FEDIL

Publication

CYBERSECURITY CHECKLIST

Ladies and gentlemen,

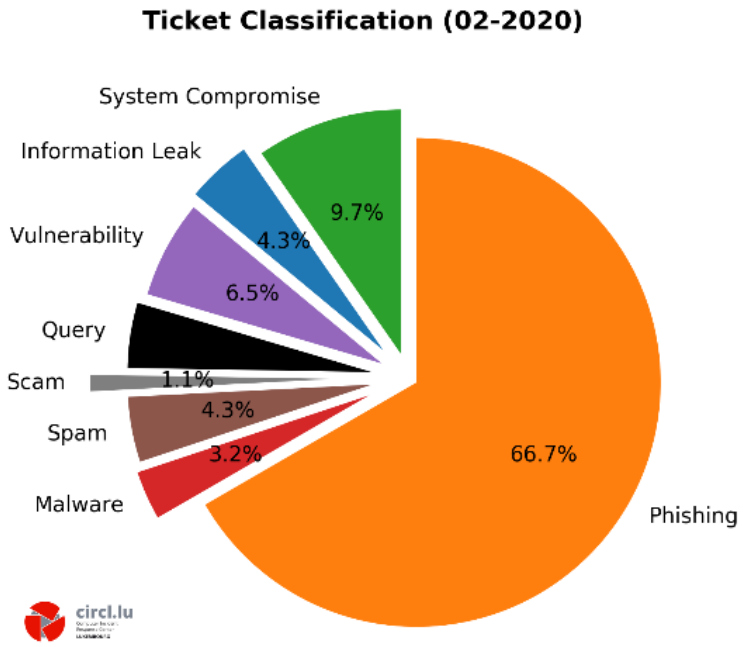
Dear members,

FEDIL, in collaboration with SECURITYMADEIN.LU, would like to draw your attention to certain elements of cybersecurity to be taken into consideration in order to limit the risks and to prevent as far as possible the cyber attacks that are multiplying and diversifying.

It is constantly important to keep a close eye on cybersecurity within your company and to ensure that adequate measures are put in place. This is more important than ever in the context of the coronavirus crisis, due to the massive recourse to teleworking, which opens up opportunities for attackers. Teleworking encourages the use of e-mail for communication, creating perfect conditions for e-mail fraud schemes.

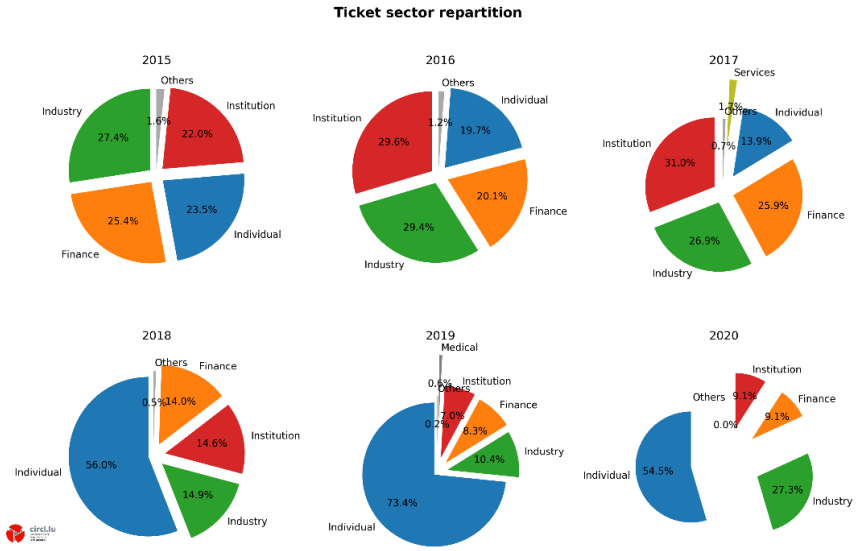
Indeed, even if the number of attacks is not increasing significantly, a certain type is experiencing a resurgence, namely phishing. The CIRCL figures from last February show the importance of such attacks with 66.7% (see graph below). This is where the problem lies, as this type of attack exploits the human factor and is aimed directly at users who are often not sufficiently prepared to identify a fraudulent email. The motivation for these attacks is primarily financial. The aim is to monetize the information obtained against a ransom, the famous “ransomware”.

The latest local examples to date have targeted the companies Cactus and Tarkett, mentioned in the press. In the case of Cactus, the group was the target of ransomware REvil. The categories of stolen data held by the hackers were published on the internet to induce the group to give in and pay the ransom demanded.



It is therefore essential to make company employees aware of the risks that may be incurred as a result of misuse of the devices, bad behaviour and the consequences of a cyber attack.

In addition, as shown in the graph below, all sectors of activity dependent on IT infrastructures, regardless of the size of the company, are targeted.



Consequently, FEDIL would like to remind you some practical advice offered by SECURITYMADEIN.LU

DEVICES

– Take special care to ensure that devices such as USB sticks, phones, laptops or tablets are not lost or misplaced.

– Preferably use the professional computer. If this is not possible, check for updates before using the home computer. Set up separate accounts for family members.

– Ensure that each device has the necessary updates, such as operating system updates (such as iOS or Android) and software/antivirus updates.

– Ensure that the computer, laptop or device is used in a safe place, for example where it can be seen, and minimise who else can see the screen (especially if the person is working with sensitive personal data).

– Lock the device if it is to be left unattended for any reason.

– Make sure that the devices are turned off, locked or stored carefully when not in use.

– Lock the camera when not in use.

– Use effective access controls (such as multi-factor authentication and strong passwords) and, where appropriate, encryption to restrict access to the camera and to reduce the risk if a device is stolen or lost.

– When a device is lost or stolen, take immediate action to ensure remote memory wiping, if possible.

EMAILS

– Use business email accounts rather than personal accounts for work-related emails involving personal data. If personal email is used, ensure that the content and attachments are encrypted and avoid using personal or confidential data in the subject lines.

– Before sending an email, make sure you send it to the right recipient, especially for emails involving large amounts of personal data or sensitive personal data.

– If possible, prefer to send encrypted emails every time.

CLOUD AND NETWORK ACCESS

– Configure the devices beforehand by setting up tools such as firewalls and IT hygiene rules.

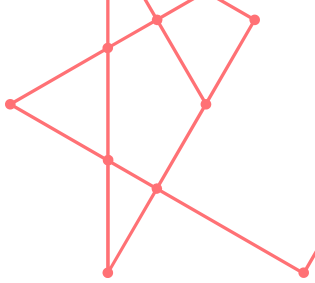
– Use a virtual private network (VPN) to ensure a direct and secure connection with the company's internal network and to protect data transfer from any malicious act.

– Do not connect to any public Wi-Fi network, unknown or uncontrolled. These networks are often used by malicious actors as preferred attack vectors to target companies through their employees.

- Connect to 3G or 4G networks if you do not have access to a secure Wi-Fi connection.

– To the extent possible, use only the organization's trusted networks or services and follow all organizational rules and procedures regarding cloud or network access, connection and data sharing.

– If you work without cloud or network access, ensure that all locally stored data is properly and securely backed up.



– Remote access software (such as TeamViewer) should be used very carefully and only by authorized employees. It should always be updated and used only when absolutely necessary.

– Check the reliability of video conferencing platforms. In particular, where files are stored when they are transferred. The same applies to file transfer platforms.

VIDEOCONFERENCE

The use of video conferencing also involves risks. There are mainly 3 types of risks:

– The main risk to be covered is data leakage through passive and unauthorized eavesdropping of confidential discussions.

– Risks related to an invasion of privacy following a misuse, configuration or software flaws allowing for example: taking control of the organizer's camera without his knowledge, recording the call or sending user account data to third parties without authorization .

– Documents, presentations, notes and other chat messages exchanged (in addition to voice) that may contain sensitive information and may end up on uncontrolled servers.

We invite you to follow the recommendations of SECURITYMADEIN.LU in order to limit the risks at the following link: VIDEOCONFERENCING AND CYBERSECURITY: HOW TO LIMIT THE RISKS?

Furthermore, it should be noted that attackers are trying to take advantage of the coronavirus crisis by capitalizing on the fear and uncertainty generated by COVID-19. Below is a non-exhaustive list of cases that you could be confronted with.

1. Coronavirus websites: Some attackers design coronavirus-related websites to invite you to download an application to keep you informed of the situation. But this is a trap!
2. Security measures against coronavirus: you are invited to download a pdf with tips to protect yourself against the virus. But the pdf file contains malicious code...
3. Fake antivirus against coronavirus: if you install it, it creates backdoors on your computer.
4. Impersonators posing as the Red Cross sell COVID-19 tests at home.
5. A fake message from the WHO (World Health Organization) installs spyware on your computer.
6. Blackmail through e-mails that threaten to infect you with coronavirus.
7. Phone hoaxes from the CDC asking people to reserve COVID-19 vaccines.
8. Scams promising $1,000 checks as economic aid in the event of a pandemic.
9. Various "stay safe from coronavirus" scams.
10. COVID-19 reduction codes to sell malware and counterfeit products.
11. Instant communication platforms are prime targets for cybercriminals.
12. In this context, the number of fake news is also on the rise.

Finally, we would like to underline the emergence of another phenomenon that allows the employee to access the company network but whose impact is difficult to know. This is the use of the private sphere and the sending of extortion emails with the subject "I know your password". The attacker claims to have compromising information about the person and demands payment of a ransom. We strongly recommend that you make your employees aware of this

type of attack and invite them to follow the recommendations of SECURITYMADEIN.LU : SEXTORTION SCAM E-MAILS: "I KNOW YOUR PASSWORD"

Coronavirus crisis or not, it is essential to act with the utmost caution when consulting emails and websites and in case of doubt, it is strongly recommended to consult and alert the IT department and cybersecurity specialists.