Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Finance FDF
General Secretariat

National Cybersecurity Centre NCSC
www.ncsc.admin.ch

NCSC

Home office

Secure use of remote access

Contents

1 Introduction

Companies are increasingly using remote methods to access their corporate networks. However, using this technology also raises the risk of cyberattacks.

Attackers use all sorts of methods to gain access to corporate networks:

- Phishing attempts (classical password phishing or so-called real-time phishing[1] in the case of two-factor authentication).
- Attacks on passwords (attacks on directory services, alteration of passwords, brute force attacks).
- Attacks on unsecured gateways.
- Malware attacks (these often go unnoticed if there is no tunnelling of the entire data traffic).

2 Countermeasures

2.1 Accessibility considerations

The use of remote access software must be considered carefully, as it can put a significant strain on bandwidth. Discuss your requirements with your internet service provider (ISP) and in-house IT specialists. Moreover, increasing the bandwidth is not advisable if downstream systems (firewalls, intrusion prevention system, switches, servers, etc.) are unable to cope with the increased data traffic.

2.2 Protection against malware/phishing

- Use a **two-factor authentication**. Crypto drives, smartcards and hardware-based one-time passwords (OTPs) such as RSA tokens or Mobile ID are regarded as good solutions. If such solutions are not feasible, software-based solutions such as Google Authenticator are also suitable.
- Enforce the **use of strong passwords**, and remind users to use a separate password for each service and to avoid sequences in passwords (e.g. Password1, Password2, etc.).
- Continuously check the log data of your remote access-equipped devices for anomalies (e.g. foreign IP addresses if most staff are located in Switzerland; IP addresses from Tor networks; VPNs or networks from hosting providers in general).
- Enforce **tunnelling** for all devices to ensure secure communication and make connections to the internet visible. Bear in mind that these measures will involve a corresponding increase in bandwidth load.
- **Ensure** that your **employees are aware** of cyberthreats, especially in the home office

[1] MELANI Semi-annual report 201119, section 4.4.2, https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte.html

environment, and **communicate contact information** that they can use if they notice anything suspicious.

- Plan for **forensic analysis preparedness**, particularly if you allow your employees to access the corporate network from their private devices.
- Make sure that all devices used for remote access are **up to date** (patches) and plan for **emergency patch rollout** in the event of critical vulnerabilities.
- It must be possible to update devices used for remote access without them being physically present on company premises.
- Make sure that employees working from home **cannot establish a connection** between their **private** network and the **corporate network**.
- Plan for the reboot/replacement of **infected devices** via remote access, e.g. using a dedicated DSL/fibre-optic connection.
- In addition to these specific recommendations, take note of the measures published by the NCSC to protect against ransomware attacks[2].

2.3 Data security

- Ensure the availability of **offline backups** in the event of ransomware attacks
- Data backup must also be possible and effective if employees save **important data locally**

In the event of an increase in the use of **BYOD** (bring your own device): draw up **instructions for using** such devices. In particular, it should be emphasised that corporate data must be securely stored (e.g. in an encrypted container), so that it can be completely wiped at a later date. This is especially important if the person concerned subsequently wants to sell their private device. Bear in mind that a lot of effort is required to completely wipe data stored on an unencrypted hard drive (if possible at all).

2.4 Awareness-raising

- Stop all **phishing awareness campaigns** to avoid unsettling your employees.
- Inform your employees about **additional risks** and ask them to report suspicious emails and/or websites to your helpdesk.
- Make sure that the **helpdesk** is appropriately staffed.
- Help your employees with the secure configuration of **WLAN networks**.
- Instruct your employees how to **contact the helpdesk** and explain how the helpdesk will

[2] https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/
https://www.ncsc.admin.ch/ncsc/en/home/aktuell/news/news-archiv/sicherheitsrisiko-durch-ransomware.html
https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/as- sets/blocked-filetypes.txt

contact them. In this way, you will prevent them from being tricked by fake support calls[3].

- Ensure that you have a simple procedure in place to **identify users** if one of them requests a password reset.

2.5 Miscellaneous

- **Document all changes** that you have initiated. In this way, you will ensure that these changes can be reversed easily, if necessary.
- **Highly privileged administrative tasks** may only be performed from specially **secured devices** that do not permit any other simultaneous internet access. Where possible, use dedicated server instances.
- If you spot **phishing or malware activity**, report this to www.antiphishing.ch.
- Only use **trusted** sources to get information about current cyberthreats[4].
- Make it easy to **deliver tools or features** that are requested in an emergency. If you are unable to offer an internally developed solution, provide information on alternative solutions. Avoid your employees searching for individual solutions that you cannot monitor.

2.6 Summary

Risk management and operational security should be quickly adaptable to the changing threat situation and should permit appropriate countermeasures if risks are judged to be critically high. Do not perform any complex changes in the current situation; instead, ensure risk mitigation through increased detection capabilities. If you have any questions, please contact outreach[at]ncsc.ch.

[3] https://www.ncsc.admin.ch/ncsc/en/home/cyberbedrohungen/fake-support.html

[4] https://www.ncsc.ch ; https://twitter.com/GovCERT_CH; https://www.bsi.bund.de/DE/Home/home_node.html ; https://www.ssi.gouv.fr/ etc.