SECURITY MADEIN.LU

Cybersecurity Agency for the Luxembourg Economy and Municipalities

THE STATE OF CYBERSECURITY IN LUXEMBOURG 2020

EXECUTIVE SUMMARY

Throughout the last ten years, **SECURITYMADEIN.LU, the Cybersecurity Agency for the Luxembourg Economy and Municipalities**, has continuously and consistently addressed relevant cybersecurity challenges and current issues. The Agency did this with a clear focus on delivering services, tools and training that contribute to enhance the cyber posture of businesses and organisations in Luxembourg.

The aim of this report is to provide an overview and the state of cybersecurity of Luxembourg in 2020. Current threats and trends, the defensive posture of the Luxembourg economy and opportunities for development for the years to come are to be discovered in the following pages. Findings, facts and figures presented in this report are based on key activities carried out in the frame of the three main areas of expertise of SECURITYMADEIN.LU:

CASES - Cyberworld Awareness and Security Enhancement Services;
CIRCL - Computer Incident Response Center Luxembourg; and
C3 - Cybersecurity Competence Center Luxembourg.

SECURITY MADEIN.LU
Cybersecurity Agency for the Luxembourg Economy and Municipalities
circl.lu cases.lu c3.lu

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Famille, de l'Intégration et à la Grande Région

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

bigi Syndicat Intercommunal de Gestion Informatique

SYVICOL Syndicat des Villes et Communes Luxembourgeoises

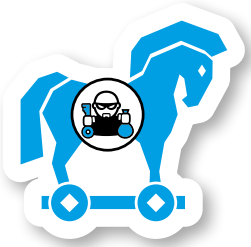
KEY FINDINGS FROM 2020

AND RECOMMENDATIONS FOR 2021

Awareness is vital, yet there are many opportunities for enhancement in its execution as well as its outreach. Password security is the all-time high, key concern. Users continue to rely on too weak, too simple to guess or too similar passwords for business-critical systems. The **CASES Trustbox** especially addressing SMEs, continues to be the ideal toolset to raise cybersecurity awareness and empower all users with better cyber hygiene (e.g., using a password manager).

Compliance is well understood; still, personal data is not protected enough. Missing measures and the lack of "end-to-end" protection mechanisms keep privacy one of the top concerns. A dedicated service, **Fit4Privacy**, addressing this issue, is planned to be released in 2021.

To support with imprecise contracts where missing clauses for information security and privacy protection create issues when dealing with service providers to implement adapted protective and preventive solutions, in 2020, CASES implemented **Fit4Contract**.



Ransomware attacks were on the rise again, less in numbers, but clearly, success rates and damage generated. For different organisations, the impact was significant, resulting in weeks or months of activity and productivity losses. Threat-actors improved their techniques, especially in phishing and social engineering, making the attacks more complex and the mitigation efforts more resource intensive.

With the rise of IoT and the digital transformation reaching all sectors and entities with all types of security maturity levels, initial infection vectors of many cybersecurity attacks (such as ransomware) came from unmaintained pieces of equipment and software. A significant number of incidents could have been avoided (or the impact could have been limited) by adequate vulnerability management, ICT infrastructure patching and network segregation. CASES and ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), in partnership with SIGI (Syndicat Intercommunal de Gestion Informatique), POST Luxembourg and the Representation of the European Commission in Luxembourg, have launched a dedicated online platform **secure-iot.lu**, supported by a national awareness campaign in order to encourage good habits among professionals and individuals.

Fortunately, a more and more extensive and timely sharing of information via platforms like **MISP** or other sharing communities played an important role in limiting the "time-to-exploit" for threat-actors.

Key competence and capacity in the incident and crisis management is lacking within many organisations, as show the lessons learned from 3 years of experience with **C3's ROOM#42**.

Last but not least, the pandemic created a whole new situation in all areas of life: the COVID-19 and the containment measures that followed made cyberattacks very active. Phishing was prevalent throughout the year, while forced digitization and telecommuting created an ideal ground for DDoS attacks. Another phenomenon was the rise of ransomware, during which vulnerabilities in the health care system have emerged.

The above findings and the need for improvement are further confirmed by extensive interaction and regular exchange between SECURITYMADEIN.LU and cybersecurity professionals through platforms like the monthly **Cybersecurity Breakfast** or the **Cybersecurity Week Luxembourg** in October each year.

CYBERSECURITY
LUXEMBOURG

SITUATIONAL AWARENESS ON CYBER RISKS

PROTECTING AND PREVENTING

SECURITYMADEIN.LU's **MONARC** platform (https://my.monarc.lu), developed, maintained and promoted by the CASES department, is "home" for more than 200 organisations, with 46 new joining entities in 2020.

Besides MONARC, CASES has developed several other solutions to raise cyber awareness and improve the understanding and treatment of cyber risks and provide relevant statistics and situational awareness of Luxembourg's cyber posture.

Among these solutions **Fit4Cybersecurity** tool has been running since 2019 and has attracted responders from both Luxembourg and abroad.

Locations and Languages: Most of the respondents were from Luxembourg (over 400 respondents), a bit over 200 were from France, then Belgium, Germany, and Canada were also the typical locations for respondents. In terms of language, 71.9% was French, English questionnaires were 15.6%, while 12.5% were German.

Sectors: The most represented sectors among the total of the respondents were construction and civil engineering (14.1%), banking, insurance and real estate (13.5%), trading, sales and mass distribution (13.3%), company support (11%) and public administration (9.1%).

Company Sizes: since its launch, Fit4Cybersecurity has been used by:

- 320 respondents of type 1 (under 5 employees)
- 163 respondents of type 2 (between 5 and 20 employees)
- 117 respondents of type 3 (between 20 and 50 employees)
- 221 respondents of type 4 (over 50 employees).

Categories: The thirteen main questions of Fit4Cybersecurity relate to various cybersecurity topics that can be aggregated into six categories (Figure 1).

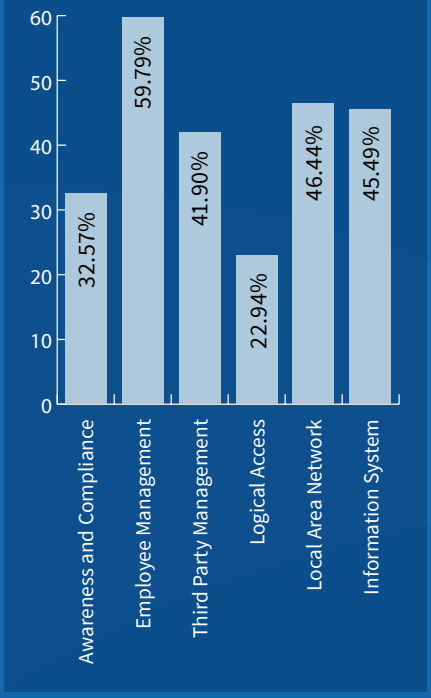
The top 3 domains where success rates were the highest, were:

- Employee Management (**best score**)
- Local Area Network (**second best**)
- Information System (**third best**)

The three lowest and most worrying areas are:

- Logical Access (**the worst**)
- Awareness and Compliance (**second worst**)
- Third Party Management (**third worst**)

Figure 1:
Success percentage by theme for categories



The worst scores were received for questions related to Passwords, Rules/Charter, GDPR, and Backups.

23% WORST SCORE LOGICAL ACCESS

cases Fit4Cybersecurity
The essential for a good start in information security

HOW RESPONDENTS IN LUXEMBOURG SCORED IN THE FIT4CYBERSECURITY QUESTIONNAIRES COMPARED TO RESPONDENTS FROM OTHER COUNTRIES?

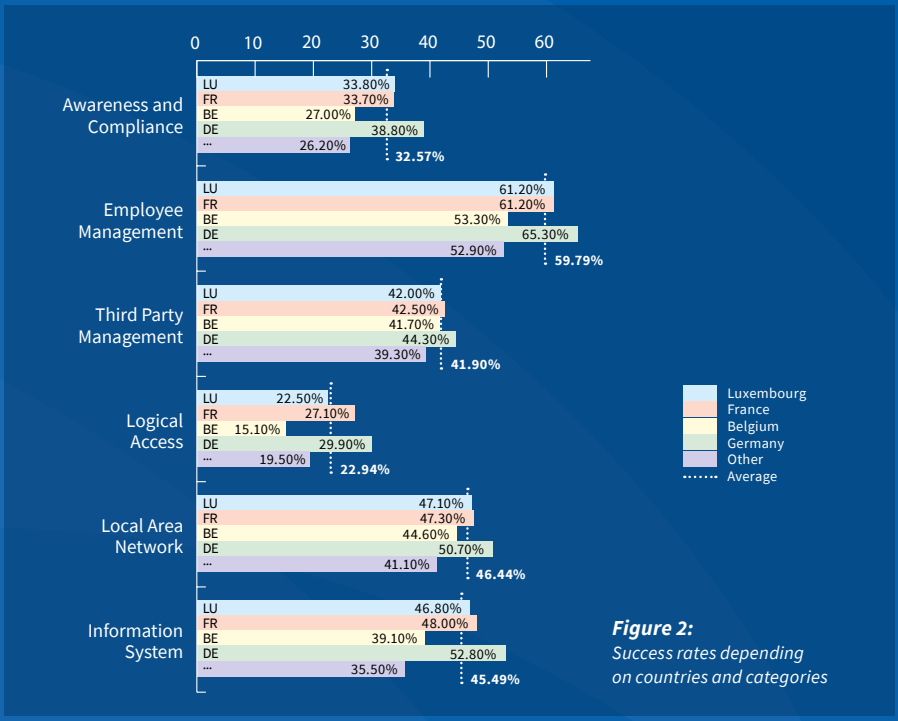


Figure 2:
Success rates depending on countries and categories

Based on Figure 2, the following conclusions can be drawn:

- Germany scored best when it came to all categories in our questionnaire.
- France and Luxembourg came second most of the times, very closely one from the other. French respondents scored better than Luxembourg when it came to Logical Access.
- Overall, Luxembourg was close to the average score for all six categories analysed in our questionnaire. The only area where Luxembourg scored below the average compared to the other countries was Logical Access.

Drilling deeper into the specific questions linked to the categories mentioned, we also observed that:

- Luxembourg scored below average when it came to BYOD questions, Passwords, and Office Cleaning.
- Luxembourg scored higher than average on the questions related to the Rules/Charter, Trainings, Home-office/Mobility, and Backups.

HOW WELL DID LUXEMBOURG RESPONDENTS SCORE ACCORDING TO THEIR SIZE OF BUSINESS?

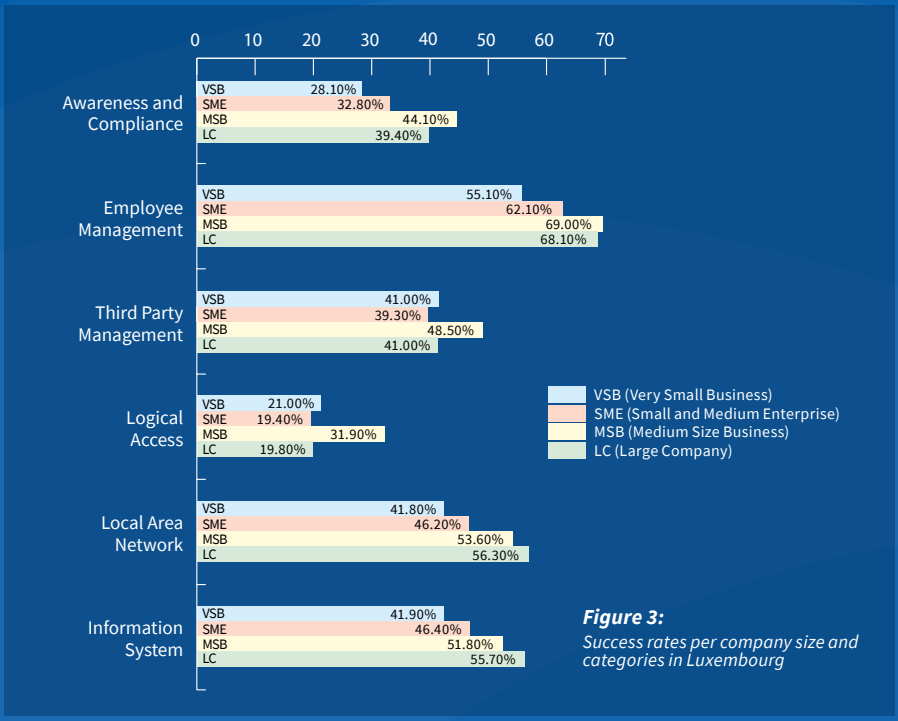


Figure 3:
Success rates per company size and categories in Luxembourg

69% SUCCESS
CATEGORY EMPLOYEE MANAGEMENT
MEDIUM SIZE BUSINESS

Figure 3 looks at the break-out on different categories of questions and the type of Luxembourg companies that replied to the question. We can conclude the following:

- The very small and the large companies scored better than the others on categories such as Awareness and Compliance, Employee Management, Third Party Management, Local Area Network and Information System.
- The medium enterprises scored worse when it came to Logical Access and Third Party Management.
- Businesses under five employees (very small) scored worse than all others, except for the Logical Access category.
- Large companies did not consistently score the best: for example, they scored less than very small companies in terms of Logical Access and were on par with them in Third Party Management.

circl
Computer Incident
Response Center
LUXEMBOURG

SITUATIONAL AWARENESS ON THREATS, ATTACKS AND INCIDENTS

DETECTING AND REACTING TO ATTACKS

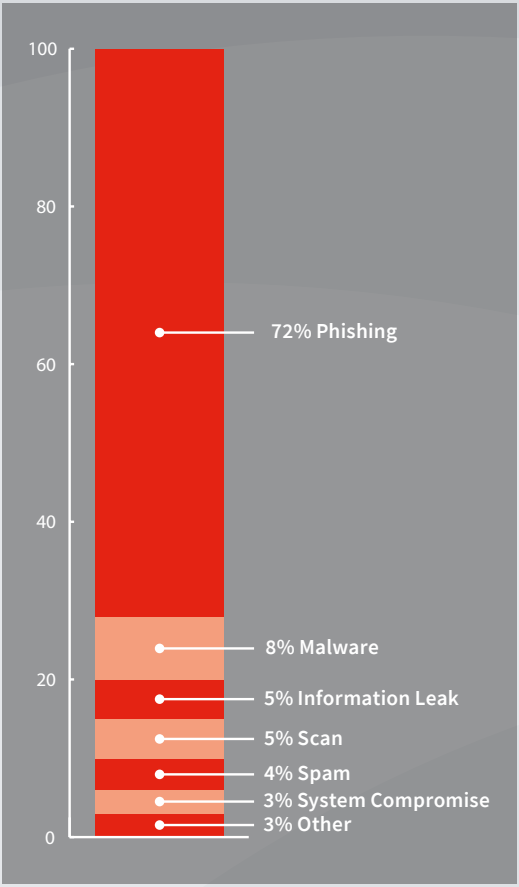
The operational statistics (https://www.circl.lu/opendata/statistics/) cover the activities related to the incident response activities of CIRCL, especially in regards to the reporting and notifications (take-down notifications, notifications about vulnerabilities) from/to third parties.

A significant number of cases (72%) handled by CIRCL in 2020 were related to all forms of **phishing**, reported manually or automatically by companies, organisations or citizens in Luxembourg.

The volume of phishing significantly increased due to various factors, including better awareness, automatic tools for reporting and the increase of remote work in 2020.

72% | OF THE CASES WERE RELATED TO PHISHING

TICKET CATEGORIES HANDLED BY CIRCL IN 2020



Fighting against phishing is a continuous challenge. CIRCL introduces an automated model for phishing notification via their in-house developed tools **URL Abuse** and **LookyLoo**, to reduce valuable time to react. Reducing the time of accessibility can help to reduce the number of victims falling into the trap. Nevertheless, hosting and cloud providers play a crucial role in handling take-down requests from CERTs such as CIRCL.

Technical investigations in ransomware cases showed an increase of threat actors in this specific field. Many of the **ransomware** cases in Luxembourg included a mixed model approach focusing on encrypting the information of the victim and leaking and/or ex-filtrating sensitive information.

Another significant part of the incidents reported (8%) and handled by CIRCL was malicious software activities. This includes **financial malware** targeting retail banking but also malware used in ransomware cases.

A profound observation was carried out in 2020 on compromised systems and on the open services connected to the Internet without filtering and additional authentication methods. This led to some compromised systems in Luxembourg, which were used to conduct full infrastructure compromise, often leading to ransomware attacks.

CIRCL produced and shared **threat intelligence** reports (278 MISP events) with their own operated information sharing community at the European and International level. Complementary reports were included in the dedicated MISP instance for COVID-19 related information, such as malicious mobile applications abusing the pandemic situation.

DETECTED VULNERABILITIES

CIRCL published a technical report (https://www.circl.lu/pub/tr-58/) in March 2020 about a **critical vulnerability** in Microsoft SMBv3, including the mitigation details. This vulnerability affected not only client systems but also servers. Adversaries can execute arbitrary code with elevated privileges, allowing an attacker to take full control over the attacked system. Notifications related to known vulnerable systems in Luxembourg were also sent to their respective abuse contact.

In 2020, CIRCL sent a significant number of notifications to various ISP and hosting providers, having accessible and vulnerable devices such as **VPN** or remote access types of equipment. The attack surface of VPN devices increased due to the recent needs for remote services. We strongly recommend organisations to include edge devices into their asset inventory and even share the details with CIRCL if they want to be proactively notified in case of vulnerability.

During the lock-down phases, a significant number of outdated and unpatched systems were connected to the Internet. For example, the Pulse Secure VPN (CVE-2019-11510) was still actively exposed worldwide, and major users of Pulse VPN did not patch their devices.

Threat actors, such as the REvil (Sodinokibi) ransomware group, were actively abusing the vulnerability to further compromise infrastructures. Moreover, Citrix Application Delivery Controller (ADC) vulnerability (CVE-2019-19781) was also abused and compromised for similar objectives.

CASE STUDY: RANSOMWARE IN LUXEMBOURG

The most severe incidents (with a significant impact on business continuity) in Luxembourg for 2020 were ransomware cases. The attackers industrialised their activity and can reproduce their techniques on different targets in a small amount of time. Ransomware attacks are global, and Luxembourg is not an exception. All sectors in Luxembourg were targeted. The most resilient organisations are the ones prepared with actual **off-line backups**.

Many organisations targeted by ransomware lacked off-line backups and were seriously impacted in their day-to-day operation and business activities.

Another critical factor in the case of ransomware is the availability of an efficient **incident response procedure** within the organisation. Controlling public communication, in the case of an incident and especially ransomware attacks, is a crucial success factor to limit the influence of the attacker communication (e.g., when the attacker threatens the victim to release the leaks).

As mentioned earlier, the origins of ransomware cases are often unprotected VPNs or devices in the organisation's external perimeters. Adequate monitoring of devices, including a patch management strategy, is critical to limit many opportunistic attacks such as ransomware.

Threat actors actively move their business model towards a mixed-model, where encryption of information and leaks are performed together.

An extra step to gain some time during a ransomware attack is to know the potential selling or announcement of leaked materials from the victim. CIRCL provides a **leak monitoring service**, based on its own open-source tool called **AIL framework** (ref: https://github.com/ail-project), to monitor the activities of ransomware threat actors.

Some cases in Luxembourg were discovered by active monitoring, and the victims took complementary actions to be better prepared in case of leaks.

c3
Cybersecurity
Competence Center
LUXEMBOURG

SITUATIONAL AWARENESS ON CYBER RESILIENCE

TESTING AND IMPROVING

The **ROOM#42** simulator is one of C3's key training infrastructures and a unique concept in Europe. Its specific immersion training approach brings up to 8 trainees in a one-hour realistic **cyberattack simulation**, offering deep and comprehensive learning based on an intense experience. It is an innovative and unique concept in Europe, through which "participants" are in a cyberattack and have to react to it.
Human dimension is the cornerstone of a cybersecurity system.

Teaching through experience in order to develop competence:

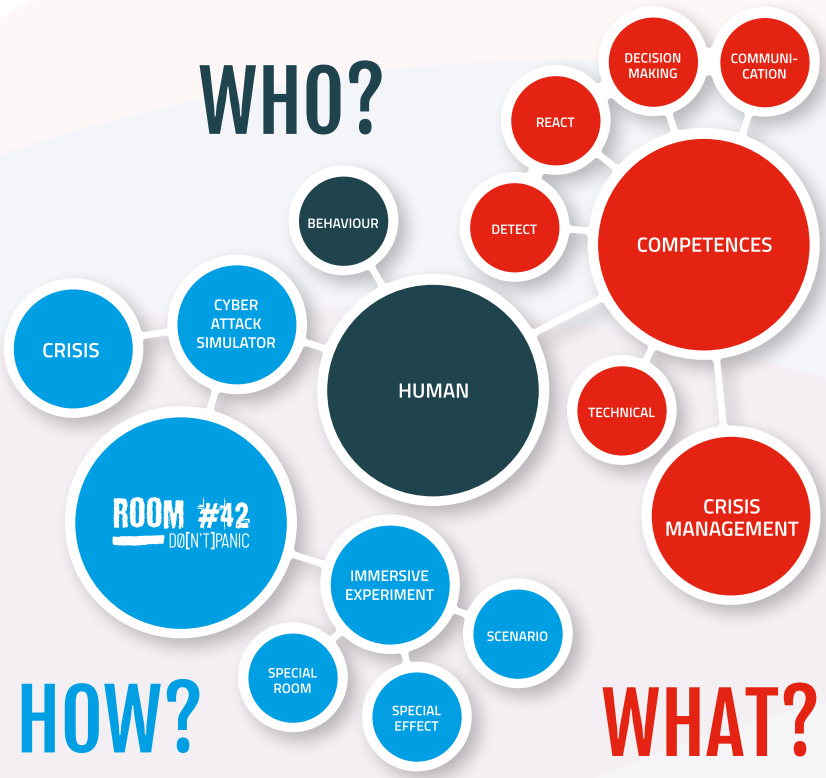
- Train by doing (Experience-based)
- Develop reflex action
- Grow individual and collective competence in cybersecurity crisis management

A success story:

- 2 years of existence and operation
- Close to 100 exercises performed
- Sectors concerned: public sector, media, insurance, banks, public health, start-ups, real estate, air control, etc.
- Various partners:

  - from the public sector:
  Institut National d'Administration Publique (INAP), House of training programs (Agence de Transfert de Technologie Financière - ATTF, Digital humanities, E-commerce, Fit4DigitalFutur), Agence pour le Développement de l'Emploi (ADEM), SCRIPT (Education Nationale)

  - from the private sector:
  European Business Reliance Centre (EBRC), Great-X (France)



The figures show the human behavioural aspects highlighted by the simulation. These results show how difficult it is to manage a crisis and how unprepared are many crisis teams. The ROOM#42 demonstrates the need to consider people and competences as keys element of cybersecurity.

100 | CLOSE TO 100 EXERCISES IN 2 YEARS

KEY FINDINGS

Attack / Incident	Results
Ransomware	**85%** of participants need more than 15 minutes to react **60%** of countermeasures are insufficient
Fake news	**65%** of participants do not clearly reject the press release
Defacing	**35%** of participants don't know what to do
Social engineering	**10 %** of participants give a password by phone to a stranger
Cybercriminals	**40%** of the participants pay the ransom
Crisis	**45%** have never activated the crisis team
CERT	**70%** of participants do not seek help from a CERT
Communication	**80%** of participants forget to communicate internally
Forensics	**95%** don't think about collecting logs and evidence

CONCLUSIONS

Based on the data and reports, the following comprehensive statements can be made regarding the cybersecurity situation in Luxembourg for the year 2020:

1. New types of phishing attacks emerged

New types of phishing emerged to bypass “3D Secure” security features when paying by credit card.

2. Increased DDoS attacks

Covid restrictions urged companies and their employees to undergo almost forced digital transformation to allow their business to continue. As a result, the use of networks for teleworking increased significantly. Criminals reacted with an increase in DDoS attacks.

3. The health sector became particularly sensitive

The ransomware threat was on the rise. The presence of cases in Luxembourg showed that the threat targeted companies without differentiating a particular sector; any organisation was a potential target though hospitals have become particularly sensitive.

4. Malicious Codes proved to be resistant to COVID-19

In 2020, there was an upsurge of a malicious code of the Trojan horse called Emotet in Luxembourg. Emotet is the most sophisticated virus ever designed, which infected millions of computers worldwide and opened the door to ransomware attacks.

5. Abusive content - Spam

The number of spam remained relatively high throughout 2020. The COVID-19 crisis “inspired” attackers to offer Chinese face masks or other types of virus protecting accessories.

In addition to e-mail spam, there was a significant increase in SMS spam campaigns, forcing recipients to register on online gaming sites or contact the e-mail address provided in the SMS.

SECURITYMADEIN.LU
circl.lu cases.lu c3.lu

Cybersecurity Agency for the Luxembourg Economy and Municipalities

CYBERSECURITY LUXEMBOURG

SECURITYMADEIN.LU - 05.2021