PRACTICAL **GUIDE**

CYBERSECURITY

Understanding, preparing for, and responding to an attack

CHAMBER
OF **COMMERCE**
LUXEMBOURG

POWERING BUSINESS

ENGLISH

Introduction

Due to its economic landscape, which includes banking and insurance sector activities and European institutions that process sensitive data, Luxembourg has considered cybersecurity to be the backbone of its digital economy since the early 2000s.

So much so that all of the companies and/or institutions active in the cybersecurity sector represent an ecosystem* consisting of more than 370 stakeholders, 30% of which have cybersecurity as their core business and 25% of which are startups. Together, they form a net that works on a global level to raise awareness, protect, and respond to the country's companies in the event of an attack.

These players include the Luxembourg House of Cybersecurity, the backbone of cyber resilience in Luxembourg. It is the leading figure in the field, supported by its two centres, the National Cybersecurity Competence Center (NC3) and the Computer Incident Response Center Luxembourg (CIRCL). It offers advice, services and training for companies in the Grand Duchy of Luxembourg.

Because unfortunately, cybercrime has become a real business throughout the world. Luxembourg is no exception, as local companies that have been victims of attacks attest to in the testimonials in this guide.

The important thing in this case is to be prepared and aware of the risks and impact that a cyberattack can have on a company. The goal is to protect the data which, if lost or stolen, could jeopardise the survival of a company. To do this, there are tools available such as simulation exercises or penetration tests that enable the various possible scenarios to be identified and prevented.

This guide provides some keys to understanding, preparing for, and responding to a cyberattack.

* https://cybersecurity.lu

Disclaimer
This document is an informative overview for professionals about cybersecurity. It does not replace the necessary consultation of specialists and legal provisions on the subject. It provides the names of some technical solutions but is not intended to be exhaustive.

Summary

A **Chamber of Commerce** publication
in partnership with **MindForest**
and the **Luxembourg House of Cybersecurity**
February 2023 (update of a brochure initially
published in November 2021)

Facts and figures[1]

PHISHING[2]
(see Types of cyberattacks on p. 12-13)
accounts for two thirds of the 1,114 incidents recorded in Luxembourg in 2020 by the CSIRT[3]. This is followed by denial-of-service attacks (DDoS - aimed at making one or more services unavailable), identity theft, and premium rate calls.

CLIENTS OF LUXEMBOURG BANKS
are particularly targeted by phishing campaigns, as banking institutions cannot be attacked directly
(see interview with Pascal Steichen).

VICTIMS OF CYBERATTACKS IN LUXEMBOURG
(according to incidents reported to CIRCL in 2020):

private individuals: 54%

financial sector: 24%

institutions: 12.5%

industry: 9%

[1] Figures based on reported incidents only. They therefore do not allow the full extent of the phenomenon to be measured.
[2] Phishing: attack intended to obtain connection details in order to commit fraud
[3] CSIRT: Computer Security Incident Response Team of POST CyberForce, established in 2020 to better combat cyberattacks in Luxembourg
[4] https://fit4cybersecurity.nc3.lu/
[5] CIRCL: Computer Incident Response Center Luxembourg, a governmental body in charge of collecting and analysing incident reports submitted by companies or individuals. www.circl.lu/opendata/statistics/#circl-operational-statistics

COMPANIES CAN SELF-ASSESS THE MATURITY of their risk mitigation measures using the Fit4Cybersecurity tool[4] of the National Cybersecurity Competence Center - NC3. The answers provided to the questionnaire, analysed by NC3, show that for VSEs and SMEs:

80% **have weak passwords,** easily guessed or created by the users, without protection

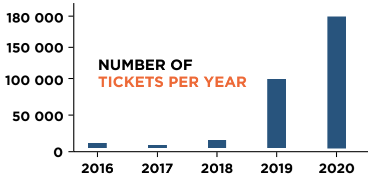
71% **have insufficient measures for the protection** of personal data and compliance with the GDPR.

70% **of VSEs and 64% of SMEs have insufficient backups,** leaving them vulnerable to crypto ransomware *(see interview with Paul Feider of Giorgetti p. 8-9).*

63% **of VSEs and 56% of SMEs do not regularly use the antivirus software they have, do not check that it is up-to-date, or do not have any antivirus software at all.**

60% **of VSEs and 54% of SMEs have vulnerable user workstations** (no procedure for authorising software downloads, machines not locked, not updated, etc.)

55% **of VSEs and 46% of SMEs do not train their staff in the software used, in cybersecurity, or in data sensitivity.**



THE NUMBER OF ATTACKS IS EXPONENTIAL:
180,000 tickets incident reports were opened with the CIRCL(5) in 2020, compared to 100,000 in 2019 and 15,000 in 2018. The percentage of phishing attacks is growing: from 16% in 2017 to 71% in 2020 and 83% in 2021.

Insights from Pascal Steichen, Director, Luxembourg House of Cybersecurity

What are the current trends in terms of cyberattacks?

Phishing has increased significantly worldwide in recent years: this is the trade-off for the progress that has been made in strengthening IT systems. For petty criminals, the entry ticket to infiltrate systems is becoming too high, while humans themselves have not been 'upgraded' and can have their identity stolen. Moreover, email, which is the ultimate gateway to trapping victims, has become widespread. We have all become dependent on technology, which provides a global playground. Even more so with teleworking, which has not escaped the attention of hackers, who have focused their attacks on videoconferencing tools, VPNs, etc. and have broadened their scope to sectors other than finance: hospitals, industry. Fortunately, in Luxembourg, we have not had any major attacks on our hospitals or government sites, as in other countries.

Are small companies of interest to hackers?

They systematically try to get in wherever they can, in large and small companies alike, and enter through the first door that opens. So any company can be a potential victim. The advantage of SMEs is that communication is more direct, and a suspicious e-mail can be identified more quickly.

How would you describe the maturity of Luxembourg companies in terms of cyber security?

They are rather well positioned. We have seen a real awareness of the risks linked to cybercrime in recent years. More and more companies are coming to us for advice. Unfortunately, it is not a question of if we will be attacked, but when. It is even likely that one has been already and is unaware of it, and the task is then to diagnose the possible traces of intrusion in one's system or networks. Often, an intrusion may have taken place months or even years before, and only do visible damage much later.

What are your recommendations?

There is still a lot to be done in companies to secure their infrastructures. And connected objects, which are often poorly protected, offer a significant scope for attacks. It is more important than ever to be vigilant and not to let up on raising awareness among staff and clients.

The challenges

For organisations, the challenges of cybersecurity are numerous. A cyberattack has consequences on many levels, both immediately and over the long term, and can result in many hidden costs.

Although companies are victims of cybercrime, they are still responsible for their data and protecting it. From the moment of detection of the cyberattack to a return to full normality, it can take up to several years, during which time the organisation will put in place an action plan to repair the damage.

Corporate image

Hacker attacks can have a significant impact on a company's long-term image. They can give investors the impression that the company is not taking cybersecurity seriously enough, and they can affect customer confidence, which in the long run can also jeopardise the company's business.

Legal issues

The legal implications are highly sector-specific. However, the GDPR establishes a European data protection regime. A breach of this regulation can cost the offending company up to EUR 20 million or 4% of the group's annual turnover.

Financial challenges

The loss of sensitive data, such as trade secrets or customer data, can result in financial damage:

- **direct:** court and legal costs, public relations, high fines, compliancy, client notification of the attack, etc.
- **indirect:** reduced sales resulting in a net decrease in turnover, loss of customer confidence, increased insurance premiums, damage to the brand, possibly even revocation of operator licences, etc.

In highly regulated areas, such as the financial sector in particular, strict quality criteria are set for cybersecurity. If they are not met, severe sanctions are applied (in Luxembourg for example by the CSSF, the ILR or the CNPD for non-compliance with data protection).

Breach of confidentiality

Confidentiality is simply ensuring that no unauthorised person gains access to data in the computer system or to paper files. It therefore has a direct link to the GDPR. It is about personal but also confidential data.

Breach of integrity

The principle of integrity recuires that data can be guaranteed at all times not to have been changed or deleted. Continuous monitoring of possible changes to data must be undertaken. Integrity can be affected by individual employee errors and therefore requires training in processing data.

Impaired accessibility

The continuity of business activities requires data to be accessible at all times. This access can be impaired, for example, by a denial of service. The more that normal business operations are supported by IT, the greater the financial damage can be if data is not accessible.

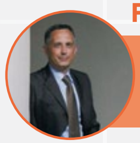
In addition to the possible consequences for the company if information security is not taken into account, employees can also be targeted by cybercriminals, for example by blackmailing them with private photos, which can also have consequences for the company.

Testimonials

(Collected in November 2021)

Felix Giorgetti (construction) and **Victor Buck Services (VBS)** (information processing and publishing service) were both victims of an attack in 2020. Their managers look back at the circumstances and consequences of this security incident.

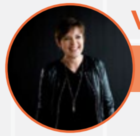
FELIX GIORGETTI



Paul Feider
Administrative, Commercial and Financial Director

Jean-Marc Sertic
IT and Organisation Manager

VICTOR BUCK SERVICES



Edith Magyaricks
CEO

FIRST SIGNS OF THE ATTACK

Felix Giorgetti: On 17 January 2020, we no longer had access to our documents and applications. We soon realised that we were victims of ransomware. **Analyses revealed that it had already infiltrated our systems in autumn 2019.** The hackers asked us to transfer USD 500,000 in bitcoins to an account, with a four-day ultimatum, or they would increase the ransom to USD 1 million

VBS: Our systems were sabotaged in August 2020. For one week, we had no access and were unable to serve our clients. This attack had a domino effect on them.

THE CONSEQUENCES FOR CLIENTS AND THE COMPANY

Felix Giorgetti: We could no longer carry out our most basic activities, supported by IT: communicating, accessing plans to work on the building sites and data to issue invoices. **It took several months to get our system fully operational again.** With the help of our IT department and external consultants, we have been gradually rebuilding it: separating our internal network from the external network, transferring data selectively and under stringent supervision, while making changes to increase security.

VBS: Fortunately, investigations to date have not shown any leakage of client data, but clients had to urgently establish fallback solutions. **Most of them have been supportive and remained loyal to us once the situation was resolved, but some have taken longer to decide to reconnect.** There was a definite impact on 2020 revenue due to this discontinuation of activity with some clients. The impact continues into 2021 as some clients only reconnected this year.

INITIAL REACTIONS

Felix Giorgetti: We immediately contacted CIRCL and the police, and then our internet service provider.
We disconnected all Internet connections so that the attack would not spread in our systems. The ransomware had also attacked some backups in our cloud, but fortunately not the backup of the system. So we were able to recover our data.

VBS: From the beginning, we were transparent with our staff as well as our clients. **There is no shame in being the victim of an attack.** It can happen to anyone. We specifically wanted to talk about our unfortunate experience so that it could be of use to others. It is often the case that intrusions come from external parties, but it is not well known that staff, through negligence or lack of awareness, can be the vectors of threats.

IMPLEMENTATION OF LONG-TERM MEASURES

Felix Giorgetti: We have invested heavily in the security of our systems, trained staff, introduced stricter password rules and a more targeted back-up system. In addition, we have limited access to our IT system to certain hours, which allows us to better monitor the activities on the servers and to act more quickly if any signs point to an attack.

VBS: Among the measures we have implemented, we have made our staff, whatever their position in the company, aware of the risky behaviour that can lead to breaches. Each person must understand that they have a share in the responsibility.

ADVICE TO BUSINESSES

Felix Giorgetti: The lesson is that it can happen to anyone, regardless of the size of the company. It is important to find the right balance between security and operationality: pragmatism is the key word. In addition, a sophisticated backup system is essential in order to have a plan B in case of an emergency and thus to minimise the loss of business and financial damage. It is important that people talk about this topic and that other companies speak up. **In the fight against cybercrime, we can learn a lot from each other.**

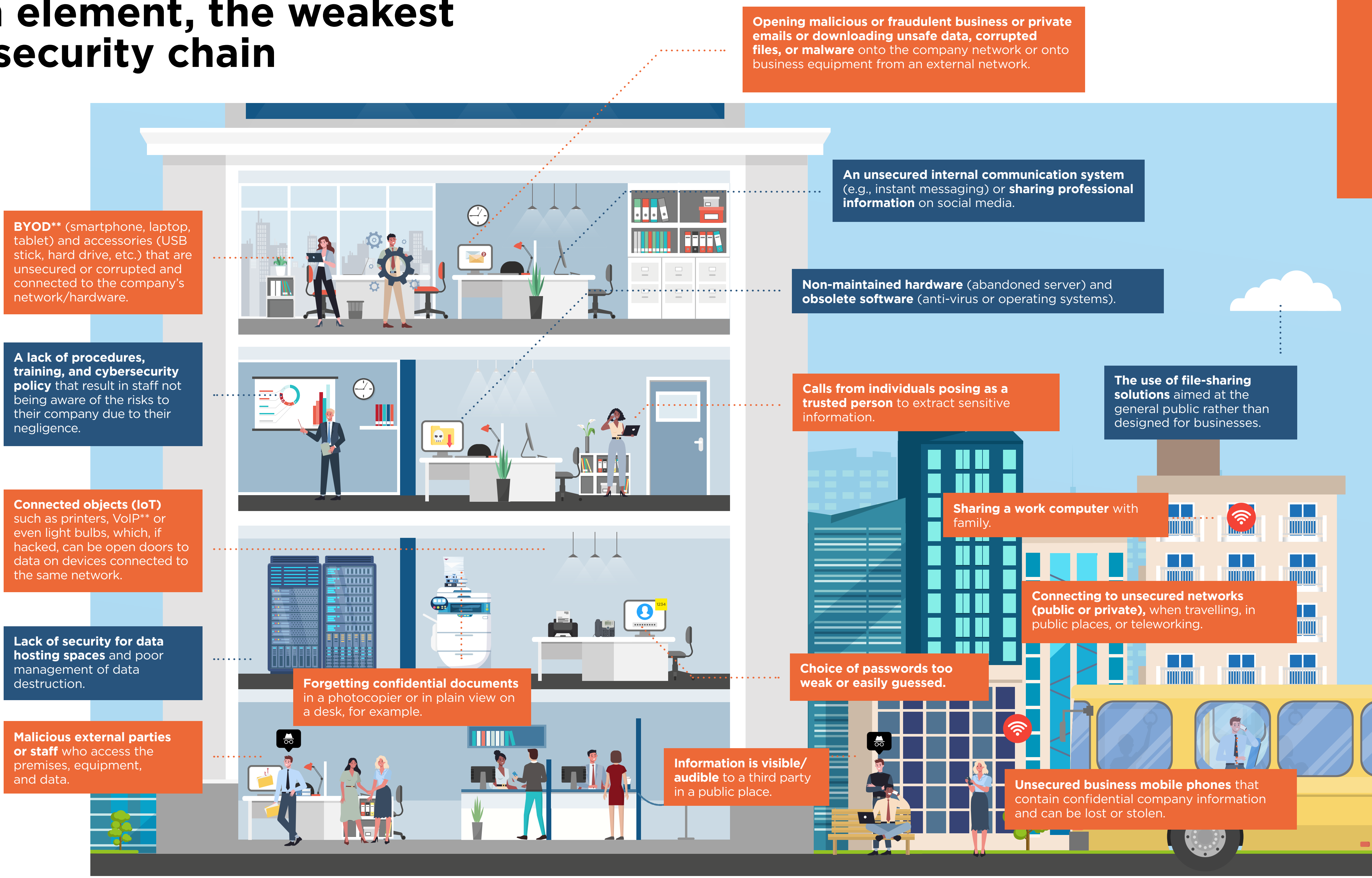
VBS: Our company, because of its activity, already had a solid framework for cybersecurity, which is not available to all SMEs. **Without investing too much, it is possible to prioritise in order to ensure that critical activities are secured, and thus to be able to continue operations and limit the impact.** This is a real issue for business leaders, who need to have at least some knowledge of cybersecurity and the risks involved, and thus prevent incidents that can occur.

The human element, the weakest link in the security chain

'The human factor can present a weakness, but can also be the first line of defence against intrusions, provided people have been informed and trained. For small companies, raising staff awareness of suspicious emails is the most effective way of dealing with threats, and is less costly than technical investment.'

Pascal Steichen,
Director,
Luxembourg House of Cybersecurity

Unfortunately, all too often, small businesses think they are immune because they are not attractive enough for hackers. This is a mistake! Hackers can use small companies, which are less well protected and often suppliers of large groups, to indirectly reach the latter. Making employees aware of the fact that their negligence, ignorance, or naivety can constitute a vulnerability makes it possible to increase the resilience of one's organisation, even if it is not a final solution.



Opening malicious or fraudulent business or private emails or downloading unsafe data, corrupted files, or malware onto the company network or onto business equipment from an external network.

BYOD** (smartphone, laptop, tablet) and accessories (USB stick, hard drive, etc.) that are unsecured or corrupted and connected to the company's network/hardware.

A lack of procedures, training, and cybersecurity policy that result in staff not being aware of the risks to their company due to their negligence.

Connected objects (IoT) such as printers, VoIP** or even light bulbs, which, if hacked, can be open doors to data on devices connected to the same network.

Lack of security for data hosting spaces and poor management of data destruction.

Malicious external parties or staff who access the premises, equipment, and data.

Forgetting confidential documents in a photocopier or in plain view on a desk, for example.

An unsecured internal communication system (e.g., instant messaging) or **sharing professional information** on social media.

Non-maintained hardware (abandoned server) and **obsolete software** (anti-virus or operating systems).

Calls from individuals posing as a trusted person to extract sensitive information.

The use of file-sharing solutions aimed at the general public rather than designed for businesses.

Sharing a work computer with family.

Connecting to unsecured networks (public or private), when travelling, in public places, or teleworking.

Choice of passwords too weak or easily guessed.

Information is visible/ audible to a third party in a public place.

Unsecured business mobile phones that contain confidential company information and can be lost or stolen.

KEY

🟧 Human error
🟦 Company negligence

**BYOD = Bring Your Own Device, the practice of using personal equipment in a professional context.*

*** Phones connected to the Internet*

Types of cyberattack

Social engineering

Psychological manipulation techniques are used on the telephone, in person, by email, or on social media to get a person to disclose information without realising it.

Ransomware

A locker ransomware is a piece of malicious software that takes a machine hostage and makes it inaccessible. It often does not affect the data, but prompts the user to pay for the use of their machine.

Cryptoransomware
(the most common type of ransomware) silently encrypts data, gradually making it inaccessible, targets all other machines connected to the network, searches for backups, and demands payment of a ransom to recover the lost data.

Phishing

The cybercriminal pretends to be a trusted third party or plays on human weaknesses (kindness, pity, greed, curiosity, libido, fear, laziness, etc.), prompting the opening of an attachment, a website, or the sharing of a password, resulting in the installation of malware or the loss of data.

Fake president fraud

A member of staff thinks they are in contact with someone in the top management of their company or the parent company. The attacker searches for information on social media to find a potential victim (profile susceptible to pressure). After several exchanges to establish trust, they request a payment/transfer of documents urgently and confidentially.

Malware (malicious software)

This is a programme developed to harm a computer system.

There are several types:

Virus: performs a malicious task on the victim's machine (stealing data, making it inaccessible, modifying it) and spreads itself to any compatible machine that connects to the infected machine. It is often transmitted via attachments or malicious storage media.

Trojan horse: often in the form of software, it opens a channel for an attacker to do whatever they want on a machine.

Spyware: sends data about what the user of a machine is doing (without warning) for commercial use or spying.

A poorly protected password

Attacks consist of guessing a password by trying all possible combinations that could form the password, using pre-defined word dictionaries that can be adapted to target a victim (e.g., first name+date of birth combination).

Denial of service

The fraudster attempts to disrupt the normal operation of the targeted server, service, or network by overwhelming it with a flood of internet traffic.

There are various signs that may indicate an attempted cyberattack:

- Strange or incorrect email address
- Spelling or syntax errors
- Link not corresponding to a known address or context
- Attachment is in a peculiar format (Word with macros, zip,...)
- Request for highly sensitive information such as login or password

The right reflexes after detecting a cyberattack:

- Contact the company's IT support in case of doubt (internal or external service provider)
- Report the incident to the CIRCL
- Contact the bank (if there is a risk of access to bank accounts)
- Change passwords
- Disconnect devices from the network, wired or wireless
- Call in experts *(see Cybersecurity professionals p. 16-17)* to help rectify the situation and ensure future protection

Don't forget

- Communicate with staff and clients, be transparent
- Raise awareness and train staff to increase company resilience
- Make regular and offline backups of data

Steps to protect your company

STEP 1
Conduct assessments (regularly)

Conduct assessments of the maturity of the company, exposure to risks, the security of data.
(see Tools and solutions p. 20-21)

Have IT systems audited to see if there is already evidence of a possible intrusion.

Take inventory of:

- existing access to sensitive information (staff, external service providers, etc.), including physical data (files);
- devices connected to the network (watch out for devices brought in by staff) and ensure they are reliable;
- the most sensitive and vital information for the company and ensure that it is secured;
- attractive assets that could be coveted (client portfolios, financial documents, personal data, ...) and ensure compliance with the GDPR;
- existing protective measures (anti-virus, firewall, etc.)

STEP 2
Prevent risks

Establish a cyber security strategy (security policy) and draw up a contingency plan with clear processes and procedures that are updated regularly. Explain them to staff and ensure that they are read and understood, for example by having a document signed.

Create an internal support structure and incident management (depending on the size of the organisation).

Know the key professionals/institutions in the field of cybersecurity. *(see Cybersecurity professionals p. 16-17)*

Ensure regular updating of software and operating systems.

Ensure that a regular back-up is set up and disconnected from the network (so as not to be infected in the event of an intrusion).

Take into account the different work configurations (in person, virtual, while travelling...).

Change passwords and have them changed regularly.

STEP 3
Raise awareness and train staff

Raise awareness of the main existing threats through internal training or training developed by experts.
(see Tools and solutions p. 20-21)

Explain the emergency plan and existing processes and test them as far as possible.

Carry out simulations.
(see Cybersecurity professionals p. 16-17)

Provide regular reminders and updates.

Set up a good practice guide for staff, including all key information.

Cybersecurity professionals in Luxembourg

PRIME MINISTER

NATIONAL STRATEGY

Interministerial Coordination Committee for Cyber prevention and Cybersecurity

PUBLIC SECTOR

High Commission for National Protection

Responsible for critical infrastructure protection and counter-terrorism coordination

GOVCERT.lu

Single point of contact dedicated to the treatment of IT incidents affecting the information systems of the government and operators of critical infrastructures (private and public) defined as operating in Luxembourg

PRIVATE SECTOR

LHC Luxembourg House of Cybersecurity

Backbone of leading-edge cyber resilience in Luxembourg.

LHC aims at capitalizing on and further developing innovation, competencies, collaboration and capacity building in the field of cybersecurity.

PROTECTS AND PREVENTS CYBERTHREATS & TESTS AND IMPROVES CYBER RESILIENCE

nc3.lu
National Cybersecurity Competence Center
LUXEMBOURG

The purpose of the Luxembourg National Cybersecurity Competence Center (NC3) is to strengthen the Country's ecosystem facing cyber threats and risks, by building cybersecurity competence and capacity, in a way that contributes to develop the cybersecurity industrial base in the country, and strengthens the strategic autonomy of the European Union.

DETECTS AND RESPONDS TO CYBER INCIDENTS

circl.lu
Computer Incident Response Center
LUXEMBOURG

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.
CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg.

CYBERSECURITY LUXEMBOURG
cybersecurity.lu

The trusted ecosystem offering extensive cybersecurity expertise

330+ PROFESSIONALS

- **319** private companies
- **37** public entities
- **9** associations

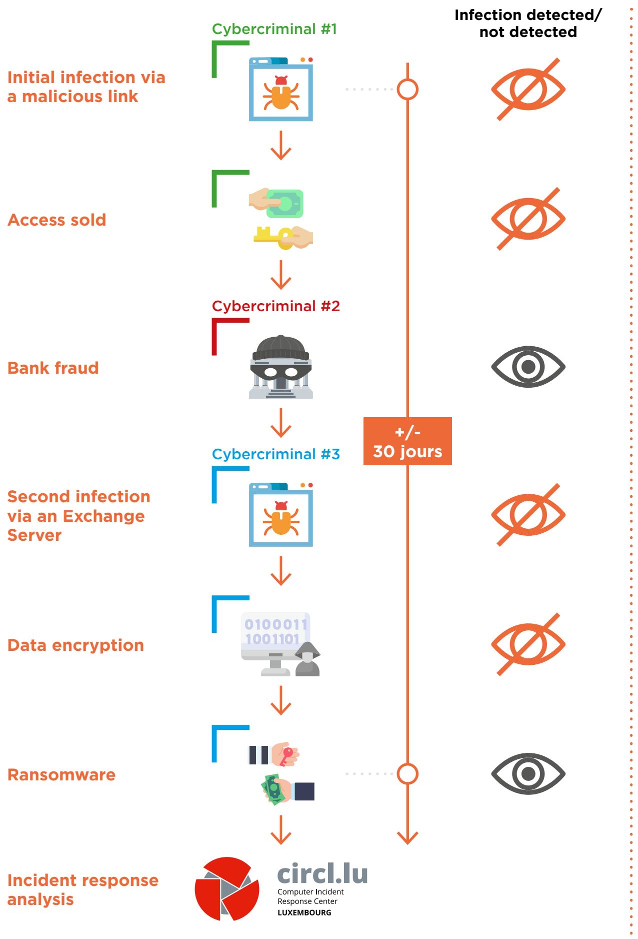
25% STARTUPS

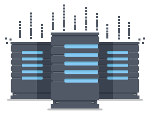
30% FOR WHICH CYBERSECURITY IS THE CORE BUSINESS

An overview of an infection scenario

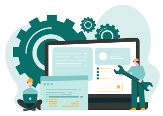
Take a look at the following example of vulnerabilities identified on certain Microsoft Exchange Servers in February-March 2021. A situation that affected a number of Luxembourg companies. As soon as the vulnerabilities were made public, the CIRCL notified the organisations for which it had identified a vulnerable Exchange Server[1], and which could lead to the theft or destruction of data or the compromise of infrastructures.
This is why it is recommended that companies provide the CIRCL with a point of contact, their domain name and IP address so that the CIRCL can notify them during its proactive vulnerability scanning.

Using this example, find out what happens before, during, and after an infection. The exploitation of a vulnerability by a first offender, if left undetected for some time, allows other potential attackers to exploit it.


Cybercriminal #1
Infection detected/ not detected
Initial infection via a malicious link
Access sold
Cybercriminal #2
Bank fraud
+/- 30 jours
Cybercriminal #3
Second infection via an Exchange Server
0100011 1001101
Data encryption
Ransomware
Incident response analysis
circl.lu
Computer Incident Response Center
LUXEMBOURG



270 Microsoft exchange servers identified as vulnerable in Luxembourg and **30 of them infected in one week** in March 2021.



Operational best practices
Make and maintain an inventory of all equipment exposed to the Internet and perform maintenance or ensure that it is done in a timely manner if outsourced. Vulnerabilities regularly appear in ICT products.

Preparing for such a situation
Having as many elements prepared in advance as possible, such as a crisis scenario and communication materials like a press release (to be adapted depending on the situation), helps to prevent reacting in a state of panic.

[1] This does not mean that the vulnerability was exploited and the server infected.

Self-assessment

In my company...

1. Employees receive training in security and information protection
❒ Yes, they had one some time ago
❒ Yes, they regularly receive it
❒ No, never

2. Everyone knows who to contact if they have questions or problems related to information security
❒ Yes, it is part of a communicated and visible procedure
❒ Yes, I think so
❒ No, I don't think so

3. To connect to the company remotely, employees have rules (choice of WIFI connection...) and protected access (VPN - Virtual Private Network)
❒ Yes
❒ No

4. Passwords must have a specific structure (12 or more characters, at least one upper case, one lower case, one number, one special character) and are changed regularly
❒ Yes
❒ No

5. Computers are subject to administrative rights or restrictions, which prevent users from installing software from an unverified or unlicenced source
❒ Yes
❒ No

❒ **6. Backups of all important data are carried out and regularly verified by recovery tests**
❒ Yes
❒ No

7. The use of personal computer equipment should be avoided within the company
❒ Yes
❒ No

Did you answer 'no' to at least one question or do you want to test your information security maturity? We recommend that you take the CASES Fit4Cybersecurity assessment (**fit4cybersecurity.cases.lu**) to obtain a score and recommendations that will help you increase your company's cybersecurity maturity

Tools and solutions
(non-exhaustive list)

A range of tools is available to companies to help them be better prepared to counter an attack: self-diagnosis to assess their situation and receive recommendations according to their needs, applications, services, videos, training, etc.
See also the lhc.lu website and the cybersecurity.lu platform which lists all the cybersecurity players in Luxembourg.

No software solution is indicated here because the choice is vast. Software could give a company the false impression that it is protected, when in fact protection consists of multiple parameters.

Either you need help, seek guidance or wish to discuss a cybersecurity related topic/project, relevant experts are there for you. With a series of committed partners, the Luxembourg House of Cybersecurity is there to guide you towards the right expert, through a Cyber Desk service. Further information: https://lhc.lu/service/cyber-desk

Communication and awareness raising

NC3 **Trustbox (https://nc3.lu/pages/trustbox.html):** Tools and materials to raise awareness and improve the knowledge and reflexes of company employees. 🇬🇧 🇫🇷

Simulation of a real-life situation

ROOM#42 by NC3 **(https://room42.lu/):**
A reconstructed office to simulate an attack situation, understand employee reactions, and teach them how to respond. 🇬🇧 🇫🇷

Training

Training courses for all levels (from beginners to IT managers), from awareness raising to technical analysis of what happens during a cyberattack, in all languages, from a few hours to several days.

See:
- **www.cybersecurity.lu/education**
- **lifelonglearning.lu**
- **www.houseoftraining.lu**
- **www.keyjob.lu**
- **www.circl.lu/services/training/**

Self-assessment tools (free, anonymous and online)

Fit4Cybersecurity *by NC3* ***(https://fit4cybersecurity.nc3.lu/):*** A service for assessing a company's cybersecurity maturity and receiving recommendations based on the results. 🇬🇧 🇩🇪 🇫🇷
(see Self-assessment p. 19)

Fit4Contract by NC3 **(https://fit4contract.nc3.lu/):** A self-assessment tool designed to help clients review their contracts with their suppliers. In the event of an incident, a good contract can make a difference, if the responsibilities of each stakeholder are clearly defined. Fit4Contract helps to negotiate a contract that will better protect the company in the event of an information security problem. 🇬🇧 🇩🇪 🇫🇷

Fit4Privacy by NC3 **(https://fit4privacy.nc3.lu/):**
An anonymous online self-assessment
tool giving concrete recommendations on key data protection steps.🇬🇧 🇩🇪 🇫🇷

Services

Threat Observatory Platform by NC3 **(https://nc3.lu/pages/observatory.html):** aims to support its users with evidence-based information on cybersecurity emerging threats, in order to facilitate their decision-making processes regarding the prevention strategies to be undertaken. 🇬🇧

MONARC by NC3 **(https://nc3.lu/pages/monarc.html):** tool and method allowing an optimised, precise and repeatable risk assessment. 🇬🇧

MISP by CIRCL **(www.circl.lu/misp):** a platform for sharing information concerning threats, which also supports the application of countermeasures and improves the prevention and detection of malware. 🇬🇧

URL Abuse by CIRCL **(www.securitymadein.lu/services/urlabuse):** a service for submitting suspicious URLs for analysis. 🇬🇧

Lookyloo by CIRCL **(https://lookyloo.circl.lu/):** a web interface that allows users to grab and submit a website page. 🇬🇧

Pandora by CIRCL **(https://pandora.circl.lu/submit):** free online service to review files or documents received by a third party. 🇬🇧

Typosquatting Finder by CIRCL **(https://typosquatting-finder.circl.lu/):** free and public service to quickly find typosquatted domains in order to assess if an adversary uses any existing fake domains. 🇬🇧

Testing Platform by NC3 **(https://nc3.lu/pages/testing-platform.html):** holds the tools and services that will help organisations to perform basic tests on their most commonly exposed infrastructures, starting with email and web servers.
The Testing Platform has a whole range of tools devoted to pentesting. Contracted hackers penetrate IT systems in order to identify breaches that could be used by cybercriminals, and to offer recommendations on how to reduce these. Several companies offer this service.
See **https://www.cybersecurity.lu/privatesector?taxonomy_values=85**

Pentesting to identify flaws in a system

Interview with Jean-Marie Bourbon, POST's Offensive Security Services. Among the 50 cybersecurity experts in its CyberForce department, POST has 9 'pentesters', who put their hacking skills to use for their clients to simulate an attack, identify weaknesses, and make recommendations for improved protection.

Why run intrusion tests if there is software for protection?

Before being able to fix a vulnerability, it must be identified. Taking on the role of a cybercriminal by simulating the techniques used during a cyberattack to test a company's vulnerabilities is the best way to protect it. Unfortunately, having antivirus software, the latest equipment, or training employees is not enough to prevent an intrusion. Conventional methods have reached their limits, as the news constantly demonstrates.

The pentester examines the options for penetrating an organisation's computer system: is remote access available? Is it only protected by a password? What are the obstacles and how can they be circumvented? It is even possible to attempt to physically enter a building to get into the server room or the manager's office to plug in a box or remove documents, etc. It is much easier than you might think, you just have to be brazen.

For a small company, 3 to 4 days of technical consulting can be enough to make an assessment of the most accessible vulnerabilities, to identify the risks, and to obtain recommendations to limit the scope of attack available to criminals.

The recommendations do not involve purchasing expensive solutions, far from it. Changing a configuration, making an upgrade, and various relatively simple actions are enough in most cases.

Free, open-source software also exists, you just need to know what is required. And then you must train your IT staff to have the appropriate response to an attack, to prevent them from facilitating intrusions in the system by taking the wrong measures.

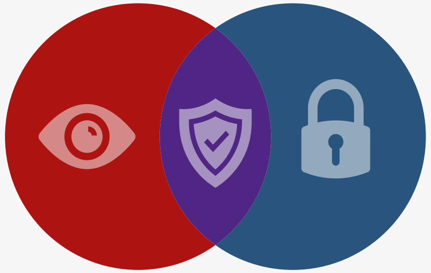
In order to train the client's IT staff, we offer exercises called 'Adversary Simulation' which simulate a real threat, as well as objectively and factually evaluating a company's exposure to attacks.

Why would cybercriminals attack a small company?

An SME may be a service provider to a large corporation or a government agency, for example. Cybercriminals will go through it, as it is often less protected, to reach their ultimate target. This is known as the 'supply chain attack'.

A CLASSIC EXERCISE
FOR AN ATTACK SIMULATION.

The reds are the attackers, the blues are the IT team who counter the attacks. The purple team is a mixed team, which helps to understand the tactics of the reds.



Red Team (offensive)

Simulates a threat using a realistic approach to evaluate the reactions of people and the effectiveness of the procedures and technology used to defend the company.

Purple Team (common goal)

Works to understand the techniques, tactics, and procedures employed by the attackers to improve its position.

Blue Team (defensive)

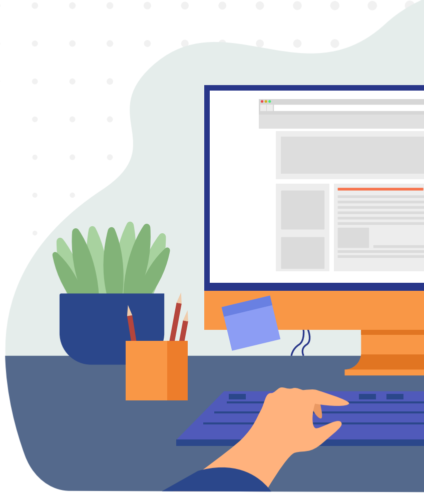
Responds to the attack, contains, and identifies the threat, monitors.

What advice would you give to a small business?

Don't rely entirely on one solution that might give the false impression of being protected. Existing solutions only protect against known attacks, but new ones are appearing every day, which offer no means of defence and for which there is no fix. We must be wary of peripheral protection alone and put up as many obstacles as possible to limit the range of attacks. Just because you can't see something doesn't mean it isn't happening. The worm can be in the fruit already and waiting to show itself.

Investing in security is like taking out insurance: it has a price and does not pay off directly. But it does limit the impact of an attack, which could lead to the disruption of business, exposure to sanctions, and, in some cases, as we have seen already unfortunately, the outright end of a company's activities.

Who can help me?



For protection, prevention, and assessment of cyber risks:
info@nc3.lu

For testing and improving cyber resilience:
info@nc3.lu

For reporting or responding to a cyber incident:
www.circl.lu/report

For reporting a security incident there are three options:

- **Fill in an anonymous online form:**
  www.circl.lu/contactform
- **Send an email, preferably PGP/GPG encrypted:**
  info@circl.lu
- **Call:**
  (+352) 247 88444

To contact the Luxembourg House of Cybersecurity and be directed to the department that best suits your needs:
info@lhc.lu

To obtain a list of tools made available by CIRCL and NC3:
https://circl.lu/services/
https://nc3.lu/

To learn more about ransomware, the most common attack on SMEs:
https://circl.lu/pub/tr-57/

For an exhaustive list of all the professionals involved in cybersecurity:
https://cybersecurity.lu