Cybersecurity check for SMEs

Version 4.0, 8. December 2025

SMEs targeted by cyberattacks

Cybercriminals are increasingly targeting small and medium-sized enterprises (SMEs) a. According to *Netzwoche*, the number of cyberattacks in Switzerland rose by an alarming 113% in the first quarter of 2025 compared to the previous year. Particularly worrying is the increase in AI-powered attacks, for example, using deepfake technologies for CEO fraud (Source: *SECO SME Portal*).

The most common causes of successful attacks are:

- Inadequate protection of systems and processes,
- Outdated IT systems,
- Exploitation of social behavior (social engineering)
- Inadequate preparation for security incidents.

The www.cybersecurity-check.ch was developed for SMEs as part of the National strategy for the protection of Switzerland against cyber risks (NCS); the first edition was published in 2020. This completely revised version 4.0 (as of November 2025) was created in collaboration with the following partners: ADSS, NCSC, BDO, digitalswitzerland, EXPERTsuisse, GObugfree, ISSS, SATW, SISA, SNV, SQS, Suissedigital and SVV.

A practical tool for protecting SMEs

The Cybersecurity Check offers SMEs specific and actionable recommendations for improving their security. It takes into account the current threat landscape, new technologies, and legal requirements. Thanks to its modular structure and focus on practical application, it is easy to use, even for those without a technical background.

The integrated self-check enables companies to evaluatetheir current security status:

- Which technical, organizational, procedural and employee-related protective measures have already been implemented,
- as well as where there is a specific need for action to ensure a minimum level of cybersecurity.

Note: The Cybersecurity Check is not intended to replace individual security consultancy, but rather to offer a sound and practical starting point for SMEs.

Table of contents

1 Organization & Processes

Why does this matter?

Cyber incidents can affect companies of all sizes – including SMEs. Organisations must not only be prepared for an emergency, but they must also ensure continuous improvement and prevention through a high level of organizational security. Companies that establish clear processes and review them regularly can respond quickly, limit damages, and resume business operations faster when an incident occurs.

A good level of organizational security means:

- Clearly defined responsibilities,
- regular backup of critical information,
- careful allocation and management of access rights,
- a well-thought-out and tested emergency plan (including alternative communication channels).

What can you do?

- ☑ Keep an up-to-date and accurate inventory of IT equipment and applications used in business-critical processes, and protect these assets from unauthorized access.
- ☑ Implement regular, automated backups of your business-critical data.
- ☑ Strengthen user management with role-based access rights and two-factor authentication.
- ☑ Develop and test a comprehensive emergency plan that reflects current threats (e.g., using emergency plan templates from UFCS and BDO).

2 Employees & Awareness

Why does this matter?

Exploiting social behavior (social engineering) is a key element of successful cyberattacks. Employees who are aware of common threats can spot suspicious activity sooner, avoid common mistakes (such as clicking on phishing emails), and remain calm in critical situations. According to the BACS, social engineering contributes to the damage in more than 80% of cyber incidents affecting Swiss companies. An informed workforce is therefore one of the most important protective factors in your cyber strategy.

Good safety behavior means:

- Recognizing suspicious messages and situations,
- handling passwords and sensitive information properly,
- following clear user guidelines for IT systems and communication channels,
- Ongoing training and practice.

What can you do?

- ☑ Integrate employee awareness into everyday work rountines.
- ☑ Protect your applications with strong passwords and two-factor authentication (2FA).
- ☑ Define clear user guidelines for the safe use of the internet and emails.

3 Technical protective measures

Why does this matter?

Technical security measures form the foundation of any cyber defense. Without up-to-date systems, protection mechanisms, and encrypted communication, your company remains vulnerable – no matter how well-trained your teams are.

Attacks have become increasingly automated, driven by AI-powered vulnerability scans, cloud exploitation, and attacks via outdated or unprotected devices (e.g., cloud storage, routers, IoT devices, remote access systems). Software vulnerabilities and missing updates continue to be among the most common entry points for attackers.

A high level of technical protection means:

- Up-to-date systems and applications,
- the use of security software,
- encrypted communication,
- Protection of all connected devices.

What can you do?

- ☑ Use appropriate hardware and software (e.g., firewalls and antivirus software) to strengthen your security.
- ☑ Regularly update your software and devices.
- ☑ Avoid connecting outdated devices for which software update are no longer available, and only connect systems to the internet if absolutely necessary.

Note: Technical security measures are not a one-off project, but an ongoing process. Conduct regular reviews – or bring in external IT specialists and certified providers to identify and close any gaps.

4 Data protection & legal

Why does this matter?

Protecting personal data is not only about building trust with customers, it is also a legal requirement. Violations of data protection laws can lead to hefty fines, legal consequences, and serious reputational damage, especially when they result from cyber incidents.

Since the revised Swiss Data Protection Act (DSG) came into force in 2023, and the EU General Data Protection Regulation (GDPR) increasingly applies to Swiss companies with EU ties, the following applies: Anyone processing personal data must implement appropriate technical and organizational measures to ensure its security. In the event of a breach, managers may be held personally liable.

Compliant data handlingmeans:

- Transparency towards data subjects about how their data is processed,
- protection against unauthorized access and data loss,
- clear roles, responsibilities and accountabilities,
- data processing agreement with external service providers (Pattern (Template)
- knowledge of and compliance with legal reporting obligations in the event of a data breach (guide)

What can you do?

- ☑ Ensure that the handling of personal data complies with the requirements of the Swiss Data Protection Act (DSG) and, where applicable, the General Data Protection Regulation (GDPR).
- ☑ Document what data you collect, process and store – and for what purpose.
- ☑ Implement appropriate technical and organizational measures to protect this data.

Note: Data protection affects all areas of your company – from your website and CRM to human resources. It's not just an IT responsibility, but a company-wide obligation. Further information and resources can be found at: https://www.edoeb.admin.ch/en/data-protection and https://www.kmu.admin.ch/kmu/en/home.html.

5 External Partners & Service Providers

Why does this matter?

Many SMEs rely on external IT service providers, cloud providers, or specialized software solutions. This makes perfect sense; qualified partners offer expertise, experience, and modern technologies that are not always available internally. Effective collaboration with external providers is therefore a key component of a strong cybersecurity strategy.

At the same time, it is essential to establish clear agreements, define responsibilities, and regularly review compliance with security standards. Even if tasks are outsourced, the responsibility for the security of your data and systems remains with your company .

A secure approach to dealing with external partners includes:

- Selecting qualified service providers with demonstrable security expertise,
- written security requirements,
- transparent communication and joint emergency planning,
- Targeted allocation and management of access rights.

What can you do?

- ☑ Work with qualified IT partners who can demonstrate compliance with security standards (e.g., CyberSeal, SN EN ISO/IEC 27001).
- ☑ Document technical and organizational requirements in writing.
- ☑ Integrate your IT service providers into your emergency planning and security processes.

Note: Even if a provider claims to "take care of everything for you," your organisation remains responsible (including for data backup and recovery). Regularly check whether your partners are adhering to security measures appropriate for your industry and company size.

For questions regarding the selection of suitable providers or contract drafting, consult national platforms such as: NCSC - Information for companies, Alliance Digital Security Switzerland - CyberSeal, ITSec4KMU or your industry associations.

6 Penetration Testing & Vulnerability Analysis

Why does this matter?

Even well-intentioned security measures are only effective if they actually work. Vulnerabilities in systems, networks, or applications often go unnoticed until they are exploited by attackers. That's why it is crucial to regularly test your IT infrastructure – ideally through qualified, independent third parties.

Especially in 2025, when attackers increasingly use automated and AI-powered scans to specifically identify vulnerabilities in companies, a proactive approach is crucial. A penetration test (pentest) simulates real attacks in a controlled and traceable manner, to identify and fix vulnerabilities early on.

A professional test provides:

- Clarity about actual security vulnerabilities,
- A realistic assessment of the associated risks,
- Specific recommendations for improvement.

What can youdo?

- ☑ Conduct regular vulnerability analyses of your systems – internally or with external experts.
- ☑ Conduct a penetration test at least once a year, or whenever there are significant changes to business-critical systems.
- ☑ Systematically address identified vulnerabilities and document the measures taken.

Note**:** For smaller SMEs, standardized vulnerability scans can be an important first step. Platforms such as GObugfree GoBugFree or ITSec4KMU offer practical support. If you want to go further, networks such as SCD-DNA or Alliance Digital Security Switzerland - CyberSeal can help identify suitable providers.

Info Box: Penetration Testing vs. Ethical Hacking

Penetration Testing (Pentest)

A clearly defined, structured, and targeted test that focuses on a specific area (e.g., a web application or network segment). The goal is to identify and assess technical vulnerabilities.

Ethical Hacking (Friendly Hacking)

A broader, less rigidly structured approach that mimics how real attackers operate – but with full authorization. This test examines technical, organizational, and conceptual weaknesses across the entire company.

A penetration test can be part of a comprehensive ethical hacking project, but it has a much narrower scope and follows a more standardized methodology.

7 Cybersecurity self-assessment

How well is your company protected and prepared against cyberattacks? Check now to see whether you meet the basic requirements.

1. Organization & Processes	Yes	no	don't know
Are the contact persons for IT security known (internal or external)?			
Is cybersecurity a regular topic in management meetings?			
Is cybersecurity part of your risk management strategy and addressed in management meetings?			
Have you fully captured and documented all your company's IT resources and business-critical processes?			
Are system- and vendor-independent backups available and restorable?			
Do you keep at least one backup in a secure, offline, external location?			
Do you regularly test the restoration of your data from backups?			
Do you use separate user accounts for administrative and non-administrative tasks?			
Do all users have only the access rights necessary for their assigned tasks (principal of least privilege)?			
Are access rights consistently assigned according to roles (e.g., accounting, HR, IT)?			
Do you use only personal user accounts and no shared accounts?			
Do you ensure that passwords for company and group accounts are changed immediately when employees leave the company?			
Do you deactivate user accounts immediately upon departures and update permissions after role changes?			
Have you identified and documented business-critical systems, data, and information?			
Are there defined fallback options such as backup equipment or emergency agreements with suppliers?			
Have you documented who works with which systems, including contact details?			
Have you defined immediate measures for emergencies, and is the emergency plan available offline, e.g., disconnecting affected systems from the network?			
Are there defined measures to quickly restore the ability to work (e.g., printing important contact details)?			
Are roles and responsibilities clearly defined in the emergency plan (e.g., IT response, legal clarification, communication, notification of authorities)?			
Do you regularly practice the emergency plan with your team?			

2. Employees & Awareness	Yes	no	do n't know
Do you conduct basic cybersecurity training for all employees?			
Does the training cover topics such as the benefits of IT security, handling logins, secure handling of information, and secure use of the internet and email?			
Do you repeat this training regularly (e.g., annually)?			
Do you use real-world examples like phishing, CEO fraud, or deepfakes in your training?			
Do you prevent uncontrolled device connections, such as plugging mobile phones into USB ports on work equipment?			
Do you foster a culture where employees can communicate openly and seek support when uncertain – without assigning blame?			
Do you make cybersecurity visible internally – e.g., through posters, newsletters, or short videos?			
Do your passwords use at least 12 characters and include uppercase and lowercase letters, numbers, and special characters?			
Do you recommend or use password managers in your company?			
Do you use two-factor authentication (2FA) wherever possible?			
Do you avoid reusing passwords? And regularly check whether employees' passwords have been compromised (e.g., via Have I Been Pwned?).			
Are there clearly defined and understandable user guidelines for email, internet, social media and mobile devices?			
Is the sharing of login data expressly prohibited?			
Do you raise your employees' awareness of suspicious emails (e.g., from unknown senders or with an unusual style)?			
Are warnings issued against using public, unsecured Wi-Fi networks?			
Is the installation of unknown apps or software regulated (desktop and mobile)?			
Is management also actively sensitized and acting as a role model in matters of cybersecurity?			

3. Technical protective measures	Yes	no	don't know
Are automatic updates enabled for operating systems, applications, and cloud services?			
Do you regularly check the update status of all devices, including printers, routers, cameras, and smartphones?			
Do you use centralized management tools for patch management (if technically and operationally feasible)?			
Are devices without update capability consistently disconnected from the internet or replaced?			
Do you use an endpoint protection solution (including antivirus software) to detect and prevent suspicious behavior?			
Is a firewall active that blocks unauthorized access?			
Do you use mobile device management (MDM) solutions for mobile devices, or are you considering using them?			
Do you use encrypted connections (e.g., VPN) for email, file transfers, and remote access?			
Do you consistently enforce strong authentication (two-factor authentication (2FA), passkeys) for external system access?			
Have you segmented your network to separate sensitive systems (e.g., accounting) from those available for general use (e.g., guest Wi-Fi)?			
Are unused interfaces such as open USB ports or Bluetooth disabled?			
Are server rooms physically secure, with no freely accessible network connections in public areas?			

4. Data Protection & Legal Information	Yes	no	don't know
Do you maintain a complete register of all personal data processed within the company (e.g., customer data, employee data, login data)?			
Is the purpose of data collection for each type of data (e.g., contract processing, marketing, HR) clearly documented?			
Have you checked whether there is a valid legal basis for each instance of data processing (e.g., consent, contract, legal obligation)?			
Do you apply the same technical security measures to personal data as to other company data (e.g., access control, encryption, backup)?			
Is access personal data restricted to authorized individuals?			
Is there a privacy policy on your website?			
Canindividuals request information about their data and have it corrected or deleted?			
Does your company have a defined procedure for handling data protection incidents (e.g., stolen customer data)?			
Can you ensure that reportable data breaches are reported to the FDPIC within 72 hours?			
Are affected individuals informed if a data breach may have compromised their rights?			
Have you concluded a written data processing agreement with all data processors (that is, partners who process personal data for your organization)?			
Do your IT service providers meet appropriate security standards (e.g. CyberSeal)?			

5. External Partners & Service Providers	Yes	no	don't know
When selecting IT and cloud providers, do you check for recognized security certifications (e.g., ISO 14001, CyberSeal)?			
Do you regularly request proof of current security measures, such as patch management, backups, and emergency procedures?			
Do you use tools like the Cybersecurity Quick Test for SMEs to clarify requirements with potential providers?			
Are there written agreements, including Service Level Agreements (SLAs), for cooperation with external partners, especially regarding data processing or system access?			
Do the contracts specify access rights, reporting obligations in the event of security incidents, and data processing location (e.g., Switzerland, EU, third country)ct?			
Are external partners involved in your emergency planning (e.g., who is informed, when, and how)?			
Do you plan and conduct joint security drills or tests (e.g., response to phishing or outages)?			
Do you receive regular, proactive security status updates from your service providers?			
Do external persons receive only the minimum access rights necessary (principle of least privilege)?			
Do you clearly document who has access to which systems – including duration and purpose?			
Are external access rights immediately removed when they are no longer needed (e.g., after project completion)?			

Preliminary note: This applies especially to SMEs that develop and operate their own solutions or that are directly connected to the internet.

6. Penetration Testing & Vulnerability Analysis	Yes	no	don't know
Do you clarify the scope of the test beforehand (e.g., network, web applications, remote access, WLAN)?			
Do you prioritize the implementation of identified measures from vulnerability analyses and penetration tests – especially in high-risk areas?			
Do you document the measures taken (e.g., updates performed, configuration changes)?			
Do you conduct follow-up tests to verify that identified vulnerabilities have been completely resolved?			
Are there clear criteria for when vulnerability analyses or penetration tests are performed (e.g., after updates, annually)?			
Are these tests an integral part of your IT security strategy?			

8 Attachment

Useful links

Authorities & Official Bodies

- **National Cyber Security Centre (NCSC) – "Protect your SME"**
  Official guidelines, checklists, and recommendations for SMEs.
  National Cyber Security Centre (NCSC) – Protect your SME
  National Cyber Security Centre (NCSC) – Information for companies
- **Federal Data Protection and Information Commissioner (FDPIC)**
  Guidelines, templates, FAQs, legal requirements for the Swiss Data Protection Act (DSG).
  Federal Data Protection and Information Commissioner (FDPIC) – Data Protection
- **Cyber attacks reporting form (NCSC)**
  Online incident reporting for businesses.
  National Cyber Security Centre (NCSC) – Reporting Form

Industry-specific support services

- **CyberSeal – Seal of Approval from the Swiss Digital Security Alliance**
  Recognizes IT service providers that guarantee an appropriate level of protection – helps SMEs select trustworthy IT partners.Alliance Digital Security Switzerland– CyberSeal
- **GObugfree – Ethical Hacking & Vulnerability Platform**
  Solution for SMEs to identify and report vulnerabilities.GObugfree
- **ITsec4KMU – Prevention and defense against cyberattacks for Swiss SMEs**
  Free, practice-oriented self-evaluation and guidelines for SMEs.
  ITSec4KMU
- **Suissedigital – SME Security Check**
  Low-threshold security check for SMEs in the digital communications industry.
  Suissedigital – SME Security Check
- **Swiss Cyber Defense DNA (SCD-DNA)**
  Model for the systematic recording and improvement of cybersecurity for SMEs.
  SWISS CYBER DEFENCE DNA

Awareness training & training materials

- **SUPER campaign**
  National campaign for basic cybersecurity protection – easy-to-understand tips for employees.
  Do it - Cybersecurity is S-U-P-E-R.ch
- **Cybernavi**
  Interactive information and training platform on cyber risks, specifically for SMEs and employees.
  Cybernavi

Norms & Standards (useful for supplier evaluations)

- **SNV – Swiss Association for Standardization**
  Information on ISO/IEC standards, including 27001, 27002 and 27701.
  Swiss Association for Standardization - SNV
- **SQS – Certification Body for Information Security**
  Certifications, audit models and industry standards (e.g. ISO 27001, data protection standards).
  Swiss Association for Quality and Management Systems | SQS Switzerland

Contact details for emergencies

Police (cybercrime):
Emergency number: 117. Cantonal police departments offer specialized cybercrime services.
www.fedpol.admin.ch

Federal Office for Cyber Security (BACS):
Reporting form for cyber incidents in Switzerland: Online reporting: NCSC - Reporting Form

Legal advice in cyber incidents:
Many cantons and industry associations offer specialized legal services. Alternatively:

- BDO Cybersecurity & Law: www.bdo.ch
- Data protection experts: www.edoeb.admin.ch

Glossary

2FA (Two-Factor Authentication)
An additional security layer that requires two independent factors for login (e.g., password + SMS code or app verification).

Asset
An asset of a company in an IT context, e.g. servers, software, data or end devices.

Backup
A copy of important data that is stored separately from the production system so that it can be restored after an incident.

Bluetooth
Wireless short-range radio technology. Open or unsecured Bluetooth connections can pose a security risk.

Cloud service
External IT resources provided via the internet (e.g., Microsoft 365, Google Workspace). Requires clear security and access rules.

Cyberattack
Attempts to compromise IT systems, steal or manipulate data, or disrupt operations.

CyberSeal
Swiss quality seal that distinguishes IT service providers who guarantee their customers an appropriate level of protection against cyber risks through suitable technical and organizational measures.

Data breach
Unauthorized access, loss, or disclosure of personal data. Legally reportable if there is a risk to affected individuals.

DLP (Data Loss Prevention)
Tools or policies that prevent confidential information from being lost or unlawfully disclosed.

Endpoint Protection
Security software for end devices such as laptops, smartphones, or servers. Detection of malware, suspicious behavior, and attacks.

Ethical Hacking (Friendly Hacking)
Authorized attack scenario in which all conceivable vulnerabilities (technical, organizational, procedural) are examined.
Pentesting is a part of this, but more narrowly and clearly defined.

Firewall
A security component that monitors data traffic and blocks unauthorized access.

IoT (Internet of Things)
Internet-connected devices such as cameras, sensors, or routers. Often a point of entry for security vulnerabilities if updates are missing.

MDM (Mobile Device Management)
Software for the central management and security of mobile devices such as smartphones or tablets.

Malware
Malicious software such as viruses, Trojans, or ransomware.

Network segmentation
Dividing a network into separate areas to limit attacks (e.g., guest Wi-Fi separate from accounting).

Emergency plan (Incident Response Plan)
A document that describes how a company should react in the event of a cyber incident.

Passkeys
Passwordless authentication method that uses cryptographic keys. Significantly more secure than traditional passwords.

Patch / Patch Management
Software update to close security gaps. Patch management = systematic updating of all devices and applications.

Pentest (Penetration Test)
A targeted, defined test that identifies weaknesses in a specified area. A structured, methodical approach.

Phishing
A manipulative message (usually an email) intended to steal logins, data, or money.

Ransomware
Malware that encrypts data and demands a ransom.

Rolling backup / offline backup
Backup stored separately from the network (e.g., external drive, tape). Protection against ransomware.

Social Engineering
Manipulation of people to obtain confidential information or access.

VPN (Virtual Private Network)
Encrypted connection that enables secure communication over the Internet.

WLAN (Wireless Local Area Network)
Wireless network. Public or poorly secured Wi-Fi networks can facilitate attacks.

Zero Trust
Security principle: "Trust no one – verify everything." No automatic relationship of trust within or outside the company.