28 March 2025 | National Cyber Security Centre NCSC

Annual report 2024

National Cyber Security Centre NCSC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Contents

Foreword

The National Cyber Security Centre (NCSC) looks back on its first year. Thanks to the new structure as a federal office, it has been possible to optimise and stabilise the services built up as the NCSC in the Federal Department of Finance (FDF). We are still a small federal office and often face the challenge of having to manage many tasks simultaneously with few resources. However, with innovative approaches, a great deal of commitment from all employees and investments in digitalisation, we have succeeded in further increasing our output and making our services available to a wider audience.

We have now laid the foundations for fulfilling our legal mandate and can scale up our services. This is important as the demands placed on the federal office by society, the economy and politics continue to increase. The threat situation in the cyber area continues to grow. The shift from globalisation to regionalisation, the fragmentation of regulation between economic areas and the increasing use of cyber as a tool for asserting interests have a direct impact on the cyber security of the economy and society.

The dialogue with other countries shows that Switzerland can play an important role in this area. The NCSC strategy is often cited as a good example, the work of the NCSC and its employees is appreciated and the way in which we conduct challenging operations with our national and international partners attracts interest beyond national borders.

However, navigating the many challenges and take due account of the wishes and ideas we receive from the business community, universities, cantons and politicians, remains an ongoing challenge. We have to make sure that we do not get sidetracked and ensure that we always deliver our day-to-day operations to the usual high standard. Furthermore, we must be ready to expand our services, if this is desired and financed.

I am proud that we have managed to offer a wide range of services while maintaining a high standard of quality. This is demonstrated by the positive feedback we receive from our partners and from the public. The next two to three years will be decisive for our further development. I look forward to working with the NCSC staff and all our partner organisations to shape cyber security in Switzerland. I also hope that politicians will set out as clearly as possible what services are expected of us, to what extent and what resources we can draw on.

The NCSC is motivated to utilise the opportunities so that Switzerland can continue to be a reliable player in the cyber sector for the benefit of the economy, society and the authorities.

Florian Schütz, Director of the National Cyber Security Centre

Key figures

13.3 million CHF Expenditure

63
Employees

62'954
Voluntary reports of cyber incidents

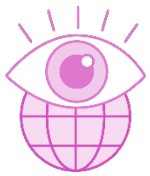
616
Media contacts

1'100
Companies on the Cyber Security Hub

991'309
Reports on devices infected with malware

371
Reports of vulnerabilities by ethical hackers

38
Weekly Cyber Situation Briefings



7
Awareness-raising Campaigns

8'116
Command and control systems identified and blocked by attackers

Status December 2024

Aims of the NCSC

Vision

Cyber security is a shared responsibility by government, business, academia and society. Many organisations and individuals find it difficult to assess and deal with cyber risks. A lack of transparency about the security of digital products, leads to uncertainty among consumers and to vulnerabilities. Due to the increasing connection of networks, extensive damage can occur, as a result of inadequately protected systems.

The NCSC's vision is to improve cyber security in Switzerland in close cooperation with all the 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 digitalisation.

Mission

The core mission of the NCSC is to strengthen cyber security in critical infrastructures, the economy, the education system, the population and in government, by coordinating the implementation of the National Cyber Strategy (NCS).

To this end, its services are built on 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

In financial terms, the year 2024 was marked by the transformation into a federal office and the imminent introduction of the reporting obligation.

Staggered recruitment and the postponement of planned IT projects resulted in a budget shortfall. These will be used to create earmarked reserves for the coming years, which will help to press ahead with the most important projects even when the budget is constrained.

Expenditure in 2024

In 2024, the NCSC's final accounts totaled CHF 13.3 million. Material and operating expenses equaled CHF 2.6 million. Of the CHF 1.9 million spent on IT, CHF 0.4 million was spent on operations and CHF 1.5 million on further developments. A significant portion of the IT expenditure was allocated to the establishment of the new reporting centre for cyber attacks on critical infrastructures. CHF 1 million was spent on the further development and expansion of the Cyber Security Hub (CSH). Not listed are the costs of federal service providers, which were borne by the General Secretariat of the Federal Department of Defence, Civil Protection and Sport (GS-DDPS). Around CHF 0.35 million was used to carry out bug bounty programs to identify and mitigate vulnerabilities in the Federal Administration's IT systems. CHF 0.33 million was used for projects implementing the National Cyberstrategy (NCS), including the development of an analysis platform for cyber incidents and awareness-raising measures.

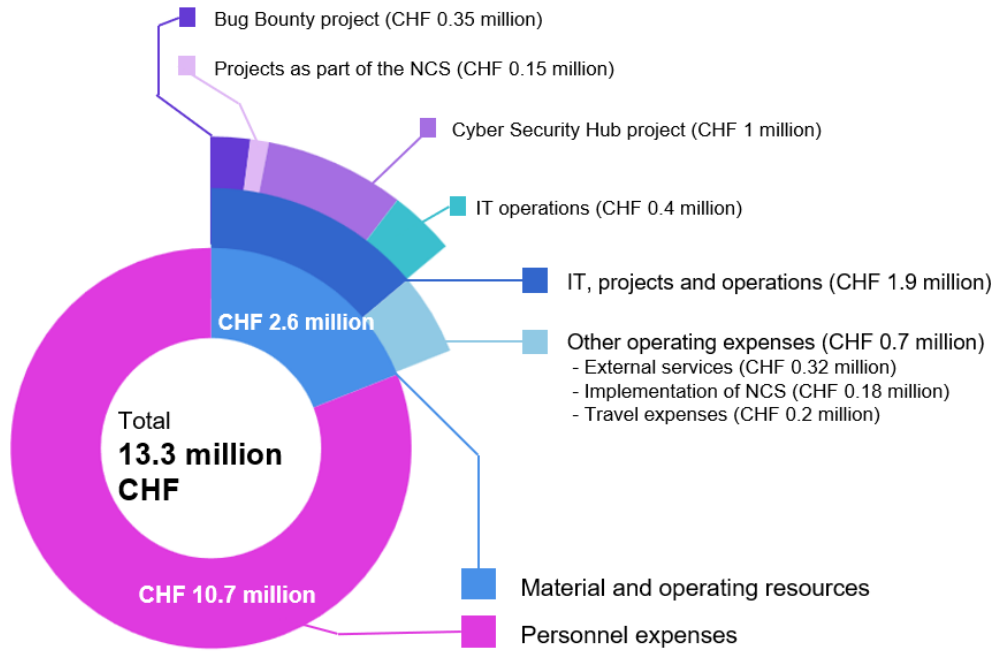


Figure 1: NCSC financial resources - invoice 2024

Use of financial resources

Most of the material and operating resources are channeled into the prevention, handling and follow-up of cyber incidents (88%). They are therefore used within the core mission of the NCSC. Administrative expenses are kept as low as possible, amounting to 8 per cent in 2024.

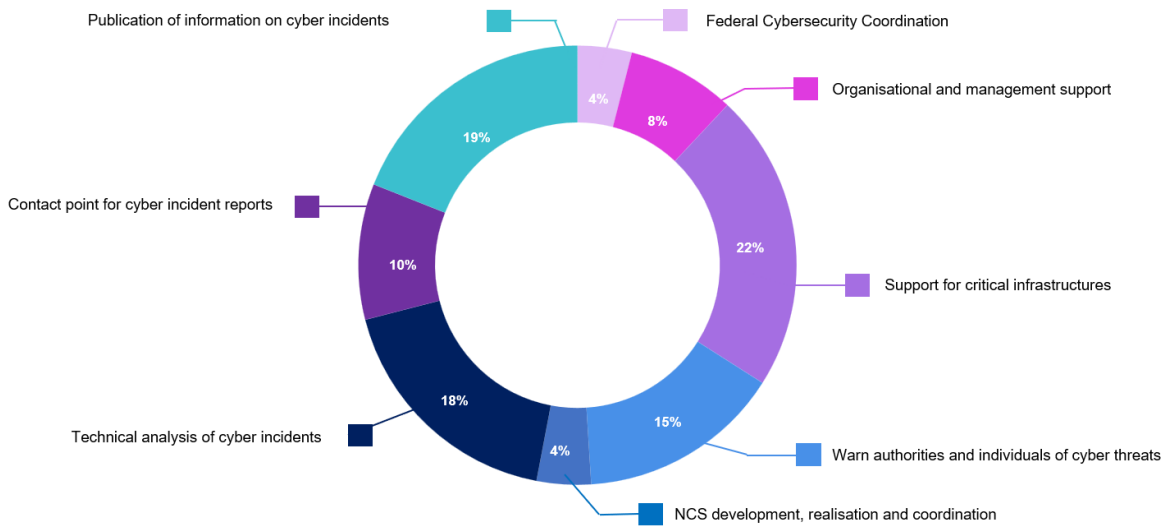


Figure 2: Distribution of financial resources by task

Personnel structure

Personnel expenses totaled CHF 10.7 million. Over the course of the year, NCSC was able to recruit 24 new employees. The Incidence Response Team was significantly strengthened. The increase in personnel was already planned at the time of the transfer to a federal office and took place in view of the introduction of the reporting obligation for cyber-attacks on critical infrastructure. To promote young talent and give them a valuable insight into cyber security, the NCSC has specifically recruited university interns to support us in our projects.

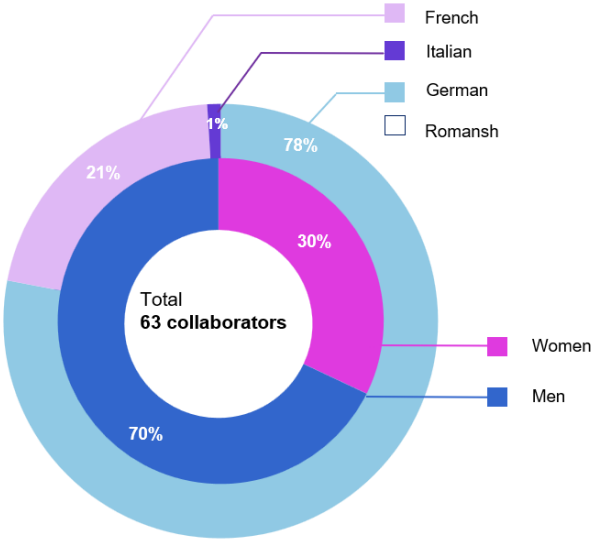


Illustration 3: NCSC collaborators in December 2024

Management method

Objectives and Key Results

The NCSC has been working according to the OKR methodology (Objectives & Key Results) since the 4th quarter of 2024. The introduction of and conversion to an NCSC-oriented OKR framework was carried out gradually, in line with requirements and administrative structure and organisational principles of the NCSC.

The planning and management tool ensures that all organisational areas at the NCSC work in a coordinated and targeted manner on a quarterly basis to implement strategic priorities and within the framework of its legal mandate. The application of the methodology strengthens the autonomy of the team, involves employees at all hierarchical levels in both the planning and implementation phases, and provides a clear framework. By creating transparency and traceability as well as a smooth flow of information within the entire organisation, the methodology also contributes to the further development of the NCSC culture.

Following the pilot phase, an initial positive effect has already been observed. The introductory phase has been completed, and the OKR methodology has been an integral part of the management tools in the NCSC since the start of 2025. The planning and management tool continues to require special attention to be optimally embedded in the structures and processes of the Federal Office in the overall context of the Federal Administration.

Objectives Q4 2024

- O1 - Interested individuals and organisations find out about the services available from the NCSC.
- O2 - The NCSC creates the starting point to position itself internationally.
- O3 - The NCSC recognises the benefits of its work.
- O4 - Switzerland's systemically important sectors are supported in their cyber security by the NCSC.

Figure 4: Visualised objectives Q4

NCSC activities based on the four strategic

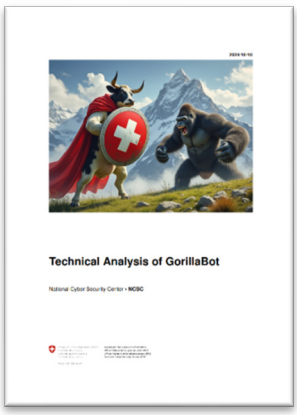
1 Making cyber threats understandable

In 2024, the NCSC has continuously and purposefully shared information about cyber threats to the economy, the authorities and the public. This information helps to strengthen protection against cyber threats in a targeted manner. As a communication channel to the public, the NCSC uses its website, where it publishes current warnings, weekly reviews and brief technical analyses. In addition, the biannual reports help to provide a comprehensive overview of the most important cyber security events and developments and to derive strategic recommendations for action.

The NCSC also contributes to a better understanding of cyber security through awareness-raising campaigns. With the SUPER Campaign 2024 and the European Cyber Security Month, the NCSC and partner organisations have addressed the general public. Specific campaigns were also organised for individual target groups, such as municipal authorities.

Preventative cyber security

In addition to providing information on cyber threats, the NCSC also strengthens prevention through the development of methods and training courses as well as publications and presentations that provide targeted support to decision-makers from across the economy, administration and politics. The core elements of this work are the minimum standards for ICT security and the recommendations and best practices. The NCSC develops these principles in close coordination with internationally recognised standardisation organisations. In 2024, the NCSC focussed on the development of principles for the integration of post-quantum cryptography and the improvement of security procedures in companies. The NCSC published results in internationally renowned journals, among others. NCSC publications, in particular the critical estimation on the use of probabilities for risk management and safety standards, has been met with international interest and contributed to a transparent and critical exchange in the field of cyber security.



"Cyber security in the supply chain" pilot project

In 2024, the NCSC, together with Planzer Transport AG, conducted a pilot project on cyber security in the supply chain. The aim was to pool expertise and resources from the industry and cyber security to develop a structured approach and practical tools to improve the cyber security of companies along the supply chain. The tools are intended to support companies in systematically identifying, assessing and managing cyber security risks in the supply chain.

The successful pilot project emphasises that cyber security is not a one-off project, but an ongoing process. Thanks to the close cooperation of all those involved, it was possible to develop a solution that contributes to increasing security in the supply chain in the long term.

Milestones and successes

Development of a structured approach: The approach developed (see diagram below) enables continuous improvement of the cyber security in the supply chain.

Pragmatic implementation: The practical and scalable approach made it possible to implement the concept quickly and gain the commitment of the associations..

Challenges overcome: The biggest challenges included defining a common approach, creating a standardized language and resource planning for parallel and overlapping activities.

Knowledge transfer for SMEs: The findings of the project will not only benefit the logistics and transport sector, but will also be made available to other SMEs in Switzerland from 2025.

Further development of the product: A specialist group will continuously work on optimising and expanding the tools in order to integrate new cyber security requirements.

Figure 5: Measures to protect against cyber attacks in the supply chain

Implementation of the National Cyberstrategy (NCS)

The current National Cyberstrategy (NCS) was approved by the Federal Council and the cantons in April 2023. In 2024, the implementation of the NCS continued to be driven forward and coordinated by the NCSC with the aim of strengthening national resilience to growing cyber threats. Implementation is supported by a Steering Committee. The NCS Steering Committee`s role was expanded to enhance its independence, strategic reach, and overall effectiveness. The Committee met for the first time in June 2024 and following its establishment, formed five working groups along the five strategic objectives of the NCS to take an in-depth look at the NCS and to assess upcoming priorities.

In September 2024, the NCSC organised the National Cyber Security Conference in collaboration with the Swiss Security Network (SSN). The conference focused on the topic of "Geopolitics and Operational Security". The conference helped to deepen the exchange of knowledge and national cooperation and emphasised the joint commitment of all stakeholders to implementing the objectives and measures of the NCS. Over 280 people from industry, academia, cantons and federal agencies attended. 93 per cent of participants rated the event as good or excellent (net promoter score (NPS): 59).
The NCSC plays a central role in the implementation of the NCS and, with the work presented in this report, makes a significant contribution to the implementation of all five strategic objectives, specifically across 15 of the 17 measures. More information on the implementation of the NCS will be published in the first NCS progress report in Spring 2025.

Figure 6: Goals and measures NCS

2 Provide means to prevent cyber attacks

The exchange of information on current threats, attack patterns and possible countermeasures is a key element in the prevention of cyber attacks. The NCSC therefore sees itself as a platform for this exchange of information and works to ensure that relevant information on cyber attacks flows together centrally, is analysed and results made available to all interested organisations as recommendations for action.

Exchange of information about the CSH

Since autumn 2022, the NCSC has been operating the Cyber Security Hub (CSH) This platform serves as a tool for the exchange and management of information on cyber threats, cyber incidents, vulnerabilities and cyber security practices.

In 2024, the CSH has been developed into a more powerful, user-friendly and efficient platform. The improvements help to ensure that organisations in Switzerland are better protected against cyber threats. This is also reflected in the fact that the number of CSH users increased from 1,000 in 2023 to 3,300 in 2024.

The companies registered on the CSH are informed about the current cyber threat situation via a weekly online exchange. Around 350 cyber security specialists take part in these events every week. (Net Promoter Score (NPS): 60).

Sector-specific initiatives

The exchange of information is also being developed through sector-specific cyber service. To this end, the NCSC supports the establishment of Cyber Security Centres (CSCs) in various sectors and communities. CSCs are sector-specific competence centres for preventative cyber security measures, information exchange, threat analyses and awareness-raising measures as well as incident management. CSCs work closely with the NCSC but also consider the requirements of the sectoral players. In particular, the NCSC acts as the central coordinator and operator of the national CSH. The vision of the NCSC is to organise all critical sectors in sectoral CSCs. Already established CSCs include the FS-CSC with the financial sector and the Swiss Industry Cybersecurity Association (SWICYBA - CSC). The Rail-ISAC and Healthcare-CSC are in the implementation phase. The concept of the IG-CSC with NGOs from International Geneva is ready and will be implemented according to available resources.

Other initiatives relate to the organisation of sector-specific roundtables with critical infrastructures.

Cyber Threat

The NCSC provides the operators of critical infrastructures with technical information on current cyber threats (so-called "cyber threat intelligence") and exchanges information with the operators of critical infrastructures.

The NCSC received 975,309 reports of suspicious websites via the antiphising.ch platform, from which over 20,000 phishing websites were identified. In addition, the NCSC received almost 1,000,000 reports of infected devices such as smartphones, computers or IoT devices and sent them to the respective operator or the responsible internet provider. Finally, the NCSC was able to identify 8,116 servers used by cybercriminals to control devices infected with malware.

Importantly, the exchange of technical information on cyber threats also takes place across borders. This enables timely tracking of the cyber threat situation. In addition, technical information can be shared quickly and appropriately, enabling a rapid response to new cyber threats. For example, in 2024, the NCSC was able to use technical analyses to identify key findings on a sophisticated spear phishing attack against European countries and warn the affected countries promptly through established channels.

An analysis platform was also developed as part of a proof of concept through a public-private partnership, which allows information on systemic cyber risks to be exchanged and analysed. Four different information suppliers from the private sector provide different information on cyber incidents at an organisational, personnel and technical level, which is analysed by the NCSC. In future, the NCSC will use this information to create products that will contribute to improving the overall cyber resilience in Switzerland.

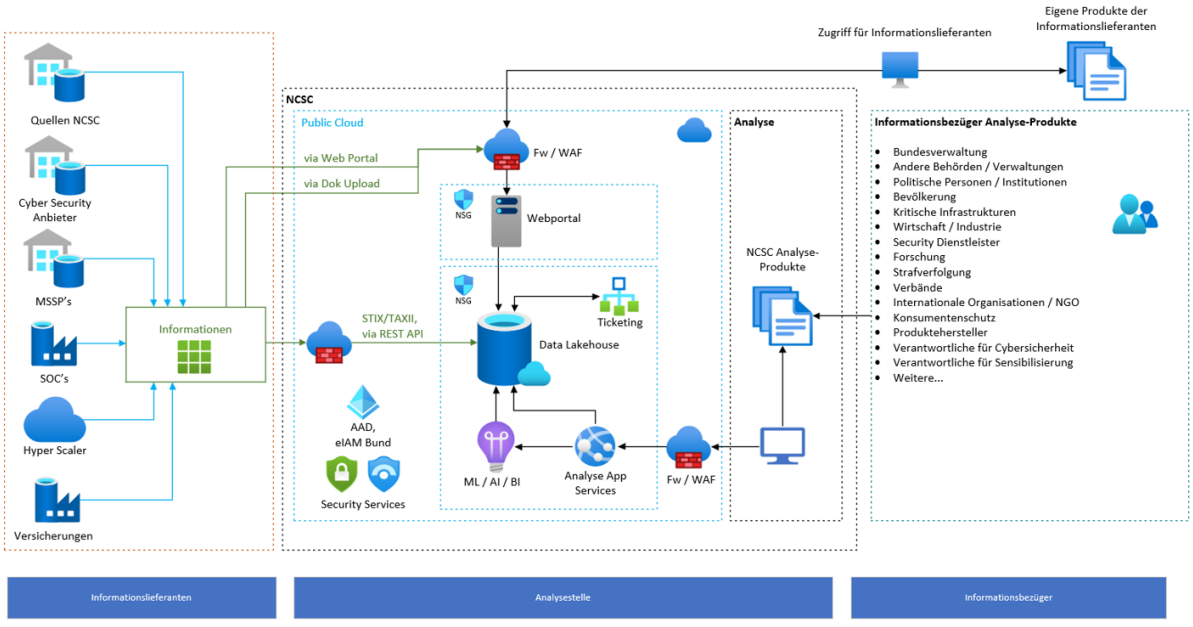
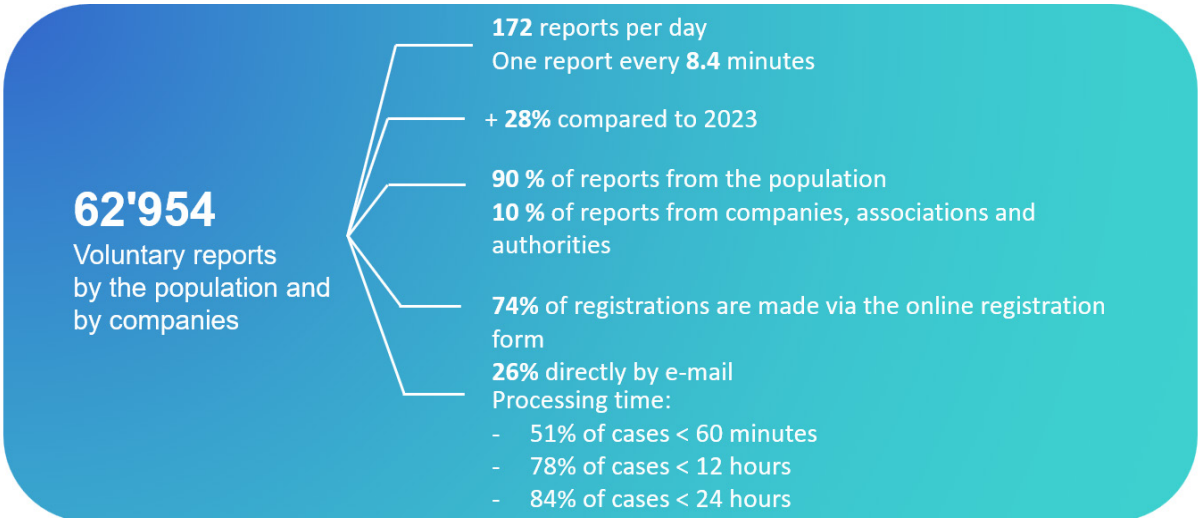


Figure 7: Logical architecture of Cyber Analysis, Research & Collaboration (CyARC)

Contact point for cyber incidents

In addition to sharing information about cyber threats to critical infrastructures, the NCSC operates a contact point for cyber incidents aimed at the public and small and medium-sized enterprises (SMEs). Through these voluntary reports, the NCSC is able to recognise possible trends in cyber threats and can publish warnings accordingly. On its website, the NCSC provides statistics on reported cyber incidents and summarises the most interesting cases in its weekly review.



Among the most frequently reported fraud offences by companies, there was a sharp increase in the phenomenon of CEO fraud, with a total of 716 reports received.

Reports of ransomware incidents fell slightly in 2024. While 109 incidents were reported in the previous year, 92 were reported in the current reporting year.

The reporting form was revised in April 2024 in order to cope with the ever-increasing number of incoming reports with the same resources, but also to provide a better service to those reporting incidents.

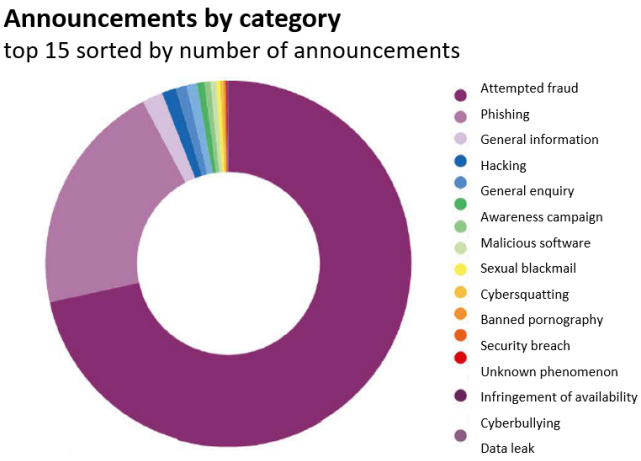


Figure 8: Voluntary reports by category

3 Reduce damage from cyber incidents

The NCSC not only analysed threats, but also supported operators of critical infrastructures, the administration and Switzerland as a business location in dealing with cyber incidents. The NCSC took over the operational management of cyber incidents across the Confederation. To this end, the NCSC operated an on-call organisation so that technical experts could be reached by telephone around the clock (24/7). The support provided by the NCSC helped to contain the damage and prevent the incident from developing further. Further work that arose after the attack, such as the reinstallation of computer systems, had to be carried out by the affected companies without the help of the federal government through which subsidiarity was maintained.

In 2024, the focus in terms of incident management was on operations against cyber threats at specially exposed events. Several such events took place in 2024. For example, the annual meeting of the World Economic Forum (WEF) and the high-level conference on peace in Ukraine on 15 and 16 June 2024. Several cyber attacks occurred during these events, but they were quickly dealt with thanks to good preparation. In addition to the overall coordination of countermeasures, the NCSC was also responsible for preparing risk analyses, vulnerability assessment of key infrastructures (attack surface management), awareness-raising among all those involved, threat intelligence and mitigation, working in close cooperation with all partners. At this point, we would like to emphasise how well the collaborations worked, as events such as these have shown. There have been several requests from abroad for Switzerland to demonstrate how such events can be adequately protected in a short space of time.

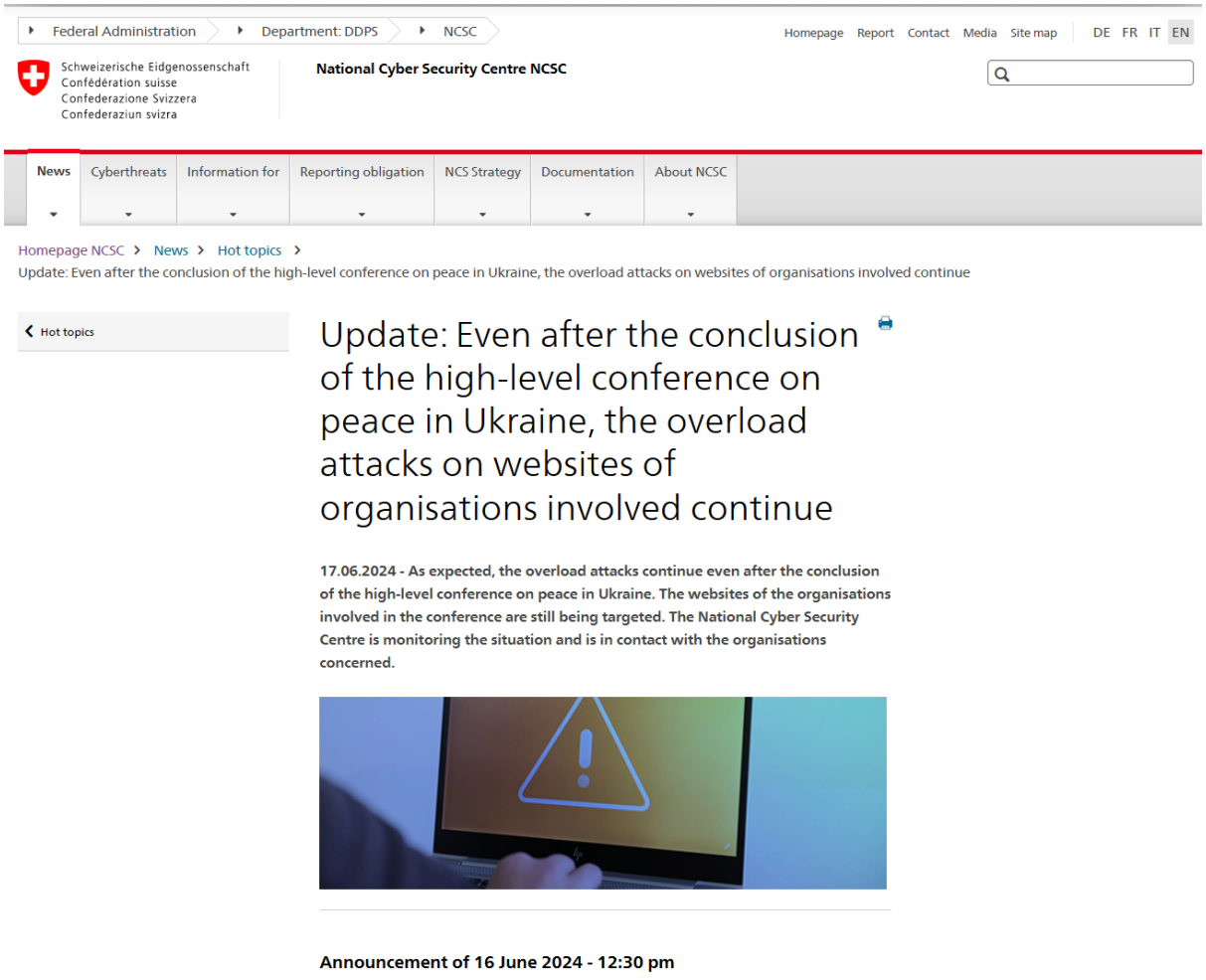


Figure 9: Situation update during the conference on peace in Ukraine

4 Increasing the security of digital products and services

Vulnerabilities in technical devices, hardware and software remain the most common entry points for cyber incidents.

To support the economy and the population with this issue, the NCSC has set two priorities: Firstly, the NCSC is the official "CVE Numbering Authority" in Switzerland, where researchers can report vulnerabilities in products. The NCSC acts as an intermediary between reporters and product manufacturers to ensure that vulnerabilities are fixed as quickly as possible, and assigns a unique number that makes the vulnerability uniquely identifiable worldwide.

Secondly, the NCSC manages the Federal Administration's bug bounty programme to strengthen the cyber security of its IT infrastructure.

The NCSC also strengthened its collaboration with the National Test Institute for Cybersecurity (NTC), an initiative of the Canton of Zug. The NTC tests IT products for security vulnerabilities if no one else does.

Bug Bounty

The implementation of bug bounty programme in the Federal Administration increases the cyber security across its IT infrastructure and reduces cyber risks effectively and cost-efficiently. In 2024, the NCSC received a total of 371 reports of vulnerabilities from ethical hackers. Of these, 239 were classified as valid following technical analysis and a total of CHF 250,900 in bounties were paid. All departments and the Federal Chancellery were affected by the identified vulnerabilities. 12% of the valid vulnerabilities, a total of 45 reports, classified as "critical", i.e. highly critical vulnerabilities, and therefore were treated with the highest priority within the federal administration and remediated without delay. A further 51 vulnerability reports were assessed as "high". Security vulnerabilities of that category represent a considerable risk for the Federal Administration and, like the critical cases, also require a great deal of attention, as the potential damage in the event of exploitation is equally considerable. The remediation process must therefore also be initiated as quickly as possible for these cases to reduce the attack surface for cyber criminals. A further 102 vulnerabilities were assessed as "medium". Finally, the remaining 41 incoming reports were distributed across the less critical "low" category.

The bug bounty programme had to be paused in September 2024 as the available budget had been used up. The bounties were mainly financed by the return of central digitisation funds within the Federal Administration.

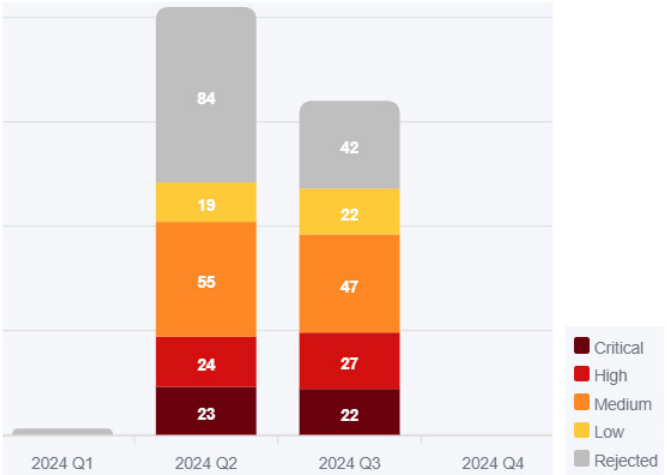


Figure 10: Number of reports on vulnerabilities

Outlook and goals for the coming year

In 2025, the NCSC will face both significant opportunities and challenges in the area of cyber security. The requirements in this dynamically growing sector are constantly increasing, which is why it is crucial to deploy the available resources in a targeted manner and set clear priorities. With a planned budget of CHF 16.1 million and earmarked reserves, which allow financial resources to be carried forward to the next year, current projects can be continued in 2025. No significant investments in the NCSC are planned in the current financial planning. At the same time, it can be assumed that cyber threats will continue to increase, particularly in view of the challenging geopolitical environment. The NCSC's approach to this challenge is twofold:

1. Focus: The NCSC prioritises tasks according to cost/benefit regarding Switzerland's short and medium-term cyber security.

2. Platform: The NCSC acts primarily as a hub and amplifier for contributions from partners. Wherever possible, the NCSC acts as an enabling and coordinating body and closes capability gaps where they exist.

Clear priorities in a growing environment

As a result of its dual tactics, the NCSC will focus on three key areas of action in 2025:

1. Further development of the digital platform: The digital platform forms the backbone of the NCSC's cyber security strategy. Its continuous improvement is crucial to effectively counter changing cyber threats.

2. Implementation of the National Cyberstrategy (NCS): The consistent implementation of the NCS remains a core task to ensure Switzerland's long-term security in cyberspace. The first NCS Progress Report will be published in Spring 2025 and will assess the progress made to date.

3. Reliable execution of operational business: The quality and reliability of operational activities are of central importance to the NCSC. The focus is placed on operational and tactical activities with short to medium-term impact, with strategic long-term projects being selectively managed at this time.

Increased efficiency through internal optimisation

In addition to focusing on these core areas, the NCSC will also continue to optimise its internal structures. The aim is to make processes more efficient through automation, to further simplify cooperation with partners and to focus even more on coordination. This will enable the NCSC's overall performance to be improved so that, at least in the medium term, it will be able to respond to growing cyber risks with consistent quality.

Long-term perspective and partnerships

The NCSC will continue to do everything in its power to achieve the best possible results with the resources available and to make Switzerland safer in 2025. In doing so, it can count on broad support of partner authorities and the private sector. The basic mandate remains unchanged: To fulfil its role as a coordinator and to provide high-quality services for the economy, society, authorities and science.

The NCSC would like to thank everyone who is committed to cyber security and helps us to fulfil our mission.

Publications and references

NCSC publications in 2024:

- Half-year report 2023/2
- Half-year report 2024/1
- Report: Telephone fraud in the cyber sector
- Brief technical analysis of the "Gorilla" botnet
- Brief technical analysis of the "Poseidon Stealer" malware
- Report on the data analyses following the cyberattack on the company Xplain
- Anti-Phishing Report 2023
- Technology review: quantum computers and post-quantum cryptography,
- Assessment of the need for action in connection with post-quantum cryptography (PQK)
- Federal IT Security Report 2023
- Recommendations for the security screening of persons in companies
- Cyber resilience measures in the context of major events and international conferences
- NCSC' initial assessment of the work of the Cyber Situation Network in connection with the high-level conference on peace in Ukraine

Scientific articles

- A. Grünert, J. B. Michael, R. Oppliger and R. Rytz, "Why Probabilities Cannot Be Used in Cyber Risk Management," in *Computer*, vol. 57, no. 10, pp. 86-89, Oct. 2024
- R. Oppliger and A. Grünert, "How to Measure Cybersecurity and Why Heuristics Matter," in Computer, vol. 57, no. 2, pp. 111-115, Feb. 2024