Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
General Secretariat

National Cybersecurity Centre NCSC
www.ncsc.admin.ch

NCSC

Information security checklist for SMEs

Contents

Introduction

This checklist is aimed at Swiss SMEs and is intended to help them increase information security in their company.[1]

The checklist is divided into two areas:

- **Organisational measures** that increase or ensure information security
- **Technical measures** that increase or ensure the security of the IT infrastructure

Technical measures play a major role in ensuring information security. Nevertheless, these have to be supplemented by organisational measures. Especially in the case of cost- and/or personnel-intensive measures, every company has to weigh up the costs of the measures against the risks that arise if they are not implemented. Non-implemented measures result in so-called residual risks. Therefore, senior management has to decide whether to bear the residual risks or to provide resources to further minimise the risks. Although the technical risks of IT systems constitute an important part of information security, a company should not limit its focus to these risks or even name the IT division as the sole risk carrier. Responsibility for risk management, the classification and ranking of information, as well as any graduated expenses for security measures made available are core tasks of senior management.

Organisational measures

Organisational measures ensure that the information security responsibilities in the company are defined.

Information for senior management about risks
Evaluate the dependency of your business processes on your IT. What are the consequences of a system failure or unavailability of data storage? What financial consequences can be expected? What countermeasures can be taken? etc.

Risks as a component of governance and continuity management
It must be possible to carry out the necessary work even if all or part of the IT system is temporarily not functioning.. This does not necessarily have to be the result of a cyberattack. Power outages, natural disasters and other scenarios can also provoke a complete or partial failure of your IT infrastrucute. Define possible alternatives and/or fallback levels for the respective systems at an early stage.

Responsibilities are regulated
Employees need to know whom they should contact if they have questions about IT security (e.g. if they receive a suspicious email) or who to inform if an IT security incident occurs. Draw up an incident response plan at an early stage. Check the effectiveness of the plan regularly, e.g. with simulations, and adapt the plan based on the findings of these exercices.

Responsibilities of companies and IT service providers
Many smaller companies outsource IT to specialised service providers. The responsibilities between you and the IT service provider must be clearly regulated.
In the contract, regulate any liability issues arising in the event that security regulations are disregarded or IT security is otherwise neglected. The contract must be formulated clearly and unambiguously. If, for example, data backups are not made due to a misunderstanding,

[1] See also: "IT, IT security and infrastructure: recommendations" on the Confederation's SME portal: https://www.kmu.admin.ch/kmu/en/home/concrete-know-how/sme-management/it-security-and-infrastructure.html

the consequences can be disastrous.[2]

Raising employee awareness
Raising all employees' awareness of dealing with the IT infrastructure is of key importance. Train your staff regularly on dealing with potential dangers in the digital world. Make your employees aware of how to deal with email and the internet. You will find corresponding rules of conduct on the NCSC website.

Knowledge of the current threat situation
Keep up to date with new information on current security threats and appropriate measures to address them.[3]

Dealing with sensitive data
Issue binding rules for classifying data and enforce them consistently. In particular, specify how classified data may be stored and/or transmitted electronically.[4] Define guidelines for the transmission of company information. As a matter of principle, confidential information should not be transmitted through anonymous channels, e.g. telephone or email.

Company information on the internet
Criminals are constantly seeking information about potential victims. Therefore, think carefully about what information you disseminate on your website or in social media, for example. Minimise the amount of information about your company that is available on the internet. Weigh up the benefits and risks of the available information. Draw up guidelines on how your employees should deal with company information, e.g. when using social media privately.

Security from procurement to disposal of the IT infrastructure
Security considerations should always be integrated into the procurement process. Not only the requirements for the launch of operations must be taken into account in the process, but also those over the entire life cycle of a system, including maintenance and decommissioning. For example, get informed before purchasing about how long security updates will be provided. Are they installed automatically? How do you know that new updates are available? Define the procedure for decommissioning parts of the IT infrastructure (e.g. how to reliably remove confidential information from the systems in question).

Password policy
Define binding password rules and enforce them consistently. The password must have a minimum length of 12 characters and consist of upper and lower case letters, numbers and special characters. Where possible, rely on two-factor authentication. It is essential to avoid the multiple use of the same passwords. Use a password manager and generate a separate password for each application. You will find various password management systems on the market for the different operating systems and devices; some are free of charge, while others require a licence. Passwords and access credentials may never be given to others.

Access permissions
Very few employees require extensive administrator rights. Only grant employees those rights that are absolutely essential for them to complete their work (e.g. marketing employees do not necessarily need access to the information in the HR division). In particular, you

---

[2] For further information, see Cooperation with IT service providers: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/zusammenarbeit-it-provider.html

[3] Every six months, the NCSC covers the most important cyberincidents both in Switzerland and internationally in its semi-annual report. The top five threats are also updated regularly on the NCSC website.

[4] Recommendations and ordinances on data protection can be found on the portal of the Federal Data Protection and Information Commissioner (FDPIC): https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html (not available in English)

should disable the rights to install any software.

E-banking
For all payment orders transmitted digitally (offline payment software; e-banking), use a dedicated computer on which you do not surf the internet or receive emails. Make sure that all of the processes relating to payment transactions are regulated and strictly enforced (dual control principle, joint signature, etc.). This applies in particular if several employees have payment powers. If need be, have the functions you do not need in your e-banking application disabled or restricted. Discuss possible security measures with your financial institution, e.g. possible country restrictions.

Technical measures

A 100% security cannot be achieved with technical measures. Often it is not the technical measures that are the weakest link in the chain, but rather human beings. If employees are not trained in the secure use of IT systems, the effectiveness of the technical measures described below can be severely impacted. However, a sensible combination of various technical measures makes a significant contribution to IT security in the corporate network and reduces the risk of malware infections.

Regular data backups
Define a process for regular data backups and strictly enforce it. You can also outsource data backups and other technical measures to a specialised IT service company.

Check the data backup regularly to ensure it functions properly. Practise importing backups from time to time so that you are familiar with the process if you ever need to rely on it.

The backup should be stored offline, i.e. on an external medium such as an external hard drive. Therefore, make sure that the medium where the backup is saved is disconnected from the computer after the backup procedure is complete. Otherwise, data on the backup medium might be encrypted and rendered unusable in the event of a ransomware attack. Keep even older backups for a certain period of time.

Virus protection
Virus protection must be installed on every computer in the company and must be updated regularly. Carry out complete system scans at regular intervals (e.g. weekly or monthly).

Firewalls
Use a firewall on every computer. In addition, protect your corporate network from the internet using an extra firewall. Use firewall rules to define which incoming and outgoing connections should be allowed. Run proxy-enabled protocols such as HTTP/HTTPS, etc. via a proxy. Evaluate the proxy log files regularly.

Security updates
Outdated software is a popular gateway for malware. Make sure that all computers and servers in your network automatically install security updates. All installed software must be updated immediately when security updates are released. Hardware such as printers, routers, etc. must also be kept up to date.

Content management systems (CMS)
Content management systems (CMS) for creating and updating websites must always be kept up to date. Most content management systems offer an automatic update function that is easy to activate. Use a web application firewall (WAF) to protect your website from attacks. You can find more measures for securing content management systems on the NCSC

website.[5] If your company is highly dependent on its online presence (e.g. online shop), then think about how you can counter a possible DDoS attack.[6] The major Internet service providers in Switzerland offer DDoS protection which you can buy now but only have to pay when you actually need it.

Log files
Log files are of crucial importance for following up on an IT incident. Ensure that critical systems such as accountancy software, domain controllers, firewalls and email servers create log files. Check the available log files regularly for discrepancies. Store log files for at least six months and include them in your backup process. Log file analysis requires extensive knowledge, which is why outsourcing to an IT service provider could be helpful.

Network segmentation[7]
Divide your company network into individual areas (e.g. separate networks for production, HR, accounting, etc.). There is no reason why HR employees should have access to your production facilities. In this way, you can prevent that for example the control computers of plant facilities that can no longer be updated become a gateway for attackers.

At least the computers of the Accounting and Human Resources (HR) departments should be in a separate network and should not be accessible from the other computers in your network. Remember that malware can also spread via network shares. Your IT service provider can advise you on planning and implementation.

Filtering potentially harmful emails
Potentially harmful email attachments should already be blocked or filtered on your email gateway or by your spam filter. A list of potentially harmful file extensions can be found on the NCSC website.[8] Such email attachments must also be blocked if they are sent to recipients in your company in archive files such as ZIP, RAR, ISO, or even in protected archive files (e.g. in a password-protected ZIP file).

Macros
Macros are used for automating Office documents. However, they can also be used to spread malware.
All email attachments that contain macros (e.g. Word, Excel or PowerPoint attachments with macros) should be blocked. Make your employees aware that corresponding warnings in Office programs must not be ignored.

Remote access
If employees need to access your corporate network from outside the company (e.g. when on business trips, working from home, etc.), this should only be possible through a virtual private network (VPN) protected by two-factor authentication. This also applies to access by external IT service providers and administrators.

Cloud services
When using cloud services, you do not have to operate an expensive IT infrastructure

---

5 Measures to secure content management systems (CMS): https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-cms.html

6 Measures to counter DDoS attacks: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ddos.html

7 "Suitable logical segmentation" issued by Germany's Federal Office for Information Security BSI: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05062.html

8 NCSC rules of conduct, email: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/verhalten-bei-e-mail.html

yourself. However, take care when using cloud services. Sensitive data should only be stored locally, never in the cloud. Ask the provider about the most important security precautions (access to data, data backups, etc.) before signing a contract.

Encryption
Encrypt important data, particularly when using cloud services on mobile devices.