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

Additional recommendations for basic protection:

The measures above reduce the risk of a cyberattack considerably. However, it is advisable to provide additional protection if possible with the following measures:

- **Provide contact in case of security incidents**
  It is worth providing an address to be contacted in the event of a security incident. This way the NCSC or the police will be able to get in touch quickly in the event of an alert. It is recommended to use the security.txt[2] standard for this purpose.
- **Keep business continuity management up to date**
  It is worth considering how core business processes depend on IT and how value can continue to be created in the event of a failure. It should also be ensured that emergency and crisis processes are up to date. As a minimum, it should be clear who informs whom and who can make which decisions.
- **Use of DDoS protection**
  Web applications, online platforms or systems that are essential for business activities should be protected by an anti-DDoS solution or by an anti-DDoS provider. Talk to your internet or hosting provider about possible solutions.
- **Use of an EDR/XDR to detect anomalies**
  Use EDR (Endpoint Detection and Response) or XDR (eXtended Detection and Response) on all clients and servers to detect and block suspicious activity.
- **Restrict access to exposed systems**
  As far as possible, restrict access to online systems, applications and platforms. This can be achieved with geo-blocking or an 'allow list' for certain IP addresses or IP networks ('whitelisting'), for example.
- **Check security-relevant log files**
  Regularly check security-relevant log files from antivirus software, EDR/XDR, web proxy or VPN, etc. for suspicious activities. Security software alerts should be checked immediately and appropriate countermeasures introduced.

Further technical and organisational measures can be found in our information sheet for SMEs at: https://www.ncsc.admin.ch/it-sicherheit-fuer-kmus-en

[2] https://www.ncsc.admin.ch/securitytxt-en