AUDIT

Critical infrastructure protection – summary report of past audits, focusing on cyber-resilience

Federal Office for Civil Protection, National Cyber Security Centre, State Secretariat for Security Policy

KEY FACTS

Critical infrastructures are essential for the proper functioning of the economy and for people's livelihoods. They include the power supply, medical care and telecommunications. Protecting these critical infrastructures (CIP) is extremely important.

Nowadays, it is no longer possible to operate critical infrastructures without using networked digital technologies. However, this also increases the likelihood of cyberattacks, which means that cybersecurity plays a key role in CIP. Against this backdrop, the Swiss Federal Audit Office (SFAO) selected nine past audits (see Appendix 4 and Appendix 5) and analysed them in relation to CIP, focusing on cyber-resilience. The SFAO identified seven success factors for effective cybersecurity and supervision:

Cybersecurity success factors	Supervision success factors
Clearly define roles and responsibilities	§ Establish binding requirements in consultation with the sectors and the different federal levels
Anchor and implement system updates and life cycles in maintenance contracts	Ensure communication and an efficient flow of information in the event of incidents
Protect critical components appropriately against access and physical intrusion	Closely monitor and control resilience measures
Conduct drills of response plans and emergency organisations	

Cybersecurity can be improved even with "simple" measures

Simple measures can often make a major contribution to improving cyber-resilience. For example, a well-structured organisation with clearly defined roles and responsibilities can have a positive impact on the implementation of security-related processes. Appropriate protection against unauthorised access to systems and/or unauthorised physical access to critical components significantly improves security. Ultimately, preparing for a possible attack is a type of lifeline to help rapidly resume the operation of critical infrastructures. Response plans and drills help with this recovery preparation.

Long projects and service lives, as well as outdated technologies jeopardise cybersecurity

Lengthy projects and the sometimes prolonged use of critical infrastructure facilities pose challenges in terms of cyber-resilience. Systems that are state of the art during planning are already outdated by the time they go into operation. While critical infrastructure systems can be used for several decades, the ICT components should be replaced every three to four years. Software components should be continuously maintained and updated with security patches. However, as ongoing renewal can be very costly and complex, it is often not carried out. This means that critical infrastructures tend to have outdated components, and the software is not always up to date and has known vulnerabilities. Such systems are easy targets for cyberattacks.

Critical infrastructure operators are required to keep critical infrastructure facilities and their ICT components up to date by means of architecture that is easy to maintain, systematic planning and consistent implementation of measures.

Protecting critical infrastructures is a joint, long-term task, and the necessary requirements are not sufficiently binding

Critical infrastructures are divided into sectors and sub-sectors. Depending on the sector, supervisory and regulatory responsibilities lie with the federal government or the cantons. Moreover, many critical infrastructures are operated by private companies. All of this makes it more difficult for the federal authorities to monitor operators. The flow of information, communication and ultimately a targeted, rapid response in the event of an incident are hindered.

The digital technologies used change quickly. Consequently, establishing and ensuring robust cybersecurity is an ongoing task, but it can be successfully performed only if all parties involved in CIP work together. The existing CIP requirements are currently incomplete and, in some cases, not binding enough. The sectoral supervisory and regulatory authorities are thus called upon to make the requirements more precise, so that the implementation of cyber-resilience measures can be imposed on critical infrastructure operators. At the time of the summary report, federal efforts were also under way to review the legal basis in the CIP area.