February 16. 2026 | National Cyber Security Centre NCSC

Annual Report 2025

National Cyber Security Centre NCSC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
National Cyber Security Centre

Contents

Foreword

Dear readers

For the Federal Office for Cybersecurity (NCSC), 2025 was a year of consolidation and deepening of our mission. Following the start-up phase, we were able to further consolidate key processes and expand the cooperation within the Federal Department of Defense, Civil Protection, and Sport (DDPS) and with our partner organizations in a targeted manner. The structures we have created have proven their worth and enable us to perform our tasks reliably and consistently.

A major milestone was the introduction of the mandatory reporting of cyberattacks on critical infrastructures. Nine months after it came into force, it is visible that the implementation is working: cyberattacks are reported on time, the designated tools are used, and the cooperation with critical infrastructure operators has been established. Moreover, the proactive communication via industry associations and supplementary explanatory videos were particularly crucial for a smooth introduction. On this basis, Switzerland now possesses stable reporting and support processes in this security-relevant area.

The approximately 65,000 voluntary reports that the NCSC received in 2025 show that cyber risks are now on people's radar and that the latter are actively protecting themselves, staying informed, and reporting incidents. The reports obtained are a key factor in providing an up-to-date picture of the situation and enabling a better assessment of the threat level. On this basis, the NCSC can perform its task of raising public awareness in a more targeted manner and better tailor information and prevention measures to current needs and threats. Another focus was put on expanding the national digital platform, the Cyber Security Hub. In addition to the reporting form for critical infrastructures, improved functions and new exchange formats were introduced. The latter strengthen cross-sector cooperation and facilitate access to relevant specialist information. The controlling instruments of the National Cyber Strategy (NCS) were also further expanded: they comprise over 90 projects with partners from government agencies, industry, and society. In addition, the establishment of further sector-specific Cyber Security Centers (CSC), such as the "Healthcare CSC", strengthened the joint implementation of the NCS.

These achievements were made in a year marked by financial uncertainty. This makes the parliamentary decision to increase the NCSCs budget by CHF 10 million in 2026 and by a further CHF 5 million from 2027 onwards even more significant. We see the Parliament's decision as a strong sign of confidence in our work. It enables us to compensate for the existing underfunding, make necessary investments, and implement new legal tasks – particularly in connection with the reporting obligation – in a sustainable manner. At the same time, this decision comes with clear expectations: in terms of impact, reliability, and responsible use of the funds entrusted to us. We will continue to pursue our strategic course consistently. Our long-term goals remain unchanged but can now be achieved with greater reliability and at an appropriate pace.

I would like to thank all employees and our partner organizations for their commitment and constructive cooperation. Together, we are making an important contribution to cybersecurity in Switzerland.

Florian Schütz
Director of the National Cyber Security Centre

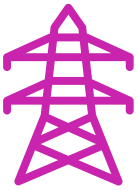
Key figures 2025

18.4 Mio. CHF
Expenditure
+ 38%

71
Employees
(including 4 university interns)
+ 5%

64’733
Voluntary reports of cyber incidents
+ 3%

501
Media contacts
- 19%



222
Reports of cyber-attacks within the scope of the reporting obligation
Newly introduced

2’347’618
Reports of devices infected with malware analyzed
+ 141%

1’600
Companies on the Cyber Security Hub
+ 45%

400
Average participants in the online bi-weekly situation exchanges
Newly recorded

525
Vulnerability reports from ethical hackers
+ 41%

17’468
Command and control systems of attackers identified and blocked
+ 115%

Compared to 2024

As of December 2025

Objectives of the NCSC

Vision

Cybersecurity is a joint task for politics, business, universities, and society. Many organizations and individuals find it difficult to assess and deal with cyber risks. A lack of transparency regarding the security of digital products leads to uncertainty among consumers and to vulnerabilities. Increasing interconnectedness means that inadequately protected systems can cause widespread damage.

The vision of the NCSC is to improve cybersecurity in Switzerland in close cooperation with all relevant stakeholders:

The NCSC lays the foundation for the secure use of digital services and infrastructures in Switzerland and enables Switzerland to become one of the leading countries in terms of secure digitalization.

Mission

The core mission of the NCSC is to strengthen the cybersecurity of critical infrastructures, the economy, education, the population, and public authorities by coordinating the implementation of the National Cyber Strategy (NCS).

To fulfill its core mission, the NCSC aligns its activities along four strategic pillars:

The four strategic pillars

1 Making cyber threats understandable

The NCSC breaks down complexity of cyber threats into tangible messages for its various audiences, in order to facilitate dialogue between government, business and society on cyber security. Thus, enabling all its partners to take active responsibility in reducing systemic risks.

2 Providing the means to prevent cyber attacks

The NCSC reduces the attack surface presented by Swiss individuals and organisations in cyberspace. It proactively warns organisations of breaches, and provides them with the requisite intelligence and tooling to help prevent incidents.

3 Limiting the damage from cyber incidents

The NCSC helps victims to limit the damage, as well as to minimise the risk of incidents propagating.

4 Increasing the security of digital products and services

The NCSC promotes business models, which incentivise manufacturers to offer products and services that are both secure and affordable. It promotes transparency for users so that they can make informed decisions about the cyber security of products and services.

Financial resources

Expenditure in 2025

In 2025, the final bill of the NCSC amounted to CHF 18.4 million. Of this, CHF 13.0 million was attributable to personnel expenses and CHF 5.4 million to material and operating expenses. Of the material and operating expenses, CHF 3.8 million was spent on IT. CHF 1.2 million of the latter was used for operations and CHF 2.6 million for further developments. The budget for further developments was increased by CHF 2.5 million using earmarked reserves. This provided the NCSC with sufficient funds to expand its existing IT-systems in view of the reporting obligation for cyberattacks on critical infrastructures introduced on April 1st, 2025.

CHF 1.8 million was spent on further developments at the Cyber Security Hub (CSH). A further CHF 0.1 million was spent on the analysis platform for cyber incidents (CyARC). CHF 0.5 million was used to implement bug bounty programs to identify and remedy vulnerabilities in the federal administration's IT systems. The remaining funds in the IT area were used for services for critical infrastructures and for cybersecurity audits in the areas of peripheral devices, photovoltaics, and open source.

Of the remaining material and operating expenses amounting to CHF 1.6 million, CHF 0.4 million was spent on external services. Of this, CHF 0.2 million was used for the further development of GEVER business processes and CHF 0.2 million for the development of an open-source target vision. Expenses for travel and participation in conferences amounted to CHF 0.3 million. The remaining funds were used for rental costs, office supplies, office equipment, and printed materials.

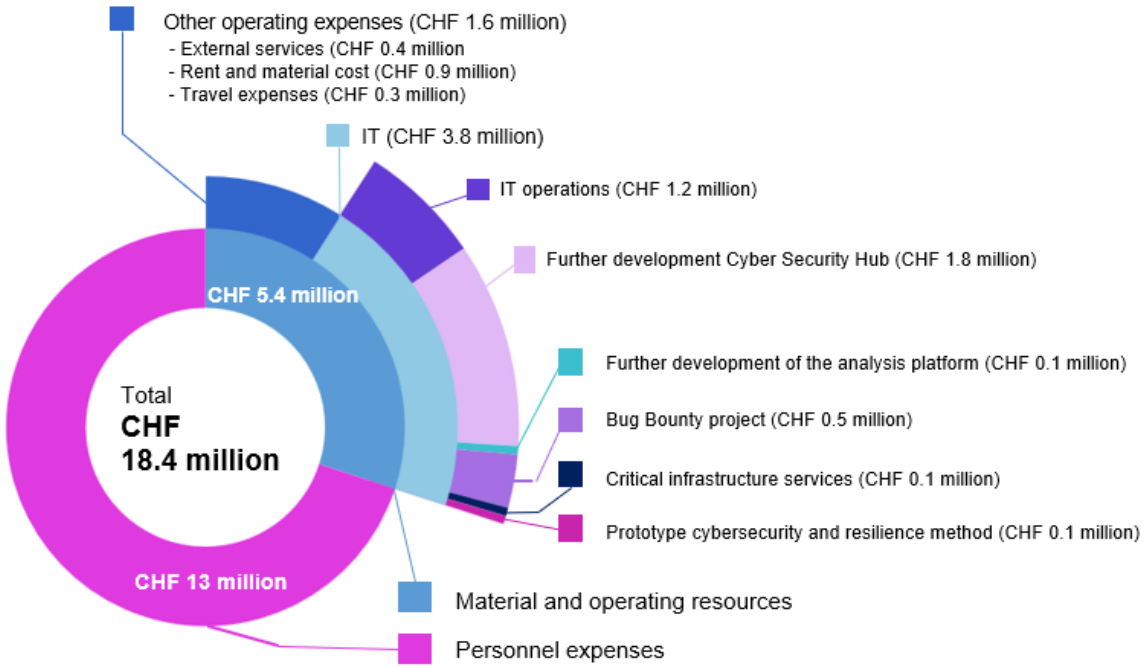


Figure 1: NCSC financial resources - invoice 2025

Use of financial resources by task

Most of the material and operating resources were used for the core mission of the NCSC. The funds were allocated to the prevention, handling, and follow-up of cyber incidents. Administrative expenses were kept to a minimum, amounting to 9 percent in 2025.

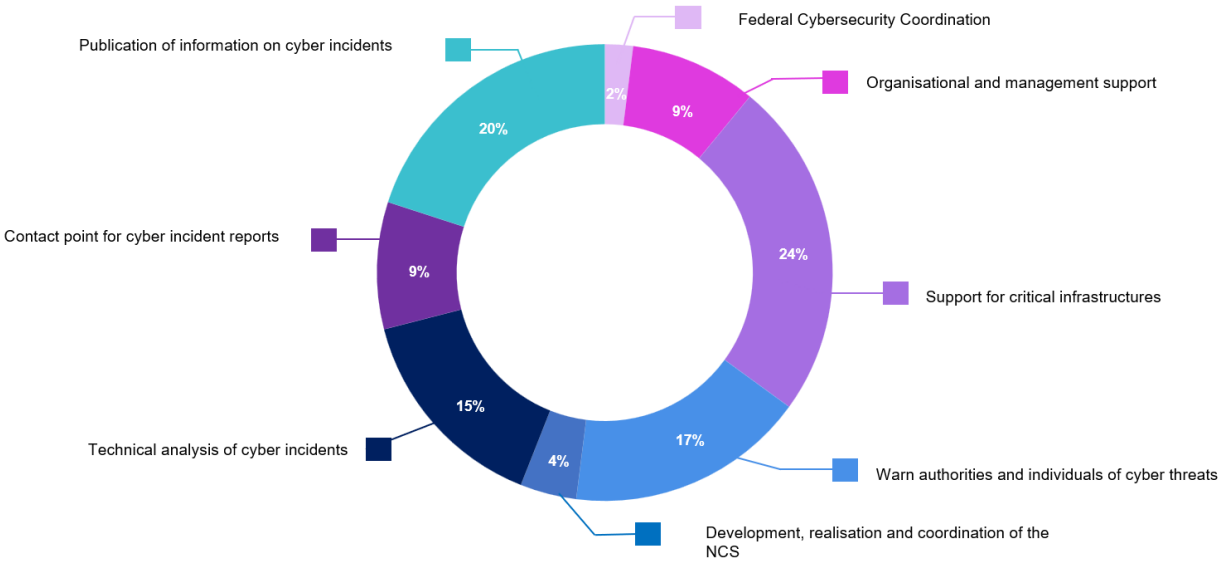


Figure 2: Distribution of financial resources by task

Personnel structure

Personnel expenses totaled CHF 13 million. This was allocated to 71 positions, including four university interns.

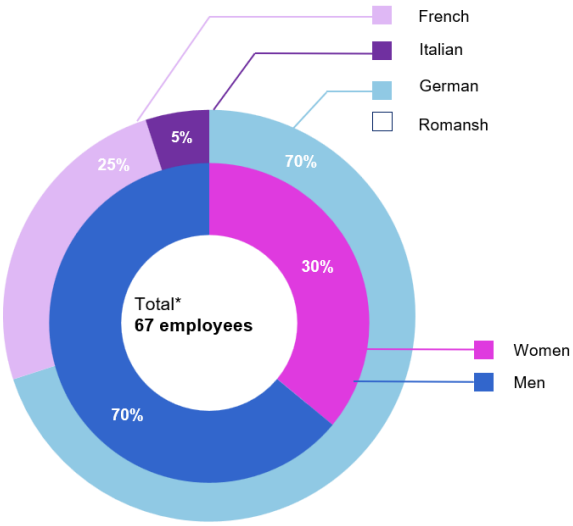


Figure 3: NCSC employees in december 2025
* excluding university interns

Activities of the NCSC based on the four strategic pillars

1 Making cyber threats understandable

One key objective of the NCSC is to enable its target groups to protect themselves effectively against cyber threats. In 2025, the NCSC therefore continued to focus strongly on preparing and disseminating information on cyber threats and possible protective measures in a manner appropriate to the target groups.

For public communication, the NCSC primarily uses its website, where it regularly publishes the latest warnings, weekly reviews, media information, and brief technical analyses. Various awareness campaigns were carried out for the public in 2025. The established "S-U-P-E-R" campaign continued as well. Thanks to its first appearance at the BEA 2025 public exhibition, the topic of cybersecurity was also brought to the attention of an even wider audience. As part of Cyber Security Month (CSM), this year's nationwide campaign focused on the topics of "online data" and "phishing." In collaboration with partner organization Netpathie and campaign ambassador Ivano Somaini, a wide range of content was created, including videos, quizzes, stickers, and an online "brown bag lunch" on the risks of oversharing and the conscious handling of digital data.

To support companies and communities, the NCSC also participated in numerous information and training events. Together with partners such as ITSec4KMU, the Swiss Insurance Association (SVV), and industry-relevant associations, practical specialist presentations, hacking demos, and workshops were held, emphasizing the importance of strengthening cybersecurity independently and the significance of secure supply chains.

Strengthening preventive cybersecurity

With the development of the Cybersecurity and Resilience Method (CSRM), the NCSC took an important step toward strengthening preventive cybersecurity in 2025. The method offers a practical approach to dealing with cyber risks, focusing on key business and production processes. It is based on extended basic protection, is aligned with international standards, and does not quantify risk. The cyber resilience assessment developed by the NCSC comprises a structured checklist that enables organizations to carry out a systematic self-assessment and will serve as a basis for comparison with other organizations.

The cyber resilience assessment is being tested under real conditions as part of a pilot project in the canton of Aargau with municipalities and companies in order to further develop the method and tool together.

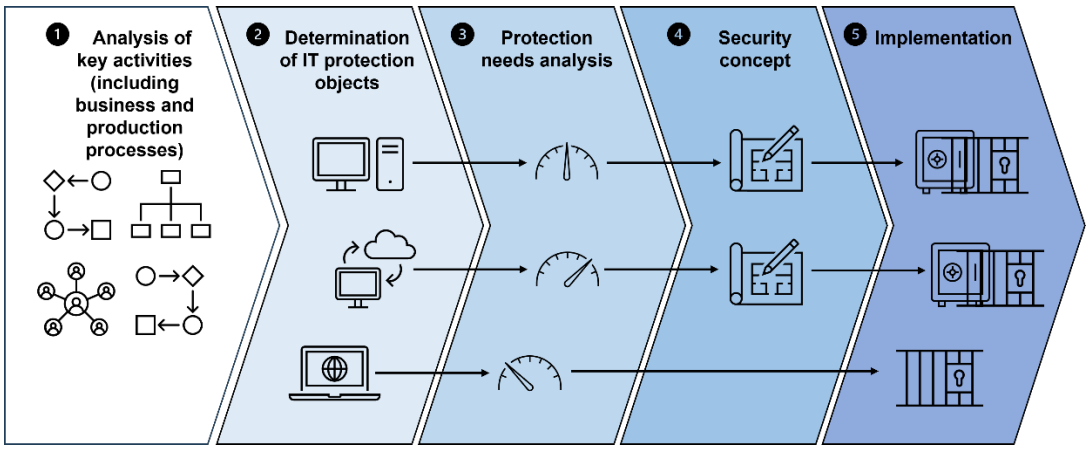


Figure 4: NCSC cybersecurity and resilience method

Cyber emergency response plan project for municipalities

Past cyber-incidents and the 2025 municipal survey conducted by "Myni Gmeind" have shown that many municipalities could be better prepared for cyber incidents. To help municipalities and organizations in Switzerland improve their cyber resilience, the NCSC and its partner network have developed an emergency concept model, practical tools, and an explanatory video, which have been published on the NCSCs website. The content was explored in depth in two online brown bag lunches.
Contingency plans are an essential part of effective risk management. They serve to proactively address potential problems and their effects rather than analyzing them after the fact. By addressing potential risks at an early stage, emergency plans enable preventive measures to be identified and implemented. They include crisis management, a crisis communication plan, key emergency contacts, and specific measures. These elements form the basis for a coordinated and appropriate response in time-critical situations.

Milestones and successes:
Development of a structured process:
The process developed (see infographic below) enables a pragmatic approach to preparing for, managing, and following up on potential cyber incidents.

Pragmatic implementation:
Thanks to the practical and pragmatic approach, the concept and associated tools could be quickly disseminated.

Knowledge transfer for SMEs:
The findings of the project not only benefit municipalities. From 2026, they will also be adapted and made available to SMEs.

Further development of the product:
A specialist group will continuously work on optimizing and supplementing the tools in order to integrate feedback from implementation and new cybersecurity requirements

Figure 5: Overview of the NCSC emergency concept

Implementation of the National Cyber Strategy (NCS)

In 2025, the focus was set on the operational implementation of the National Cyber Strategy (NCS). Building on the establishment of the steering committee in the previous year, the governance structures were further consolidated and specifically expanded for the implementation of the NCS in order to strengthen coordination between the numerous parties involved. To this end, regular exchange formats were created to promote dialogue and cooperation. A key result of this work is the design of an NCS implementation forum, which will be introduced in 2026. This forum will serve as a platform for reviewing progress in the implementation of the NCS, providing impetus for new measures, and supporting the strategic development of the NCS. An important step in this direction was the kick-off workshop in December 2025, which was attended by around 60 implementation partners. The aim was to design the future forum formats. The discussions underscored the high relevance of such platforms for the successful implementation of the NCS. The insights gained are now being incorporated into the preparation of the regular implementation forums planned from 2026 onwards.

Thanks to the further development of NCS portfolio management, the implementation portfolio now comprises over 90 projects supported by more than 70 implementation partners and covering all five strategic objectives. An overview of the active projects is available on the NCSCs website.[1] In addition, a clearly structured process for including new projects[2] has been developed and published so that interested parties are able to transparently understand the criteria for inclusion in the portfolio.

National Cyber Conference 2025

On September 25th, 2025, the Swiss Security Network and the NCSC organized the National Cybersecurity Conference (NCSK) in Bern under the theme "Cyber resilience: regulation or personal responsibility?" Around 250 participants from politics, administration, business, and science discussed the balance between legal provisions and self-responsible measures to strengthen digital resilience. The event provided a platform to exchange best practices and ideas for the further developing the NCS. Contributions from politics, research, and practice, as well as breakout sessions on regulation and personal responsibility underscored the shared responsibility of all stakeholders.

[1] Implementation of NCS
[2] New NCS Projects

2 Providing resources to prevent cyber attacks

Information exchange via the Cyber Security Hub (CSH)

The Cyber Security Hub (CSH) is the central platform for the operational exchange of information between the NCSC and the operators of critical infrastructures. In 2025, the technical expansion of the CSH was continued and consistently geared towards the reporting obligation under the Information Security Act (ISA). Since April 2025, a multilingual reporting procedure for cyber incidents has been available in the CSH, including initial reporting and final reporting. This has been integrated into the existing processes of the NCSC. In August, the "Share with NCSC" function was also activated. This enables additional information relevant to the assessment of the cyber threat situation or to measures for protecting critical infrastructures to be transmitted to the NCSC via a secure channel. By the end of November 2025, around 40 reports had been received via this channel.

The NCSC continued to use the established formats in 2025. In particular, these included the weekly cybersecurity report, which summarizes the most important events and developments on two pages and informs more than 6,000 users in around 1,600 organizations via the CSH. In addition, the NCSC continued its regular online exchanges on cybersecurity. There were 39 exchanges in German and French, with an average of just under 400 participants. These offer the CSH community a central platform for continuous dialogue, exchange on current developments and incidents, and networking between the participating organizations.

Cyber Threat Intelligence

In the area of cyber threat intelligence, the NCSC made significant progress in detecting and containing complex cyber threats. On a particular note is the identification and analysis of a large-scale ORB (“Operational Relay Box”) network. These are covert infrastructures used by state-sponsored actors to conceal cyber-attacks. The NCSC was able to identify a network of over 2,000 compromised systems and share the findings within the framework of international cooperation. This effectively limited the misuse of these systems.

At the same time, the NCSC observed an increasing threat to Switzerland from the group known as "Trader Traitor," which is believed to be backed by North Korean groups. Their activities are directed in particular against companies in the financial and crypto sectors. The attackers primarily use social engineering methods, contacting specialists in a targeted manner with supposed job offers and tricking them into executing malicious software.

The NCSC continuously monitors these threats and carried out several technical awareness-raising measures for partner organizations during the reporting year. By specifically disseminating warnings and technical indicators, the NCSC made an important contribution to preventing infections and strengthening the defenses of affected organizations.

Sector-specific initiatives

The Cyber Security Centers (CSC) program continued to be developed in 2025. The concept serves to pool industry- or sector-specific knowledge and link it to the NCSC. One focus was set on deeper cooperation between the NCSC and the Swiss Financial Sector CSC (FS-CSC). With a new cooperation agreement, both organizations are joining forces to specifically address the growing cyber risks in the financial sector. At the heart of the partnership is a structured exchange of information: FS-CSC analysts gain access to relevant NCSC data and use it to create situation reports and analyses for the financial center. These findings are incorporated into the work of the members and the CSH, strengthening the overall assessment of the situation. In addition to the financial sector, two further sector-specific centers have been established: the Healthcare-CSC and the Rail ISAC. Following completion of the pilot phase, the Healthcare-CSC was founded in August 2025 as an association comprising 18 hospitals. This promotes the exchange of threat information, joint protective measures, and best practices in the healthcare sector.

Figure 6: Signing of the new cooperation agreement with the FS-CSC

At the same time, a platform was set up with Rail ISAC to support the Swiss rail industry in defending against cyberattacks.

In addition to the CSCs, the NCSC promoted sectoral exchange with electricity supply organizations by holding two roundtables. These served to communicate the current threat situation and facilitate a moderated exchange between participants on sector-specific issues.

Contact point for cyber incidents

The NCSC receives voluntary reports from the public as well as companies in Switzerland via the contact point. In 2025, the NCSC received 64,733 reports, which enabled it to identify developments and new threats on the internet at an early stage and publish corresponding warnings. In addition, the NCSCs website reported weekly on the current threats thanks to the information provided in the voluntary reports.

Attempted fraud was the most frequently reported type of threat. Another clear trend was the change in the area of phishing attacks. While generic phishing emails continued to be detected, there is a clear trend towards increasingly personalized attack methods. In particular, there was a significant increase in fraud attempts in connection with online classified ads. In addition, telephone fraud and phishing attempts have also become more established. The language barrier, which was previously considered an obstacle, is playing an increasingly minor role. Another interesting finding is the increased use of artificial intelligence (AI) by criminal actors to make scams more realistic and convincing. AI is used particularly in the area of online investment fraud, for example to create fake interviews or professional-looking advertising content.

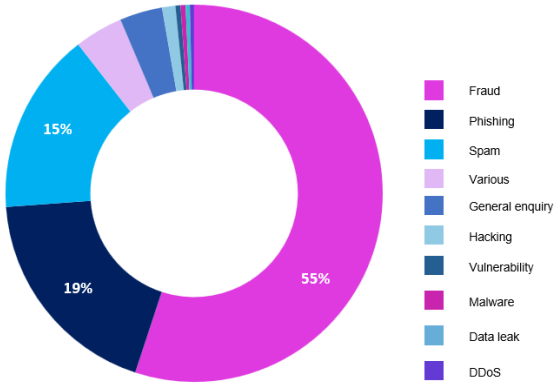
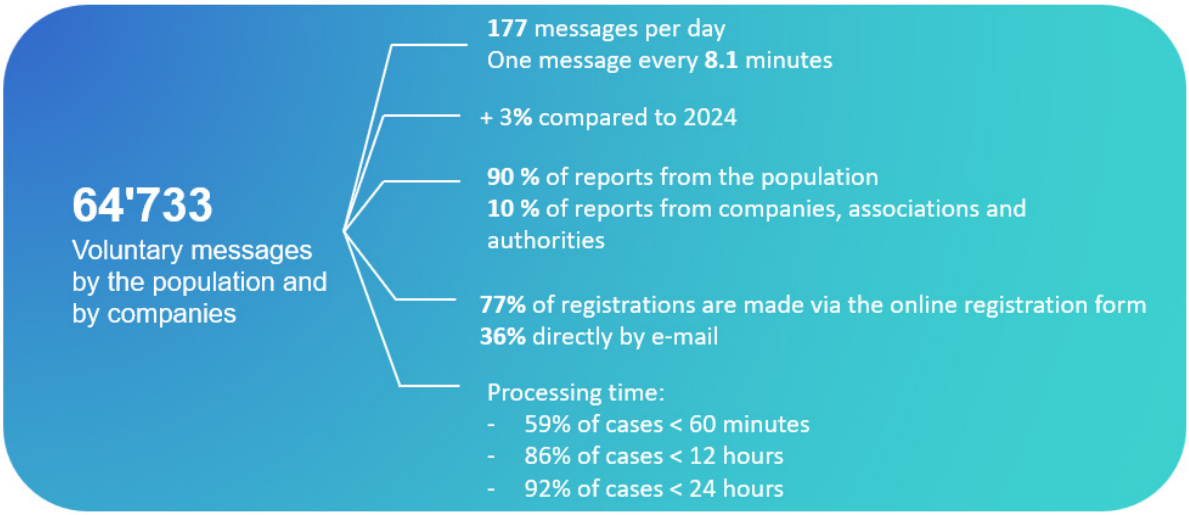


Figure 7: Voluntary reports by main category

Over the course of the year, the public reporting form was adapted to the changed requirements. The legal reporting obligation is now also fully integrated into the public reporting form. In addition, the option of redirecting reporters to the Suisse ePolice website, where online criminal complaints can be filed for certain offenses, has been improved. Communication with reporting people has also been optimized: the standard responses have been completely revised and are now more closely aligned with users' information needs. Internal processing procedures have been further optimized, reducing the average processing time per case.



Introduction of mandatory reporting

Since April 1, 2025, there has been a legal obligation to report cyberattacks on critical infrastructures in Switzerland. Operators of organizations subject to reporting requirements – for example, energy or drinking water suppliers, transport companies, or cantonal and municipal administrations – must now report cyber-attacks to the NCSC within 24 hours of their discovery. This new obligation was introduced by a revision of the Information Security Act (ISG) and is enshrined in Articles 73 ff. ISG. The reporting obligation is specified in the new Cybersecurity Ordinance (CSV), which also came into force on April 1st, 2025. The organizations subject to reporting requirements are specified in Article 74b ISG, while exceptions are regulated in Article 16 CSV.

In order to make the reporting process as simple as possible, the NCSC provides organizations subject to the reporting obligation with the Cyber Security Hub (CSH) (see Information exchange on p. 11) as a central reporting platform, as well as accompanying explanatory videos and information sheets. By the end of 2025, 222 reports had been received. The reports received enable the NCSC to improve its analysis of the cyber threat situation in Switzerland. This allows attack patterns on critical infrastructures to be identified and analyzed at an early stage, enabling potentially affected organizations to be warned in an appropriate timeframe in order for them to take preventive and defensive measures. Because the reporting form is provided on the CSH, there is an incentive for operators of critical infrastructures to register on the platform. The introduction of the reporting obligation thus promotes the general exchange of information and achieves an effect that goes beyond the fulfillment of legal obligations.

The most frequent reports came from public administration organizations, the information and communications sector, and financial and insurance companies. Analysis of the reported cases shows that the most frequently reported types of attacks are hacking (19.5%), followed by DDoS attacks (17.6%), and theft of access data (11.8%). Malware (9.5%), ransomware attacks (9.2%), and data leaks (8.8%) were also reported more frequently.

On October 1, 2025, the sanctions provisions also came into force, according to which fines of up to CHF 100,000 can be imposed for non-compliance with the reporting obligation after appropriate warning procedures. However, the first few months show that the organizations subject to reporting requirements are taking the new regulation seriously and fulfilling their responsibility for national cybersecurity.

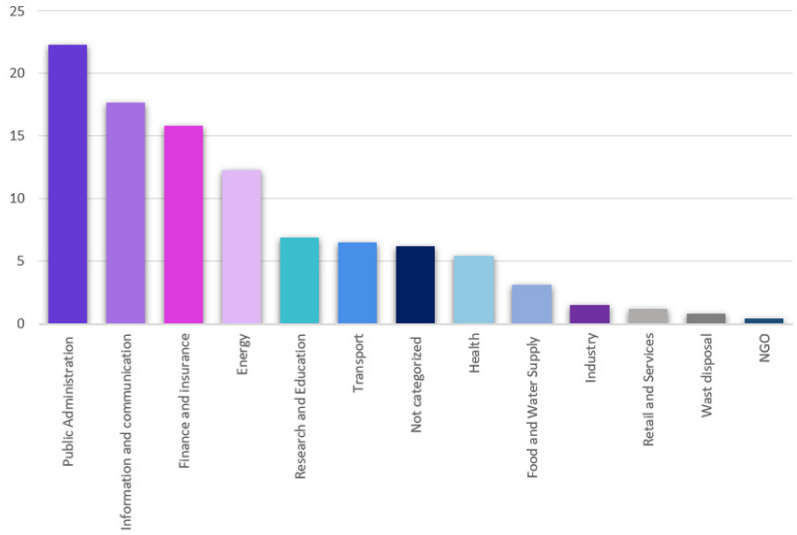


Figure 8: Processed attack reports per main sector in percent

3 Reducing damage from cyber incidents

Warnings about serious cyber threats via Alertswiss

In order to warn the population and businesses even more effectively about serious cyber threats, the NCSC has stepped up its cooperation with the Federal Office for Civil Protection (FOCP) and has also been able to publish warnings via the Alertswiss app and web platform since mid-September. This provides an additional channel for informing and warning the population as quickly as possible in the event of large-scale or novel cyberattacks and protecting them with specific instructions on how to respond.

Operations of the NCSC at major events

In 2025, the NCSC took on the central management of cyber security in the cyber situation network at three major events again: the World Economic Forum (WEF) in January, the Eurovision Song Contest (ESC) in May, and the UEFA Women's Euro in July. A core component of these operations was early warning and threat analysis: the NCSC evaluated indicators and reports, created threat scenarios, and issued timely warnings to operators of critical infrastructures so that they could take preventive protective measures. At the same time, operational support was provided, ranging from technical recommendations and incident response coordination to direct assistance in dealing with ongoing attacks.

The operations were carried out within the close framework of the cyber situation network and in intensive cooperation with event organizers, the police, and other federal authorities. Joint situation conferences, coordinated communication channels, and standardized reporting processes made it possible to shorten response times and secure information flows.

Information exchange

The MISP platform (“Malware Information Sharing Platform”) operated by the NCSC continued to be used in 2025 as a central tool for the automated exchange of technical information on cyber incidents. It supports the proactive protection of Swiss critical infrastructures by enabling the timely flow of information between national and international partners and the organizations involved. Technical information on 4,615 cybersecurity incidents (MISP events) was exchanged via the platform. This information came from both Switzerland and abroad. Moreover, the NCSC has newly integrated 30 operators of critical infrastructures in Switzerland into the MISP platform. In addition to the MISP platform, which is reserved exclusively for operators of critical infrastructures, the NCSC operates three other such platforms for other interest groups, such as cantonal and national police forces.

4 Increasing the security of digital products and services

Vulnerabilities in hardware and software remain key gateways for cyberattacks. The NCSC therefore focuses on the targeted testing of critical components on which the administration and economy rely. In the reporting year, the focus was on two areas: the federal administration's established bug bounty program and a pilot project on the security of open-source software.

Open Source

Open source software (OSS) already plays a major role in the secure operation of critical infrastructures, as the software used today often relies on OSS. To actively strengthen the security of OSS, the NCSC 2025, together with the National Cybersecurity Testing Institute (NTC), carried out a pilot project in which the applications "TYPO3" and "QGIS" were tested as examples. The investigation confirmed that relevant vulnerabilities also exist in established projects. These were remedied as part of the project in direct cooperation with the developer communities. The NCSC is now using these findings to develop the basis for long-term support for OSS security by the federal government.

The NCSC has also introduced a binding open-source strategy and established "open source by default" as a working principle. In doing so, the NCSC is strengthening the interoperability and innovative capacity of its products and creating an open basis for projects, architectures, and procurements.

Bug Bounty

The federal administration's bug bounty program has established itself as an efficient tool and an indispensable addition to traditional security testing. Ethical hackers test the federal government's systems according to clearly defined rules. Since bounties are paid out exclusively for technically validated vulnerabilities with a demonstrable impact, the model is extremely cost-efficient. Financial resources are thus targeted where real risks exist.

The bug bounty program regularly identifies relevant and critical vulnerabilities that are not always detected in conventional tests. In 2025, the NCSC received a total of 525 reports of potential vulnerabilities. After analysis and review, 328 reports were recognized as valid and led to measures to remedy or improve security in the federal administration. A total of around CHF 260,000 in rewards was paid for these reports.

The NCSC is continuing the bug bounty program and is committed to establishing such programs as an established instrument of information security in Switzerland.

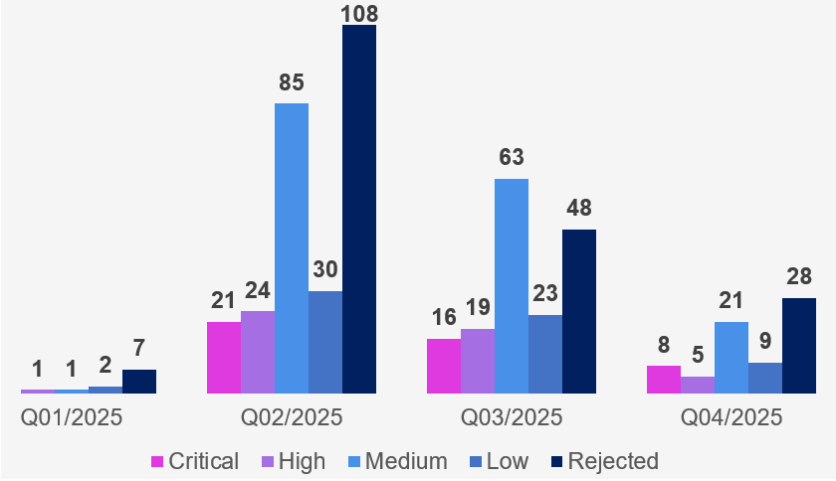


Figure 9: Reported vulnerabilities and their classification

Impact management NCSC

As part of its operating concept, the NCSC is constantly developing and optimizing its planning and control instruments. Particularly, it focuses on creating transparency and traceability and in the overall context of the Federal Administration.

The NCSCs impact management brings the basic mandate and all associated core activities of the Federal Office into a structured and aligned process and provides insight into the various levels of impact. The output provides information about the services and products provided by the Federal Office, while the outcome and impact focus on the medium- and long-term effects to be achieved among the respective target groups and sections of society. All impact chains are managed consistently in the organizational portfolio and linked to programs, projects, and other initiatives in line with the core activities of the Federal Office.

The coordinated and targeted implementation of strategic issues within the framework of the statutory mandate continues to be carried out at the Federal Office in accordance with the OKR methodology ("Objectives & Key Results"). The consistent quarterly prioritization, planning, and management of the necessary financial, human, and time resources associated with OKR, as well as the associated controlling in the form of reviewing the achievement of results, ensure successful strategy implementation. Following its introduction last year, the 2025 management method has been further established. Among other things, particular focus is placed on coordinated cooperation while promoting team autonomy within the NCSC.

Taken as a whole, impact management provides a holistic view of the Federal Office's activities. It contributes to orientation, highlights connections and allows changes to be identified at an early stage and responded to in a targeted manner. It thus forms the basis for learning-oriented, impact-oriented action and supports the NCSC in continuing to fulfill its mandate in a reliable, transparent and targeted manner in the future.

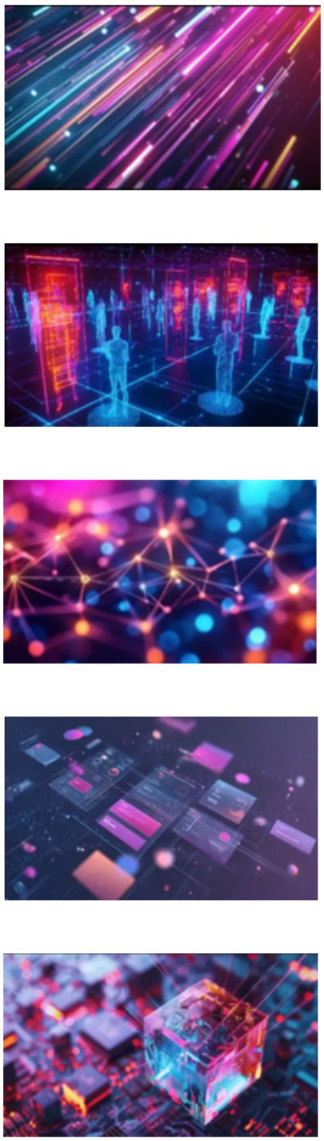


Figure 10 – 14: OKR NCSC

Publications

NCSC publications in 2025:

- Emergency planning is the key to cyber resilience
- First implementation report on the National Cyberstrategy (NCS)
- Technology consideration: Quantum computers and post-quantum
- Technology consideration: Cybersecurity and resilience
- Technology consideration: Passkeys
- Press releases NCSC
- Measurability and testability of IT security
- Technology Brief: Confidential Computing
- Technology Brief: Cloud Computing
- Technology consideration: SCION
- The weeks in review
- Semi-Annual Report 2024/2
- Semi-Annual Report 2025/1
- Open-Source-Strategy NCSC (available only in German)

Scientific articles

A. Grünert, J. B. Michael, R. Oppliger, and R. Rytz, “On the measurability and testability of IT security,” *Computer*, vol. 57, no. 3, pp. 120–126, Mar. 2025, https://ieeexplore.ieee.org/document/10896924