CYBERSECURITY QUICK CHECK FOR SME

Notes and further information for a minimum level of protection

The following explanations show why the points mentioned in the quick check www.cybersecurity-check.ch are essential for minimal cybersecurity protection. Most of the notes and supplementary information come from the following sources:

- Publication «More information security for small and medium-sized enterprises (SMEs)», which was updated in 2016 by the Information Security Society Switzerland ISSS (in German only)[1]
- Information for SMEs provided on the portal by the Reporting and Analysis Centre for Information Assurance MELANI or the publication «Information security checklist for SMEs», updated in 2018 [2]

Further sources are mentioned accordingly.

[1] https://www.kmu.admin.ch/dam/kmu/de/dokumente/savoir-pratique/Informatique-et-IT/InfoSurance_10_Points_Programme_FR.pdf
[2] https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

1. Tasks, powers, responsibilities

If IT security tasks, powers and responsibilities have not been settled, it is an indication that the topic of cybersecurity is not given the necessary importance.

More than a third of Swiss SMEs have already been affected by cyber-attacks; even small businesses such as restaurants and hairdressers are potential attack victims[3]. Many companies underestimate the risk[4] and do not have sufficient protection. The appointment of a cybersecurity officer who competently manages the IT security area is a prerequisite for effective basic protection. Particularly smaller SMEs can work together with external experts in this area.

Further information

ISSS (in German only)
Creating specifications for IT officers
Information security for SMEs, Point 1

MELANI
Organisational measures for defining responsibilities
Checklist for SMEs, p. 2-3

2. Raising awareness among employees, clients, suppliers and service providers

The best technical measures for protecting against cyber risks are useless if employees do not know, understand and correctly implement the security guidelines and code of conduct.

Training to detect emails containing malware or links to compromised websites is top priority. Most digital attacks are carried out via email. All unsolicited emails with attachments or links that you receive must generally be distrusted. However, other simple activities that are used by virtually all employees also entail dangers that are often underestimated, e.g. when surfing online or using badly chosen passwords. Once malware is in the system, it can have extensive financial and legal consequences.

Further information

ISSS (in German only)
Informing IT users about guidelines
Information security for SMEs, Point 8

Raising employee awareness
Information security for SMEs, Point 15

MELANI
How do I protect myself?
Rules of Conduct
MELANI portal

[3] SMEs react too little to cybercrime, publication on the SME portal of the Federal Department of Economic Affairs, Education and Research, EAER: link to the publication (in German only)
[4] Cyber risks in Swiss SMEs: 2017 final report, joint study by SIA, SQS, ICTswitzerland, ISSS, FITSU, Federal Expert Commission: link to the study (in German only)

3. Data protection guidelines

Loss of data or data protection violations can result in criminal consequences, high fines and a serious loss of image. The consequences could possibly pose a threat to a company's existence.

Your company is responsible for the secure handling of confidential and personal data and must comply in particular with the provisions of the Data Protection Act (FADP), the Federal Copyright Act (CopA) and the Swiss Code of Obligations (CO). Even by creating a guest list for a company event, you collect personal data that you have to protect. Moreover, the EU's new General Data Protection Regulation (GDPR) came into force on 25 May 2018, and some of this also applies to Swiss companies. Check whether you are affected and take corresponding measures, as violations can result in high fines.

Further information

ISSS (in German only)
Adhering to confidentiality requirements
Information security for SMEs, Point 11

Treating electronic and non-electronic data confidentially
Information security for SMEs, Points 13,14

Federal Data Protection and Information Commissioner FDPIC (in German only)
Dealing with personal data
FDPIC portal

Federal Department of Economic Affairs, Education and Research EAER (in German only)
GDPR challenge
EAER SME portal

Economiesuisse (in German only)
«GDPR – Is your company affected?»
Online-Check and GDPR factsheet

4. Password guidelines and user administration

Weak and/or re-used passwords and unclear access and administrator rights constitute a significant security risk that can easily be avoided.

Encourage your employees to use strong passwords and a different password for each service. Use a password manager, do not write down the passwords and do not pass them on to third parties at any time. Use two-factor authentication where possible. Regulate access to data via a superordinate user administration that your employees know, understand and consistently adhere to. In the process, ensure that each user has only the most vital access rights and delete them when employees leave the company.

Further information

ISSS (in German only)
Using strong passwords
Information security for SMEs, Point 6

Protecting access to data
Information security for SMEs, Point 12

MELANI
How do I protect myself?
Rules of Conduct
MELANI portal

Passwortcheck (in German only)
How to test the strength of your passwords
Passwortcheck.ch portal

5. Up-to-date protection against malware

An up-to-date antivirus program is indispensable on every IT device and is part of the basic protection against viruses, worms and Trojans.

Computer viruses often enter the system cleverly camouflaged via email attachments from known senders[5]. Malware can thereby enter your system easily and destroy and manipulate data and paralyse the entire IT infrastructure. Poorly protected computers can become a tool for targeted attacks by hackers and spread malware. This endangers not only your company, but also third parties.

Further information

ISSS (in German only)
Keeping antivirus programs up to date
Information security for SMEs, Point 3

MELANI
How do I protect myself?
Software and Parameters
MELANI portal

Measures at the technical level
Checklist for SMEs, p. 4-5

List of antivirus software
MELANI website

6. Configured and updated firewall

The use of a powerful firewall significantly reduces the risk of attacks. Together with antivirus software, it is part of the basic protection for every IT device and is often available free of charge as additional software with antivirus programs.

Further information

ISSS (in German only)
Protecting internet access with a firewall
Information security for SMEs, Point 4

MELANI
How do I protect myself?
Software and Parameters
MELANI portal

Information on firewalls
Checklist for SMEs, p. 6

[5] Reporting and Analysis Centre for Information Assurance MELANI publication on the topic of malware: to the publication (in German only).

7. Keeping devices and systems connected to the internet up to date

If operating systems, antivirus software, firewalls and other applications are not kept up to date, attackers can penetrate through known security vulnerabilities. Data can be destroyed and manipulated or your infrastructure can be misused for criminal purposes.

Update computers regularly and check all software products regularly for updates to eliminate security vulnerabilities – this also applies to all mobile devices used in your corporate environment. Use automatic update functions whenever possible. Systematically determine the cycle according to which all devices are checked in this respect.

Further information

ISSS (in German only)
Checking and maintaining IT systems
Information security for SMEs, Point 16

Updating software regularly
Information security for SMEs, Point 5

Protecting mobile devices
Information security for SMEs, Point 7

MELANI
How do I protect myself?
Software and Parameters
MELANI portal

8. Protected and encrypted WLAN network

Unsecured and unencrypted WLAN networks and those secured with outdated protocols allow unauthorised access as well as hacker access. All devices connected to your WLAN and the data stored on them can be read, manipulated and misused for criminal acts.

Protect your wireless network with a firewall, encryption and strong passwords. Set up separate access for your clients and guests.

Further information

ISSS (in German only)
Protecting internet access with a firewall
Information security for SMEs, Point 4

Encrypting mobile data storage devices and transmissions
Information security for SMEs, Point 13

CHIP.de (in German only)
5 tips for effectively protecting your internet access
CHIP.de website

MELANI
How do I protect myself?
Peripheral devices
MELANI portal

9. Encryption of (data) transmission (e.g. VPN)

Confidential information and business or personal data may fall into the wrong hands during transmission.

Reliable encryption of your communication and data during transmission reduces this risk.

Further information

ISSS (in German only)
Encrypting mobile data storage devices and transmissions
Information security for SMEs, Point 13

Computerwoche (in German only)
Methods for encrypting hard drives, emails, file transmission
Computerwoche website

10. Backups

Data loss cannot always be traced back to criminal acts; even water damage can destroy important data and information. Back up your data regularly to avoid a permanent loss of data, as some data is subject to a legally prescribed retention obligation.

Make regular backups of your data, keep them in an external, protected location, and regularly check whether the data can be restored from the security media. Every SME should make a back-up daily. Define a process that governs the frequency with which you back up certain data and adhere to it consistently.

Further information

ISSS (in German only)
Securing data with backups
Information security for SMEs, Point 2

MELANI
How do I protect myself?
Software and Parameters
MELANI portal

11. Minimum emergency response arrangements

In the case of an IT incident, you need to be able to act quickly to limit damage and minimise costs.

Define how employees should behave in an emergency and what actions are to be triggered. Define fall-back levels for a temporary total IT failure so that the most important work can continue to be carried out. Determine contact persons and ensure their availability in an emergency.

Further information

ISSS (in German only)
Ensuring an uninterruptible power supply
Information security for SMEs, Point 17

Keeping important elements redundant
Information security for SMEs, Point 18

Emergency preparedness
Information security for SMEs, Point 19

12. Outsourcing

Check whether all of the quick check points are regulated in the contracts with your outsourcing partners.

You have addressed the questions that are key to achieving a minimum level of cybersecurity protection. A summary providing more detailed information – specifically for SMEs – is available at www.cybersecurity-check.ch.

Impressum

Authors:

Umberto Annino (ISSS) | Norbert Bollow (SNV) | Maya Bundt (SVV) | Daniel Caduff (BWL) | Lucius Dürr (SQS) | Xaver Edelmann (SQS) | Andreas Kaelin (ICTswitzerland) | Marcel Knecht (SNV) | Arié Malz (EFD) | Felix Müller (SQS) | Gunthard Niederbäumer (SVV) | Reinhard Niederer (Druckerei AG Suhr) | Peter Reber (SQS) | Daniel Rudin (ISB – MELANI) | Ronald Trap (SNV)

Editorial:

Annalena Kassner (ICTswitzerland) | Lena Schneider (ICTswitzerland) | Adrian Sulzer (SATW) | Nicole Wettstein (SATW)