Audit of the effectiveness of incident management in protecting federal ICT from cyber-risks

National Cybersecurity Centre

Key facts

As the Confederation's specialist unit for ICT (information and communication technology) security, the National Cybersecurity Centre (NCSC) issues cybersecurity specifications within the Federal Administration, checks compliance with them and helps service providers to eliminate vulnerabilities.

The Ordinance on Protecting against Cyber-Risks in the Federal Administration adopted by the Federal Council entered into force on 1 July 2020. It provides the legal basis for the creation and expansion of the NCSC, and regulates the structure, tasks and powers of the authorities involved. The Ordinance grants the NCSC the power to take the lead in dealing with a cyberincident that jeopardises the proper functioning of the Federal Administration, after consulting the units concerned.

As part of this audit, the Swiss Federal Audit Office (SFAO) reviewed the effectiveness of the relevant process. In particular, the audit focused on issues relating to the timely flow of information from the sources to the NCSC, and on the merging of this information with the Centre's own monitoring results. In addition, the detection of cyberincidents and the timely implementation of measures, as well as the flow of information to the relevant units, was assessed.

The incident management process is clearly defined, published and applied. In general, the roles and responsibilities have been assigned but the role of IT security officer for the organisational units (ITSOO) must be strengthened. There is room for improvement as regards an overview of the participants when external service providers are involved. The framework conditions are generally appropriate but the communication channels and timeliness of reports must be improved.

Cyberincident reporting needs to be quicker

It is important that cyberincidents are reported immediately, to enable higher-level analysis and appraisal of the threat. This could allow the threat of a lateral spread across the entire Federal Administration to be contained or, at best, prevented. During the audit, the SFAO observed that communication with the NCSC needs to be expanded further. For example, horizontal management, especially the exchange of information between service providers, is not yet ensured in all areas. Moreover, the IT security officers of the departments must be informed more quickly.

The coordination/harmonisation of cyberincident categorisation also presents a challenge in cases where the incident affects more than one service provider. Where there is none, there is a risk that different service providers will assign different priorities to the same incident. Such a situation can also lead to inconsistent communication to third parties.

The role of the ITSOO should be strengthened and an overview of external service providers should be established

The ITSOOs have an important role in the reporting of cyberincidents: as service users, they report cyberincidents to their service providers, who in turn inform the NCSC. However, since there are different levels of maturity depending on the size of the service user, not all officers have assigned a deputy. Thus, in the ITSOO's absence, cyberincident reporting, and in turn the report to the NCSC, can be delayed. This situation should be corrected immediately.

In the event of a cyberincident, it cannot be ascertained quickly which applications and services from which provider, and for which administrative unit, need attention. As a result, when an IT security incident at an external service provider is reported, the affected administrative units cannot be informed immediately, which increases the vulnerability of the Federal Administration in general. Therefore, the creation of an overarching inventory should be considered.

Tools should be deployed more efficiently

The procurement of monitoring tools should be harmonised and centralised at Federal Administration level, to avoid the use of different tools with the same or similar functionalities. This would exploit economies of scale in terms of costs and knowledge base expansion.

Model contract clause must be optimised

The Federal Procurement Conference has drawn up a model contract clause on cyber-risks. The contractual provisions on information security are a step in the right direction. However, deadlines for reporting cyberincidents vary and would have to be defined in accordance with usual practice. Moreover, the clause would have to be renegotiated for long-term contracts.

Original text in German