7 tips for your business's cyber security

Cyberattacks can be categorized into active and passive according to their intention. The purpose of active attacks is specifically to attack you. In the case of passive attacks, individuals with malicious intent cast out a wide net and count on the likelihood that someone will get stuck there.

Are there any measures to minimise the damage caused by a cyberattack and could these also save from a passive attack net? In the case of an active attack, it is very likely that some kind of a security gap will still be found for entrance. However, if you are 100% convinced that your company's cyber defence system is impenetrable, then it is useful to order a pen-test (i.e. a simulated attack on your company) to test the capability of your company's cyber defence system. Below we outline some measures that could be useful in limiting the extent of the damage caused by a cyberattack and that could save from a passive attack net.

Due diligence measures

1. **Application of personal cyber hygiene**

Personal cyber hygiene usually refers to people's routine behaviour on their devices and on the Internet. Like washing hands, good cyber hygiene can prevent your computer systems in the fight against viruses (or at least reduce the likelihood of infection).

Personal cyber hygiene includes, for example:

· using a strong password – it is not a good idea to use the same password for multiple accounts. In particular, the use of the same password in professional and private life should be avoided.

· two-factor authentication (2FA) – even if your password is guessed, people with malicious intent cannot access your information.

· the ability to recognize phishing email – the more typical phishing email features are, for example, when the sender's name and email address do not match; hyperlinks in the text of the email message lead to an unfamiliar website (this can be checked without clicking on the link, by holding the cursor above the link); or countless misspellings in an email message that should have been sent by an official company.

· regular updating of the software – constant postponement of updates means that the security systems of your devices have not been updated either. Using older versions means that hackers have had more time to find vulnerabilities in the version of the system you are using.

The company's cyber hygiene also includes the training of employees so that the employees can identify potential threats and do not accidentally become a "weak link" through which malicious individuals can penetrate the company's internal systems.

Of course, corporate cyber hygiene is better if employees do not use their work email address for private operations like logging into an Amazon or Netflix account. In such a case, the email allegedly received from Amazon on the work email immediately raises doubts and, as a rule, people do not start clicking on various hyperlinks there – naturally you do not let an uninvited guest to your home.

2. **Knowledge of the company and its security risks**

As a manager of a company, it is important to know what your company's security risks are and what information may seem attractive to malicious individuals.

When it comes to the attractiveness of the data, it is, for example, worth analysing which data can cause the most damage to the company. Such data may include industry trade secrets, patient health data collected by a medical company or financial data of clients. Even if a cyberattack is not aimed at stealing this data, restricting access by hostile intruders to certain data can also harm the company.

In addition to identifying valuable data, it is also important to protect it. In the case of security risks, it is worth analysing, for example, whether all information on the company's intranet can be accessed or access restrictions are in place. The potential damage of a ransom attack, the most common type of a security incident at the moment, can be reduced by backing up your data. More information on cyber risk analysis can be read in Estonian HERE or English HERE.

In the ideal world, all employees have the most modern and properly updated security systems, from which no evil can get through, and all company information is equally and perfectly protected. In the real world with limited resources, prioritising is important. Thus, company managers should be able to identify their company-specific risks and, as a matter of priority, address the threats with a higher potential for harm.

3. **Regular checks**

Does your company's cybersecurity monitoring take place regularly or only when the damage becomes public? Even if it is not reasonable for a company to hire a separate specialist to deal with cybersecurity, a proactive approach will help to significantly reduce the likelihood and extent of the damage. However, for larger companies, investment in the programmes with real-time control capabilities may be necessary. This, as a rule, allows for faster detection of an attack and can reduce the extent of the damage caused.

You should pay attention to your company's cybersecurity already when developing the service and planning cyber costs in the company's budget of expenses in good time. Regular risk assessment and updating the necessary software and action plans will also contribute to better implementation of the above-mentioned due diligence measures.

However, the cyber incident happened – what to do?

4. **Notify CERT**

CERT-EE assists the authorities in Estonia in dealing with security incidents and provides technical support in resolving incidents. CERT is also coordinating the response to incidents occurring simultaneously. You can read more about CERT HERE.

If among other things, personal data was leaked because of a security incident, it may be necessary not only to inform CERT but also the Data Protection Inspectorate.

5. **Keep records, as much as you can**

Data related to security incidents may be needed later – i.e. when the incident occurred, what was the nature of the incident, how the systems were accessed. Even if, based on this information, the organizer of the security incident is not found, it can help prevent attacks of the same kind. This information will also help to strengthen your company's security system.

6. **Assess possible legal liability**

If confidential information or personal data were collected from your databases as a result of a security incident, the consequence may be a civil liability to partners, customers or employees. This does not automatically mean the need to go to court, but the involvement of legal experts at the moment of becoming aware of the incident will help to plan further activities more effectively and assess the extent of the potential damage. A legal analysis of the situation will also help determine whether you may have a claim against any of your service providers or partners.

It is certainly not a good solution to ignore the problem without analysing it, as the company may be obliged to inform its cooperation partners or customers of a security incident due to an agreement between them or under the General Data Protection Regulation of the European Union (GDPR).

7. **Revert to the implementation of due diligence measures**

The security incident showed where the gap in your company's security systems is. This is an opportunity to improve your security systems and to complement due diligence.

(Author: Gerda Grauberg)

LIISI JÜRGEN
ATTORNEY AT LAW,
PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE