Tips for SMEs

Company networks are generally more difficult to protect against cyber-criminal attacks than private ones. The reasons can be found in their increased complexity and the serious economic consequences of interruptions or breakdowns. Concise measures to minimise risks are therefore vital.

The most important points to remember:

- To weigh up risks and implement measures, you should draw on **guidelines and info sheets** issued by established institutions.
- Identify the **processes, systems and data** most valuable to your company, and start with those.
- To increase your information security, you should consider taking **technical** as well as **organisational measures**.
- Define **responsibilities, competences and contact points** for security-related issues.

Company networks are generally complex structures which grew over time, and which include various data flows and interfaces with customers and business partners. Even short-term disruptions, or even worse, breakdowns of this infrastructure, often result in serious economic effects for a company. This makes SMEs generally prone to greater risks of cyber-criminality than private individuals.

To increase SME resilience - their so-called ICT resilience - against such risks and to minimise risks in this regard, SMEs need to take suitable protective measures. Due to their complexity and volume, these are however generally quite cost- and resource-intensive. Careful consideration is therefore of utmost importance.

Use guidelines and info sheets

How should SMEs approach such an immense task? And how do they ensure that nothing is overlooked?

Many established institutions have looked into these issues and have intensively addressed the implementation of ICT protection measures especially for SMEs. Over time, various guidelines and info sheets have been drawn up this way. These enable SMEs to proceed both efficiently and effectively. It is therefore highly recommended to draw on such tools.

As an introduction to this subject matter, we would recommend the “Information security checklist for SMEs” (https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html) by NCSC. This very compact info sheet explicitly addresses Swiss SMEs and is meant to help them increase the information security of their system environment and inside their company network.

Identifying processes, systems and data

Where and with what should you start? Which processes, systems or data should SMEs address first?

The basis to answering this question is a (simplified) risk analysis. To this end, all processes, systems and data of particular importance for a company’s value-added chain should be identified and assessed as to how vulnerable they are to ICT risks.

Taking technical measures

Technical measures form the first line of defence to counter cyber-criminal risks. The catalogue of potential measures is a long one. But which measures are the right ones?

This question largely depends on each SME's specific threat situation. However, some technical measures can still be considered universal and therefore form part of every SME’s basic protection. The following are certainly measures which fall into this category:

- Regularly running data back-ups (https://www.ebas.ch/en/data-back-ups-in-an-sme-environment/)
- Installing and operating up-to-date antivirus software (https://www.ebas.ch/en/virus-protection-in-an-sme-environment/)
- Regularly running security updates (https://www.ebas.ch/en/patch-management-in-an-sme-environment/)

Taking organisational measures

Technical measures alone cannot provide extensive protection. Therefore, additional organisational measures will also always be necessary.

There is an extensive lists of organisational measures, too. Items of particular importance though are:

- Raising employee awareness and training them on a regular basis
- Establishing a strict password regime (https://www.ebas.ch/en/password-guidelines-for-sme/)
- Securing processes for critical applications (e. g. double verification principle with e-banking applications)

Defining responsibilities, competences and contact points

Who is responsible for data back-ups? Who is responsible for running security updates? Who can employees contact, for instance if they suspect a malware infection?

To run your operations smoothly, responsibilities, competences and ICT security contact points inside an SME should not just be defined, but all employees should also be familiar with them.

A suitable information platform can promote low-threshold access to the appropriate places. This will allow for reductions in reaction times in case of any and an increase in the notification quota.

Swiss SMEs are increasingly becoming the target of cyber-criminal attacks, with sometimes serious consequences for the company affected. Risk reduction measures are therefore vital.