Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

How can the NCSC help me increase my resilience?

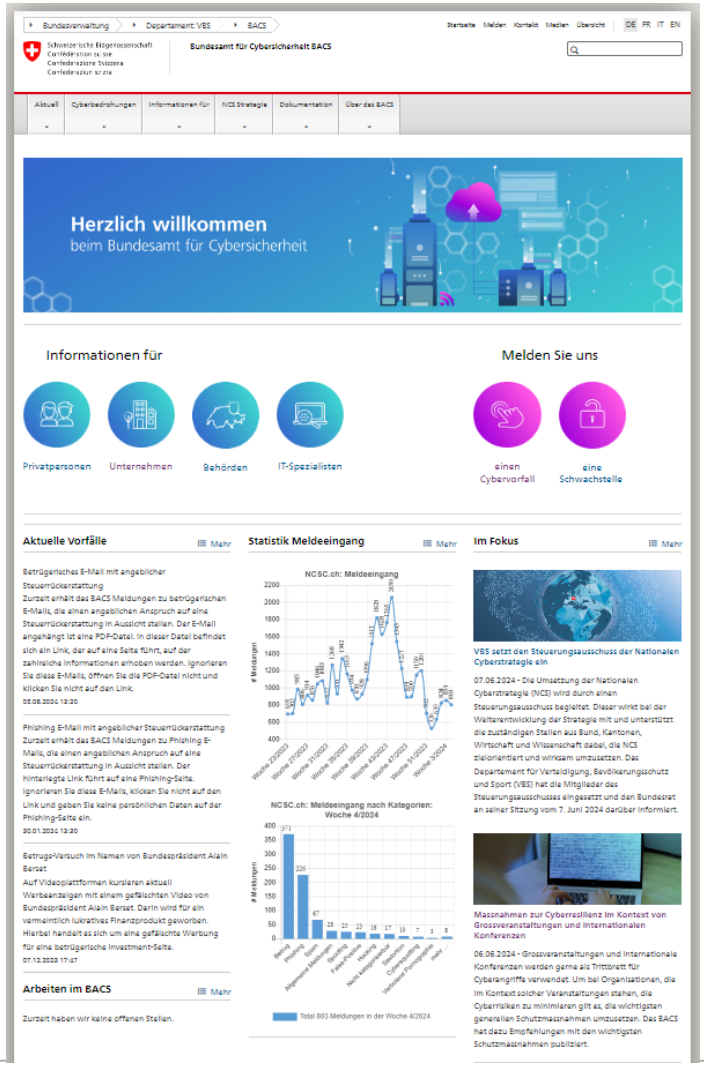
June 11th 2024 // Monica Ratte

National Cyber Security Center (NCSC)

The National Cyber Security Centre is the **federal government's competence centre for cybersecurity** (and new federal office since 1 January 2024) and thus the first point of contact for businesses, public services, educational institutions and the population when it comes to cyberissues.

It is responsible for the coordinated implementation of the national cyberstrategy (NCS).

➢ https://www.ncsc.ch/



National Cyberstrategy NCS

The national cyberstrategy (NCS) was approved by the Federal Council on 5 April 2023 and by the cantons on 13 April 2023. **The strategy sets out the objectives and measures with which the federal government and the cantons, together with the business community and universities, intend to counter cyberthreats**. A steering committee will be established to plan and coordinate the implementation of the strategy, and will also refine it. Its role is to be expanded and its independence increased.

2.1.2 Strategic objectives

Secure digital services and infrastructures: Switzerland implements measures nationwide to strengthen cyber-resilience. The Confederation and cantons create the necessary conditions to ensure that a high level of protection is guaranteed, that secure digital infrastructures, products and services are used, and that risk appetite is consciously managed.

Follow the news

National awareness campaigns

S-U-P-E-R.ch

Who am I?

Information for

Individuals

- Buying and selling online
- Child and youth prevention
- Nine practical tips for secure mobile phone use
- …

Companies

- Cooperation with IT service providers
- Do you have your payment processes under control?
- Home Office - Secure use of remote access
- …

Authorities

- E-learning on cybersecurity and information security for towns, cities and communes
- …

IT Specialists

- Security in the Internet of Things (IoT)
- Measures to protect industrial control systems (ICSs)
- …

Incident discovered?

NCSC

What's your report about?

- An email/a text message/a WhatsApp message
- A phone call
- Social media
- A computer/a smartphone/a tablet/a system
- An online advertisement (goods, job) or an online purchase
- A website/a web service/a web platform
- Financial damage
- Extortion
- Report directly

Suisse ePolice

For certain offences, it is possible to file a online criminal complaint. You cannot file a complaint via Suisse ePolice if you are resident in one of the following cantons: AG, BS, GE, JU, NW, OW, SH, SO, TI, UR, VD, VS.

I would like to file a criminal complaint

Me

An email/a text message/a WhatsApp message

I would like to report another case

I am prompted to click on a link

I clicked on the link

I am prompted to log in

I logged in

Phishing

Criminals use phishing to lure victims into providing their passwords and other personal information.

learn more ...

Fraudulent email concerning alleged tax refund

learn more ...

Phishing: This incident applies to me - I would like to report it

Measures – Phishing

As soon as you realise that you have entered your password on a phishing site, change this password for all services where you use it. If you provided credit card details, contact your...

Show all measures ...

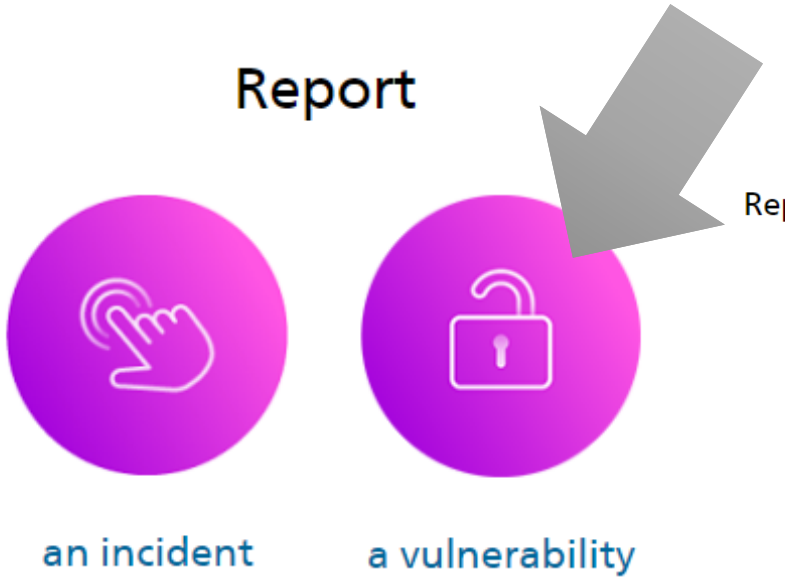
The measures listed help me and I would like to support the NCSC and report the case

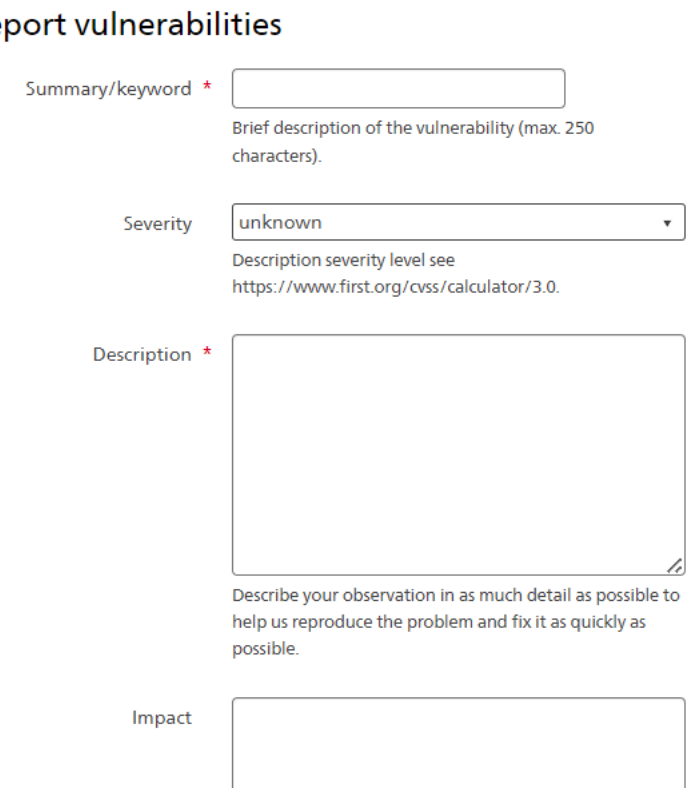
back

NCSC

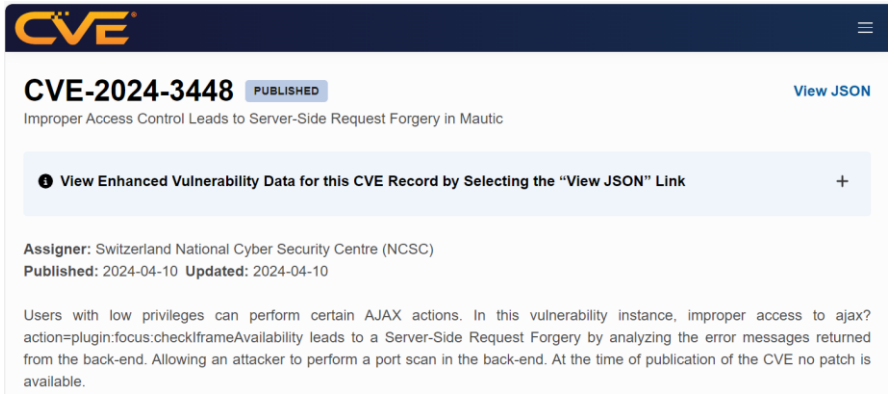
Further information will help us to deal with the case (The communication of contact details is voluntary).

Vulnerability discovered?

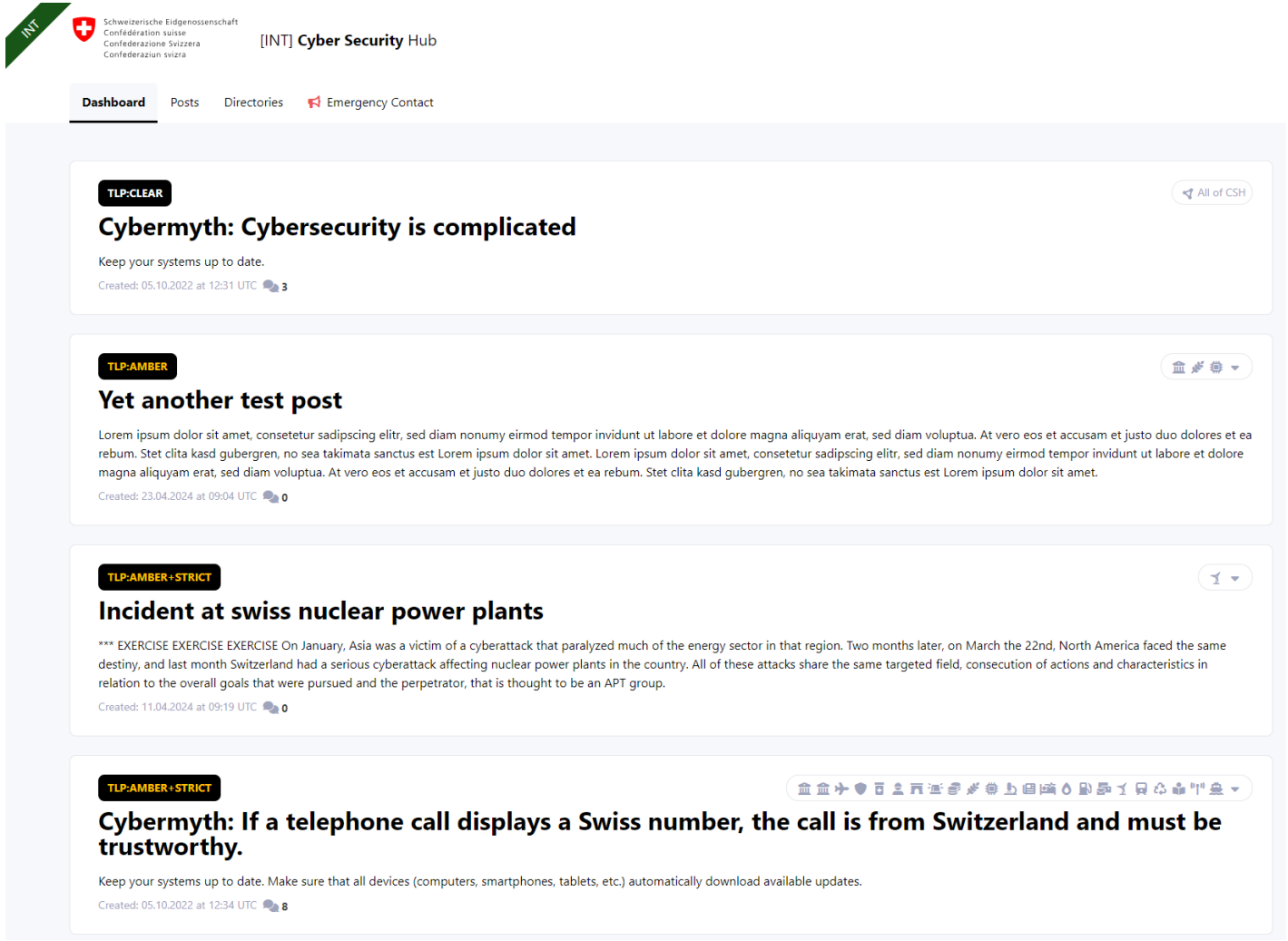




The NCSC was recognised by the competent independent US organisation, MITRE as a **CVE Numbering Authority**. In this role, the NCSC is responsible for preparing and publishing information about the vulnerabilities reported to it and the associated CVE records. The NCSC is the official contact point for reporting security vulnerabilities in Switzerland, but also maintains their CVE IDs for international exchange.



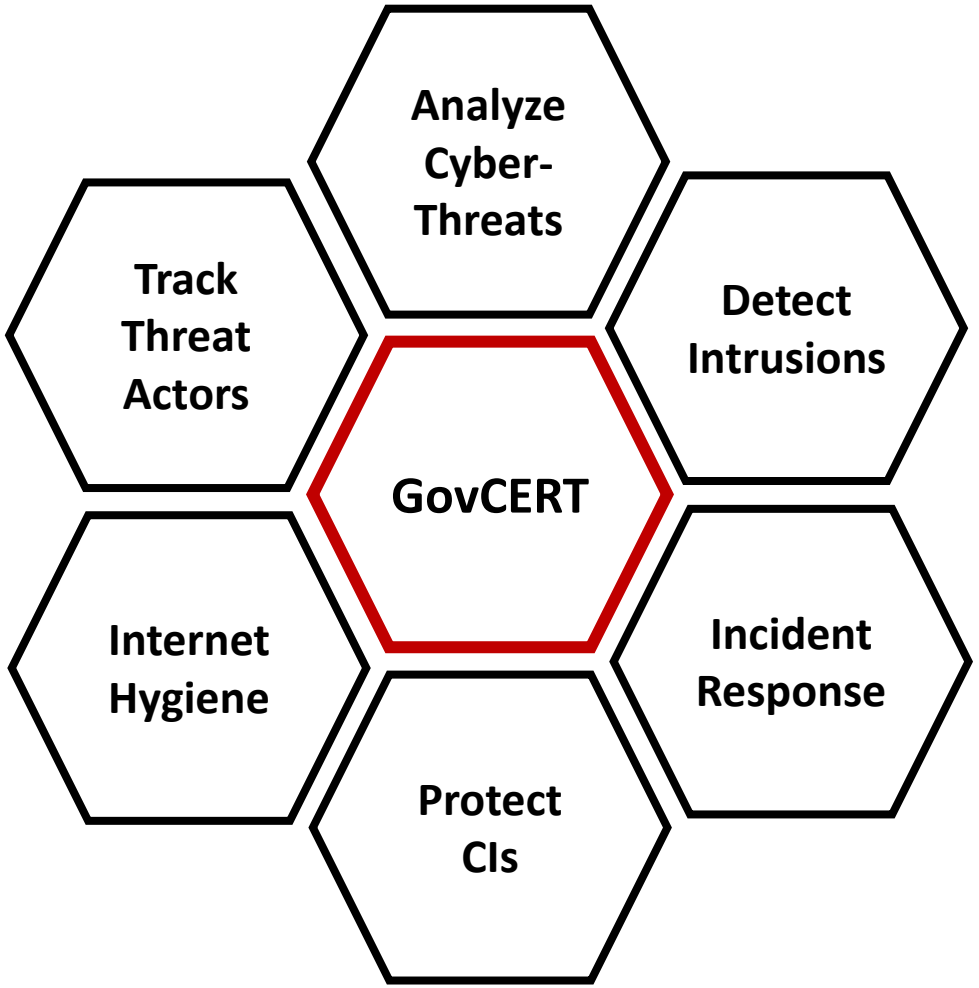
Cyber Security Hub (CSH)



The aim of the CSH is to provide operators of critical infrastructures (critis) with **targeted information and warnings on cyber threats (e.g. ongoing cyber attacks, early warnings, instructions for self-protection)** and to enable the secure exchange of information between NCSC and critis.

GovCERT

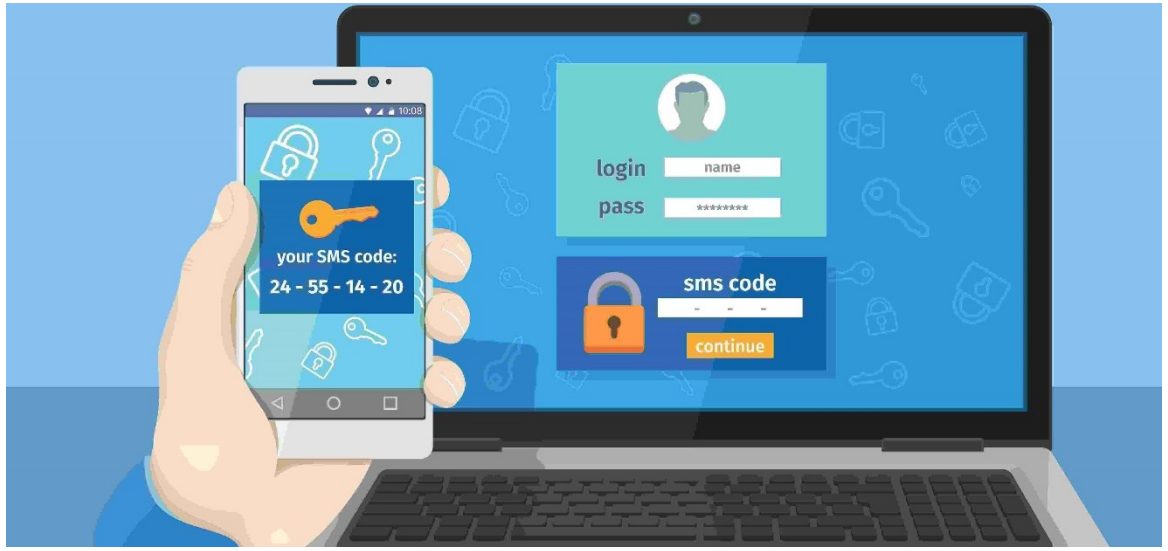
- Support from GovCERT with technical expertise
- Access to technical data for blocking or monitoring purposes



What can I do to prevent incidents?

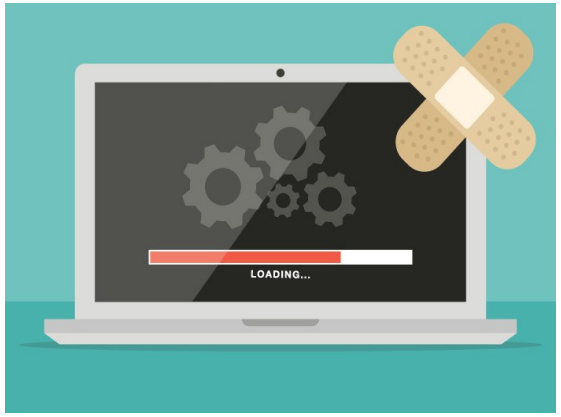
What can I do to prevent incidents?

- **Two-factor authentication** (2FA / MFA) for internal resources accessible from the Internet (Sharepoint, web mail, remote access, etc.)



What can I do to prevent incidents?

- **Life cycle und patch management**
  - **Security updates** must be installed promptly
  - Software and devices that are no longer supported by the manufacturer and no longer receive security updates (**“End of Life”**) harbour a high security risk and must be replaced promptly

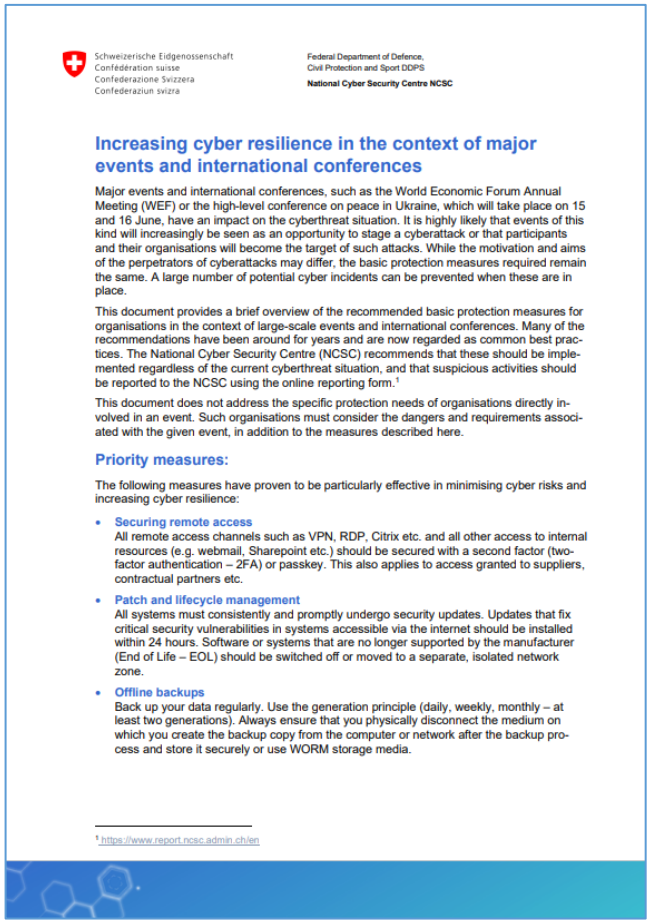


What can I do to prevent incidents?

- **Backups:**
  - Create regular backups of your data
  - Store these “offline”, i.e. physically separated from the company network

Increasing cyber resilience in the context of major events and international conferences

Updated information depending on the actual situation



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Increasing cyber resilience in the context of major events and international conferences

Major events and international conferences, such as the World Economic Forum Annual Meeting (WEF) or the high-level conference on peace in Ukraine, which will take place on 15 and 16 June, have an impact on the cyberthreat situation. It is highly likely that events of this kind will increasingly be seen as an opportunity to stage a cyberattack or that participants and their organisations will become the target of such attacks. While the motivation and aims of the perpetrators of cyberattacks may differ, the basic protection measures required remain the same. A large number of potential cyber incidents can be prevented when these are in place.

This document provides a brief overview of the recommended basic protection measures for organisations in the context of large-scale events and international conferences. Many of the recommendations have been around for years and are now regarded as common best practices. The National Cyber Security Centre (NCSC) recommends that these should be implemented regardless of the current cyberthreat situation, and that suspicious activities should be reported to the NCSC using the online reporting form.[1]

This document does not address the specific protection needs of organisations directly involved in an event. Such organisations must consider the dangers and requirements associated with the given event, in addition to the measures described here.

Priority measures:

The following measures have proven to be particularly effective in minimising cyber risks and increasing cyber resilience:

- **Securing remote access**
  All remote access channels such as VPN, RDP, Citrix etc. and all other access to internal resources (e.g. webmail, Sharepoint etc.) should be secured with a second factor (two-factor authentication – 2FA) or passkey. This also applies to access granted to suppliers, contractual partners etc.
- **Patch and lifecycle management**
  All systems must consistently and promptly undergo security updates. Updates that fix critical security vulnerabilities in systems accessible via the internet should be installed within 24 hours. Software or systems that are no longer supported by the manufacturer (End of Life – EOL) should be switched off or moved to a separate, isolated network zone.
- **Offline backups**
  Back up your data regularly. Use the generation principle (daily, weekly, monthly – at least two generations). Always ensure that you physically disconnect the medium on which you create the backup copy from the computer or network after the backup process and store it securely or use WORM storage media.

[1] https://www.report.ncsc.admin.ch/en

➢ https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/massnahmen-grossanlaesse-konferenzen.html

Ask questions

Thank you!

Monica Ratte
Co-head of GovCERT (NCSC)