anderen Arten von Cyberbedrohungen zu schützen.

Als Betreiberin kritischer Infrastruktur räumt Swissgrid dem Schutz vor Cyberbedrohungen höchste Priorität ein und verpflichtet sich zu einem kontinuierlichen Verbesserungsprozess.