LUXEMBOURG CYBERSECURITY WEEK – 19 to 29 OCTOBER : IS YOUR IT SECURITY GOOD ENOUGH?

The fact that the current health crisis is ongoing, and that therefore teleworking continues to be encouraged, puts your company at risk of becoming victim of cyberattacks.

The main goals of hackers during these cyberattacks are to gain unauthorised access to and steal confidential information or data, and to extort money from their victims.

The consequences of these cyberattacks can cause extensive damage, in particular in terms of:

- Cyberstalking;
- Personal data loss and data breaches;
- Theft of know-how and trade secrets;
- Forced shutdown of company's business activities;
- Financial losses; and
- Loss of reputation.

Raising awareness and knowing how to react to cyberattacks are key in the fight against hackers.

What is considered a cyberattack ?

- **Phishing**: this generic term is often used for situations involving sending bait, i.e. a fraudulent communication which may take the form of an email, a text message or a telephone call aimed at obtaining confidential information from the recipient, including confidential financial data, specific to the person, the targeted company or its managers, for example. Different types of phishing attacks can be distinguished according to their modus operandi:
    - **Spear Phishing**: sending personalised emails to employees and managers of a company;

    - **Whaling**: sending a personalised email to political figures and top executives;
    - **Smishing**: cyberattacks send via text messages; and
- **Vishing**: cyberattacks via phone calls.
- **Trojan horse:** these are often sent by email with an attachment containing malware which can infect a computer or even a whole computer system.
- **Ransomwares:** these are designed to enter the IT system to steal confidential data andrestrict access to the computer system by encrypting the system and data. In order to remove the encryption, the victim is asked to pay a high ransom.

How to react ?

In general:

- Be vigilant when receiving unusual requests by email, calls or texts;
- Check the content of emails, in particular for spelling and syntax errors which can provide clues;
- Check the sender’s email extension;
- Check that your connection is secure;
- Copy and paste part of the request into your search engine to check if such a request has not already been pinned before replying to it; and
- Contact the sending company to check the legitimacy of the request and, if necessary, inform it that it is also a victim.

Within the company:

- Train your employees and make them aware of good practices;
- Inform your employees about the communication and collaborative work tools available to them;
- Put in place data protection and data security policies;
- Have a password policy in place requiring all employees to have strong and regularly updated passwords;
- Be equipped with professional anti-virus software and blocking tools for access to malicious sites;
- Be equipped with security tools that render your IT environment as robust as possible, such as a dual authentication system; and
- Get in touch with an independent insurance intermediary in order to find out about the various offers available in terms of cyber insurance policies.

Our Media, Data, Technologies & IP Department is happy to work alongside you to help you implement these good practices within your company.

If you are the victim of an attack, please do not hesitate to contact us.