swissgrid

Swissgrid AG
Bleichemattstrasse 31
Postfach
5001 Aarau
Switzerland

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

Factsheet

Cyber security and critical infrastructure

Date June 2023

1 Digital transformation and cybersecurity: understanding the risks

Digitalisation refers to the process of using digital technologies to transform and automate business operations and processes. This may include the use of technologies such as cloud computing, the Internet of Things (IoT), big data analytics and machine learning, among others. The goals of these digitalisation efforts are to optimise operational efficiency, improve planning accuracy and enhance operational reliability, safety and resilience.

As a result, the infrastructure of power grids is increasingly controlled by intelligent information and communication technologies. The availability, integrity or confidentiality of data and systems are potential risk factors: in the worst case, cyber threats can lead to a widespread blackout, leaving large areas without electricity for an extended period of time. This could cause significant disruption to essential services and critical infrastructure as well as to society and the economy.

It is essential for operators of critical infrastructure to implement robust cybersecurity measures to prevent cyberattacks and mitigate the potential impact of an attack.

2 Cybersecurity: a top priority

As an operator of critical infrastructure, Swissgrid recognises the importance of cybersecurity in today's digital landscape. We prioritise the implementation of robust security measures to safeguard our systems and ensure the safe operation of the Swiss transmission network.

The Swissgrid cybersecurity programme is built on the following pillars:

- Risk assessment: the programme identifies and assesses cybersecurity risks to the organisation's information and systems.

- Governance: the programme defines roles, responsibilities and processes for managing cybersecurity risks and ensuring accountability.

- Asset management: the programme identifies and manages all assets, including hardware, software and data, to understand their value and criticality to the organisation.

- Access control: the programme limits access to sensitive data and systems to authorised personnel and uses multi-factor authentication to secure access.

- Incident response: the programme establishes a plan to respond to cybersecurity incidents and minimise their impact on the organisation.

- Security awareness training: the programme provides ongoing training to all employees on cybersecurity best practices and their roles in protecting the organisation’s assets.

- Continuous monitoring: the programme continually monitors the organisation’s systems and networks for potential security threats, and proactively identifies and mitigates risks.

- Business continuity management (BCM): the programme incorporates BCM practices to ensure that critical business processes can continue in the event of a cybersecurity incident or other disruption.

- Disaster recovery: the programme establishes a disaster recovery plan to restore critical systems and data in the event of a cybersecurity incident or other disruptive event.

- External collaboration: the programme collaborates with external partners, such as industry peers, vendors and government agencies, to identify and mitigate cybersecurity risks.

The threat landscape is constantly evolving, and cyber attackers are always looking for new vulnerabilities and techniques to exploit them. Therefore, a cybersecurity programme cannot be a one-time implementation; it must be an ongoing process of continuous improvement.

Continuous improvement involves regularly reviewing and assessing the cybersecurity programme, identifying weaknesses and areas for improvement, and making necessary adjustments to strengthen the programme. This process should be informed by regular threat assessments and vulnerability scans as well as ongoing training for employees and collaboration with external partners.

By incorporating continuous improvement into our cybersecurity programme, we aim to stay ahead of emerging threats by adapting to changing circumstances and maintaining a high level of security over time.

The Swissgrid information security management system has been certified to ISO/IEC 27001, one of the most widely recognised and accepted international information security standards.

3 Summary

Digitalisation involves the use of networks, cloud computing and other digital platforms that can be vulnerable to cyberattacks. Organisations need to implement robust cybersecurity measures to protect their systems and data from disruption, breaches, theft and other types of cyber threats.

As an operator of critical infrastructure, Swissgrid treats protection against cyber threats as a top priority and is committed to an ongoing process of continuous improvement.