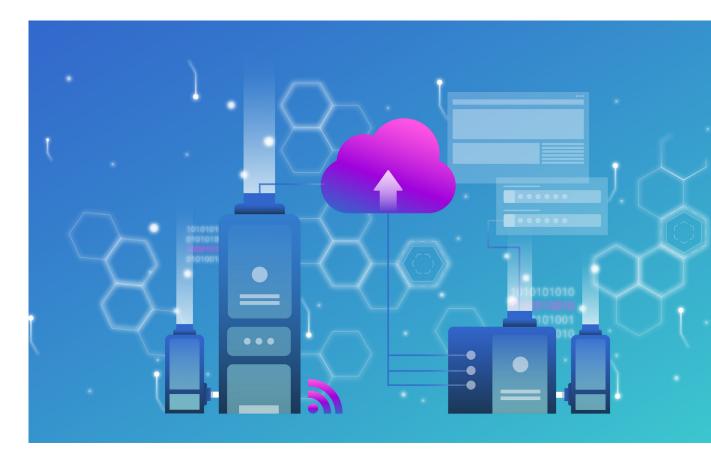
6 May 2024 | National Cyber Security Centre NCSC



# Strategy of the 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 NCSC

# **Overview / Contents**

1	Introduction: Challenges for cyber security in Switzerland	3
2	The NCSC's vision	4
3	Mission: The four strategic pillars of the NCSC	4
	3.1 Making cyber threats understandable	5
	3.2 Providing the means to prevent cyberattacks	5
	3.3 Limiting the damage from cyber incidents	6
	3.4 Increasing the security of digital products and services	6
4	The NCSC's operational model	7

## **1** Introduction: Challenges for cyber security in Switzerland

Switzerland currently faces the following main challenges in relation to cyber security<sup>1</sup>:

- High vulnerability of businesses, authorities, academia and the general population to cyberattacks;
- Insufficient ability to respond to systemically relevant cyber incidents and crises;
- Low maturity of digital products and services, in terms of cyber security and lack of quality control mechanisms thereof;
- Only selective understanding of all aspects of cyber security in business, society and politics;
- Lack of transparency and data, in order to assess information on cyber security and deriving respective political and economic measures in response;
- Limited protection of actors, which are not considered critical infrastructure;
- Lack of coordination and legal grey areas between official and private cyber security instruments.

These challenges lead to cyberattacks often being successful and causing serious economic damage, as well as posing a high risk of failures in national critical infrastructures.

Reports of cyber incidents resulting in damage have risen by around 30% annually in recent years. The number of reports from non-critical infrastructures has roughly tripled in the last 12 months. In 2023, the NCSC processed 187,000 phishing reports and identified, as well as shut down 8,223 websites in Switzerland that were used for phishing. In several hundred cases reported, the NCSC has detected malware in critical infrastructures and has worked with the companies concerned in eliminating it. On average, every 40 hours the NCSC is called on, to provide support in dealing with a malware infection.

SMEs in particular are increasingly being targeted by cyber criminals. Attackers use ransomware attacks to encrypt and steal data. They then demand a ransom for decrypting and preventing publication of the stolen data. These attacks are highly automated, which is why it takes little effort for criminals to attack even small businesses. In Switzerland, around 75% of all businesses generate less than CHF 500,000 in sales per year. It is particularly difficult for these businesses to invest in cyber security. They rely on digital products and services being developed and maintained securely, and on security services being available at low cost.

But the general public is not immune to cyberattacks either. Here, cyber fraud is the main concern. Growing anxiety and a need for information and support are clearly noticeable.

At the same time, Swiss universities and innovative companies are producing attractive cyber security solutions. However, bringing these to the market or even creating global standards is proving a challenge.

<sup>&</sup>lt;sup>1</sup> Based on the <u>effectiveness review 'National Strategy for the Protection of Switzerland against Cyber Risks</u> <u>2018</u> <u>to 2022'</u> the <u>National Cyber Strategy (NCS)</u> and the weekly reports and case statistics of the contact point, GovCERT and OIC.

## 2 The NCSC's 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 foundations for the secure use of digital services and infrastructures in Switzerland and enables Switzerland to become a world leader in secure digitalisation.

### 3 Mission: The four strategic pillars of the NCSC

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 strate-gic pillars:

Making cyber threats understandable Providing the means to prevent cyberattacks Limiting the damage from cyber incidents

Increasing the security of digital products and services

#### 3.1 Making cyber threats understandable

The NCSC breaks down the 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.

One of the questions most frequently asked by managers of businesses and other organisations, as well as members of the public is: "What can we do to protect ourselves from cyberattacks?" Cyber security is also a topic frequently discussed by politicians.

Decision-makers are constantly faced with the challenge of assessing cyber threats and identifying counter-measures.

The NCSC collects information on the various aspects of cyber incidents; it identifies correlations, pinpoints areas where action is needed and topics for discussion, and makes recommendations. In this way, the NCSC enables an informed dialogue about cyber threats to take place and empowers all stakeholders to meet their responsibilities, as to reducing systemic risks. The NCSC's analyses provide a basis, on which providers of cyber security solutions can improve their services and products in a needs-based manner.

#### **3.2 Providing the means to prevent cyberattacks**

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.

Cyberattacks require preparation. This means that the attackers analyse targets for vulnerabilities, either develop malware themselves or purchase it, eventually launching their initial access attacks. Most attackers use similar methods and approaches. The NCSC can identify the methods used by attackers and share related information and warnings with partners and potential victims. The information ranges from technical details relating to the attack vectors, to findings on how a particular attacker selects its targets. This information can be used to warn the organisations concerned so they can increase their protection accordingly.

Reducing exposure to attack is even more important than early detection. Three factors significantly weaken cyber security: 1) vulnerabilities in systems, 2) misconfiguration of systems and 3) incorrect use of systems.

The NCSC reduces the attack surface of systems used by Swiss individuals and organisations by encouraging the early detection and elimination of vulnerabilities. It warns of attacks and provides information on how to ward them off. In order to prevent large-scale attacks with potentially systemic effects, the NCSC uses technological instruments in a targeted fashion and works with the relevant authorities to draw up regulations on the protective measures required.

The NCSC develops technologies for detecting and responding to threats. It provides this service, when no other suitable products are available on the market or the risk situation justifies market intervention. In-house developments for detection and defence are made available as open source software/methodology whenever possible.

#### 3.3 Limiting the damage from cyber incidents

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

Cyber incidents cause various types of damage. The damage depends on the business model or the personal situation of the victim. In addition, there is often a risk of the damage spreading in the event of a cyber incident. Firstly, attackers can use the victim's network to attack other targets. Secondly, malfunctions triggered by cyber incidents can cause considerable damage to third parties.

Damage can be reduced, if the effects of cyber incidents are limited in terms of time and disruption caused. First and foremost, the NCSC is committed to preventing systemic dangers, which jeop-ardise the functioning of the state. This does not only cover system failures, but also major economic damage that can have a significant impact on the gross domestic product (GDP). The NCSC supports victims in dealing with incidents, by providing specialist advice and organisational support. Depending on the potential extent of the damage, support services range from consulting to full cyber crisis management, including technical defence and recovery measures. In principle, the NCSC provides services to private individuals as a secondary line of defence. This means that victims must first cope with an incident on their own, whenever possible, or by calling on services from the private sector.

The NCSC creates national and international structures, which facilitate coordination in the management of cyber incidents. The NCSC takes the lead in incidents that affect multiple authorities in Switzerland. The NCSC also helps organisations and private individuals to be optimally prepared, to deal with a cyber incident by providing documents and recommendations on best practices.

#### 3.4 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.

Security researchers have found that almost every application has at least one security-relevant vulnerability. Even hardware is not immune to flaws, which compromise cyber security. Such faults cannot be completely avoided given the complexity of today's ICT systems. However, the majority of issues can be avoided or quickly recognised and eliminated, by having a well-structured development process, and by conducting tests over the entire product life cycle. Greater investment in cyber security inevitably makes products more expensive. Secure products however, will always have to compete with more cheapely assembled products. It is often unclear to the consumer, how secure a product is and whether a higher price really stands for more security.

The NCSC supports and develops initiatives and models, which create transparency in regard to the cyber security of products and that will support a beneficial market for secure products. Examples of these initiatives and models range from labelling schemes to regulatory proposals, incentives and financing models.

## 4 The NCSC's operational model

In order to implement this value proposition as efficiently as possible, the NCSC consolidates and aggregates existing content and information, ensures their quality and conveys them between service providers and recipients in a needs-based fashion.

The NCSC is committed to the cooperation model set out in the NCS and works closely with the cantons, the private sector and universities. The aim of this collaboration is, to pool expertise and to provide mutual support so that the protection against cyber threats can be optimised.

The NCSC creates original content and only provides services itself, if no adequate third-party services are available, if such services cannot be used for the benefit of all, or if they have to be provided directly by the federal government, due to legal requirements or for reasons of confidentiality. In particular, the NCSC also sees itself as an "incubator" that initiates new services for, which there is a need. It will transfer these services to other organisations, as soon as they have reached a certain maturity and can be provided by another body in a better way.

Where possible, the NCSC provides its services in digital form, based on the platform model. Direct services are only provided where absolutely necessary, particularly in connection with incident management support and aspects of awareness-raising. Focusing on the platform model makes it possible to scale the NCSC's services with a manageable use of resources.

To this end, the NCSC has set up and operates a self-service platform, which provides access to information on cyber threats, specific and general recommendations and resources for prevention and information sharing.