Co-funded by
the European Union

EYESonCS

EyesOnCS
Compendium of Cyber Security Needs

English
October 2023

Projektdaten

Acronym: EyesOnCS
Title: **Enhancing Cyber Security – Development of trainings using "Escape Room" Model**
Project No.: 2021-1-DE02-KA220-VET-000033003
Duration: 01. January 2022 – 31. December 2023 (24 months)
Programme: Erasmus +, Key Action 2: Cooperation partnerships in vocational education and training

Projekt Lead: Fachhochschule des Mittelstands (FHM)

Issue: October 2023

Participating project partner organisations

Staatlich anerkannte, private
Fachhochschule des
Mittelstands (FHM)

virtualcampus

AKADEMIE ASW

fb
finance & banking
Associazione
per lo sviluppo organizzativo
e delle risorse umane

Stay tuned!

Follow us

Find out more about
the project here:

www.eyesoncs.eu

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of Content

Figures

1 Introduction to the Topic

Not a day without cybercrime. The cybercrime situation around the world has increased significantly in recent years. One of the reasons is the ongoing digitization in nearly all spheres of work and life. Whereas in the past, crimes and attacks were characterised by a bank robbery or other physical attack, they are now characterised by an attacker sitting on a beach with a laptop and gaining illegal access to a bank's distribution system to extort a ransom. The industry association Bitcom counts more than 220 billion Euro in damages per year. For small and medium-sized companies an attack and the tapping of trade secrets can mean economic ruin (Streim, A., Mann, S. (2021)). The Corona pandemic has also enabled new work formats in a short period of time. The corresponding protective measures have not been established or adapted in parallel. This opens ways for attacks on security and vulnerabilities for invaders and offenders. For this reason, it is of immense importance to inform employees about the effects and consequences of a cyber-attack and to raise their awareness accordingly.

This compendium was developed in the context of the Erasmus+ project "EyesOnCS". The project team pursues several goals with the development of this publication:
First, an overview will introduce strategies for cybersecurity (CS) enforcement, especially in SMEs. It then discusses the particular challenges faced by SMEs in implementing cybersecurity. Subsequently, the compendium focuses briefly on the importance of education and training in averting CS attacks. This is followed by a comprehensive collection of cybersecurity cases that have occurred in practice. These cases were collected by the international project team from companies and other institutions and are documented in detail for the purpose of this compendium.

The target groups for this compendium are primarily companies and educational institutions that can use the collected CS cases for training purposes.
After an introduction to the general security topic, the second chapter deals with important national and European CS strategies. In this context, the role of ENISA (European Union Agency for Cybersecurity) is explained and highlighted. In this regard, the ENISA Consolidated Annual Activity Report says: “In 2021, ENISA was confronted with the challenges brought about by the pandemic, which affected capacity-building activities at multiple levels. On the one hand, several courses and exercises had to be converted for online delivery, for obvious reasons. This change posed a few challenges since the conversion[1]”.
In addition, the compendium focuses in this chapter on the EU Cybersecurity Act which introduces an EU-wide cybersecurity certification framework for information and communication technology (ICT) products, services, and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes, and services only

[1] ENISA: Consolidated Annual Activity Report 2021, Attiki, 2022

once and see their certificates recognized across the European Union.[2]
Furthermore, in this second chapter, the compendium attempts to record and present various national security strategies. For practical reasons, the list is not exhaustive. The following, among others, are explained:

- the German association "Deutschland sicher im Netz e.V. (DsiN)[3]"
- the CERT-Bund[4], a Computer Emergency Response Team for federal authorities
- the Italian National Cybersecurity Strategy for 2022/26
- the Portuguese National Cyber Security Centre (CNCS).

The third chapter summarizes challenges for SMEs regarding cybersecurity. For this purpose, the authors are employing the ENISA three-fold approach including recommendations for SMEs.[5] In this regard the compendium covers the following areas:

- Area People
- Area Processes
- Area Technical.

This project aims at implementing particular SME recommendations on an educational level. The ENISA SME-recommendations6 focus on three different areas. This compendium lists a set of guiding questions for CS-checkups and also for the judgement of collected practical CS-cases (see chapter 5).

Besides, the project aims at developing special virtual CS training methods and implementing them based on so-called scenarios. Therefore, relevant concepts for CS training are described and evaluated in chapter 4 of the compendium. These include Game -Based Learning and Educational Escape Rooms (EERs).

A particularly important and extensive part of the compendium consists of the summary description and evaluation of practical CS cases that the project partners have researched, compiled, and evaluated in their respective home countries of Italy, Germany and Portugal. Chapter 5 describes 26 of such practical cases in a uniformly structured and comparative form.

[2] EUR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 320 19R0881 - EN - EUR-Lex.

[3] Deutschland sicher im Netz, https://www.sicher-im-netz.de.

[4] Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html.

[5] ibid.

2 National and European Strategies

At the European level, cybercrime prevention and cybersecurity strategies are still under development. There are already some good approaches but also still many challenging tasks. Currently, there are only a few government agencies that address this issue, which is particularly important for SMEs.

One of these agencies is the ENISA (European Union Agency for Cybersecurity)[6]. It has the task of contributing to a high common level of cybersecurity throughout Europe. ENISA actively supports the European Union's policy to increase cyber security and the trustworthiness of information and communication technology products and services through cyber security certification. In addition, the Agency contributes to making the Union's infrastructure more defensible and ultimately to ensuring a secure digital environment for European society and citizens.

The past Corona pandemic has further increased the activity of European citizens in various networks, such as the Internet, both in professional and private environments. Unfortunately, the pandemic has opened further gateways for coordinated and adapted methods of attack. For cyber-criminal attackers, this has been increasingly easy due to the lack of distinct defence structures, know-how and defence mechanisms. ENISA has learned from this and has therefore once again significantly stepped up its crime-fighting activities. In this regard, the ENISA Consolidated Annual Activity Report says: “In 2021, ENISA was confronted with the challenges brought about by the pandemic, which affected capacity-building activities at multiple levels. On the one hand, several courses and exercises had to be converted for online delivery, for obvious reasons. This change posed a few challenges since the conversion”.[7]

In 2019 the EU Agency for cybersecurity became stronger through the EU Cybersecurity Act.[8] It grants a permanent mandate to the agency and gives it more resources and new tasks. Now, ENISA will have a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes. It oversees informing the public about the certification schemes and the issued certificates through a dedicated website. Furthermore, ENISA is mandated to increase operational cooperation at the EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross-border cyberattacks and crises.

[6] https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity

[7] ENISA: Consolidated Annual Activity Report 2021, Attiki, 2022

[8] EUR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 320 19R0881 - EN - EUR-Lex.

In addition, The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for information and communication technology (ICT) products, services, and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes, and services only once and see their certificates recognized across the European Union. The EU cybersecurity certification framework for ICT products enables the creation of tailored and risk-based EU certification schemes. It provides EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards, and procedures. The framework will be based on agreement at the EU level on the evaluation of the security properties of a specific ICT-based product or service. It will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements.[9]

At the national level in **Germany**, the association "Deutschland sicher im Netz e.V. (DsiN)"[10] supports consumers and small businesses in dealing safely and confidently with the digital world, as well as offering learning opportunities for people in private and professional environments.

Another very worthwhile and helpful support for SMEs is the CERT-Bund[11], the Computer Emergency Response Team for federal authorities, which is the central point of contact for preventive and reactive measures in the event of security-related incidents in computer systems. In addition to the support for federal authorities, the citizen CERT provides free and neutral information about current attacks by malware as well as about security vulnerabilities in computer applications.

In May 2022, **Italy** announced its National Cybersecurity Strategy for 2022/26, a crucial document to address cyber threats and increase the resilience of the country. The strategy, developed by the Italian National Cybersecurity Agency, includes 82 objectives, and aims to address the following challenges:

- To ensure a cyber resilient digital transition of the Public Administration (PA) and of the productive system.
- To predict the evolution of the cyber threats to reduce their impact on national infrastructure and organisations.
- To prevent online disinformation in a broader context of the hybrid threat.
- To manage cyber crises.
- To strengthen National and European strategic digital sector autonomy.

[9] European Commission: The EU cybersecurity certification framework, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

[10] Deutschland sicher im Netz, https://www.sicher-im-netz.de.

[11] Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html

The Italian cybersecurity strategy combines security and development, in compliance with the values of our Constitutional Charter. It takes into consideration the provisions of the European Union cybersecurity strategy of December 2020, the EU Strategic Compass for Security and Defence of March 2022 and the recent NATO strategic guidelines. To achieve this new vision, Italy conceived a cybersecurity ecosystem based on the collaboration between public and private sectors. In such a system, the active contribution of the Institutions is complemented by that of economic operators – primarily those entrusted with the management of infrastructures on which depend the provision of essential services by the State – the world of universities and research, and civil society as well.[12]

In **Portugal**, the National Cyber Security Centre (CNCS) is the operational coordinator and Portuguese national authority specialised in cybersecurity working with State entities, operators of essential services and digital service providers, ensuring that cyberspace is used as an area of freedom, security and justice, for the protection of all sectors of society.[13] CNCS mission is to contribute to the free, reliable and secure use of cyberspace in Portugal, through the continuous improvement of national cybersecurity and international cooperation, in coordination with all the competent authorities, and the implementation of measures and instruments required for the anticipation, detection, reaction and recovery of situations that may compromise the operation of critical infrastructures and national interests. CERT.PT coordinates the response to incidents involving State entities, operators of Critical infrastructures, operators of essential services, digital service providers, and, in general, national cyberspace in Portugal.

[12] ACN Italy: National Cybersecurity Strategy 2022 – 2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf, seen 29.7.22

[13] Cyber security intelligence: National Cyber Security Centre Portugal (CNCS), https://www.cybersecurityintelligence.com/national-cyber-security-centre-portugal-cncs-2730.html.

3 Challenges of SMEs

Cyber-attacks can put small and medium-sized companies before the end of their business. SMEs are often family-run businesses whose production and trade secrets are based on a long tradition. In practice, this is often in considerable contrast to the prevailing protective measures, which are usually associated with considerable costs for SMEs and/or lack the corresponding know-how. The number of cyber-attacks on SMEs has increased exponentially in the last three years. They are also increasingly becoming the object of targeted economic and industrial espionage. Basic thematic knowledge is familiar to employees in corporate groups with their own corporate security departments. They have a certain level of awareness and receive in-house training at regular intervals. In the event of an attack, responsibilities and procedures are named and rehearsed. All these structures are generally not in place in SMEs. Most employees generally do not know how to handle sensitive data. This not only jeopardises a company's ability to do business, but also, in the worst case, many jobs. After all, SMEs are also part of the supply chain. A successful cyber-attack on an SME company can therefore also have a major impact on the supply chain and have an impact on a government agency or other larger corporations.

According to a recent survey[14] over 80% of European SMEs stated that cybersecurity issues would have serious negative impact on their business within a week of the issues happening, out of 57% saying they would most likely become bankrupt or go out of business. Despite this, SMEs do not seem to appreciate that cybersecurity is not something that impacts only larger organisations. SMEs therefore need to be aware of the impact cybersecurity issues can have on their business. Many SMEs believe that the security controls included in the IT products they purchase are sufficient and that no additional security controls are required unless mandated by regulation or law. This compendium is intended to help provide more clarity in this regard. Therefore, the ENISA proposes a three-fold approach including recommendations for SMEs[15]:

- Area People
- Area Processes
- Area Technical.

This project aims to implement the below SME recommendations on an educational level. They include keeping software up to date, applying strict access control rules, making use of cloud services and more.

The ENISA SME-recommendations[16] focus on four different areas. Within the areas major checkpoints including leading questions are listed. This listing might also be used as a questionnaire for a self-test.

[14] ENISA: Cybersecurity for SMES- Challenges and Recommendations, European Union Agency for Cybersecurity (ENISA), Attiki, 2021
[15] ibid.
[16] ibid.

Guiding Questions for the Area PEOPLE

Responsibility	Does a director, or equivalent, have responsibility for cybersecurity?
Employee Buy-in	Have all members of staff given written acknowledgement that they have read, understood, and accepted the information security policy?
Employee awareness	Do all users of your computer systems receive regular training on their security responsibilities on how to identify and deal with various security threats? Ensure that staff are aware of, and can verify, all contact points and communication channels.
Cybersecurity Training	Do staff members with specific security responsibilities receive proper and regular training to support their role?
Cybersecurity Policies	Have you a documented security policy, with associated operating procedures, signed off and fully supported by senior management?
Third Party Management	Does senior management authorise third party access to confidential and/or commercially sensitive information pending completion of appropriate confidentiality forms?

Guiding Question for the Area PROCESS

Audits	Are critical systems, such as firewalls and routers regularly tested for vulnerabilities? Are computers checked to ensure no copies of illegal software are present?
Incident planning and response	Is there a plan of dealing with security incidents? Are all default passwords on all systems reset from the default vendor installed passwords? Are users forced to use complex and hard to guess passwords?

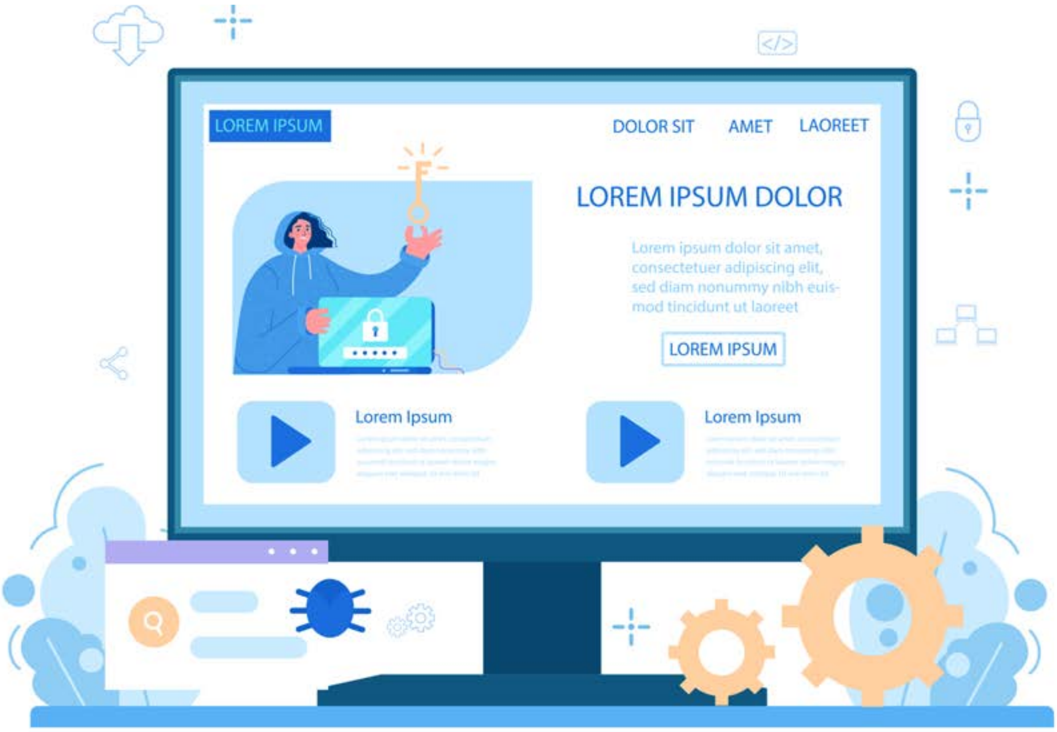
Software patches	Is there a mechanism to ensure that critical security patches are deployed to systems in a timely and audited fashion?
Data Protection	Are systems and databases that store personal data secured properly to ensure compliance with regulatory and legal requirements such as the EU General Data Protection Regulation, the Cyber security act[17] and the Data Protection Act?

Guiding Question for the TECHNICAL AREA

Network security	Are external connections, such as to the Internet, authorised by senior management, properly documented, and secured using Firewalls?
Anti-Virus	Are all computer systems protected with the most up to date anti-virus software? Are users educated on how to identify and deal with suspect emails or files that may contain computer viruses?
Encryption	Do all devices storing data have full disk encryption enforced? Do you use Virtual Private Networks (VPNS) when communicating over the Internet on public networks?
Security monitoring	Are the log files of important security devices actively monitored to detect potential security breaches?
Physical security	Are critical IT resources, such as file servers, secured in a secured area that is protected from unauthorised access? Are home office measures in place ensuring secured areas comparable to the office (closed doors when leaving the workplace, no third-party access to information via windows or else)?
Secure backups	A good backup may save your business from a ransomware attack. Do you regularly backup critical data and systems to secure offline storage? Do you regularly test restoring from your backups to verify you can fully recover your data and systems?

[17] European Commission: The EU cybersecurity certification framework, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework.

4 Role of education and training – Relevant concepts for the Cybersecurity Training


LOREM IPSUM
DOLOR SIT
AMET
LAOREET
LOREM IPSUM DOLOR
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet
LOREM IPSUM
Lorem Ipsum
Lorem Ipsum

The fact that successful cybersecurity depends not only on technical protection but also to a large extent on raising employee awareness and confidence in acting is not always recognized by companies. Although one in four companies continuously identifies the need for action in corporate security and makes more resources available, the focus is clearly on technical protection. In SMEs often training and awareness-raising of employees takes place only to a limited extent. This means that too little attention is paid to the human protection factor, which is becoming even more important with mobile working and in the home office. Raising awareness of the safety risks associated with flexible workplaces are gaining in importance. Obviously, it is important to make companies conscious of the new opportunities for attacks that can arise from mobile work and home offices.

It is therefore advisable to offer training courses that focus on this topic. Furthermore, it is valuable to sensitise companies with written information or lectures by institutions.

4.1 Game -Based Learning

Videogames appeared on the consumer market about 50 years ago and their societal impact steadily grew until they became a fundamental social and cultural element (Oblinger 2006). Games are endogenous systems, with problem-solving activities structured by game mechanics and game rules. The engagement in games and play is internally motivated in the sense that individuals participate in them voluntarily. Gameplays describe the interaction between the player and the game elements that lead to different behaviours and produce different results. To a great extent, games involve the evaluation of choices by the player which promotes his/her immersion, a phenomenon experienced by an individual when he/she is in a state of deep mental involvement (Agrawal et al, 2020). But games also contribute to socialisation and to help players make connections between the cause and effect of their decisions, which can contribute to critical and logical thinking. They also improve various cognitive, intrapersonal, and interpersonal skills like perceptiveness, attention, memory, visual and auditory analysis and synthesis, comparison, classification, and generalisation.

While initially thought as simple entertainment objects, the design and/or use of videogames for other purposes was seen as a logical step to take advantage of the motivation and engagement that users experience while playing. As such, videogames are now used for education and training, awareness raising, advertising, research studies, public health campaigns, etc. These games, called Serious Games, are generically defined as "[games] that do not have entertainment, enjoyment or fun as their primary purpose" (Michael and Chen 2006, p. 21) or as "… a mental contest, played with a computer in accordance with specific rules, that uses entertainment to further government or corporate training, education, health care, social awareness, public policies, crisis management and strategic communication objectives" (Zyda 2005, p. 26). Serious games explore the inherent motivation and immersion of players through the use of adequate game mechanics and dynamics to develop specific skills and competences, to transmit a desired information (or message) to the user or to reinforce the acquired knowledge or awareness while the user is immersed in a fun environment.

Education is the area with more (successful) examples of the utilization of serious games therefore generating the "game-based learning" term, which focuses on the development of games that are designed with specific learning objectives in mind. Users can 'learn by doing' and 'learn by error' in a controlled environment that supports knowledge, skill and competence development and can even improve teamwork, social skills, leadership, and collaboration (Juzeleniene et al. 2014).

Game-Based Learning aims at extracting components that make gaming appealing and combine these with the desired information and knowledge to be transmitted to the user, creating an interactive source for learning that, in turn, motivate each user to extend their own knowledge and deepen their study in a challenging, engaging, and instant approach

(Prensky, 2003). The following advantages have been related to the use of educational games (Abt, 1987):

- Games introduce users to problems and to problem solving. Games may be used for motivating learners to engage in educational processes, encouraging them to create and collaborate.
- Games have clear objectives. When carefully designed, game objectives can be linked to educational ones, contributing to educational achievement.
- Through visualization, games contribute to a better understanding of abstract concepts.
- Players take on realistic roles, design strategies, and make decisions. This contributes to the development of critical and analytical thinking as well as problem-solving skills.
- Games provide real-time feedback. This facilitates the understanding of the consequences of their choices uncovering the links between cause and effect. This process contributes to the scaffolding of knowledge.
- Games may also be used for learners´ evaluation of consequences in a safe environment. They may also be deployed in authentic evaluation, that is processes that simulate how it will be used in real life contexts.
- Games are beneficial and effective for (initial) trainings covering dangerous processes and practices or if deploying physical spaces for training is expensive.

4.2 Educational Escape Rooms (EERs)

An "escape room" is a game in which a team of players discover clues, solve puzzles, and accomplish tasks in one or more rooms to achieve a victory goal in a limited time period. Games are set in a variety of fictional locations, such as prison cells, dungeons, laboratories and even space stations, depending on the theme of the game. The players` goals and the challenges they encounter are also aligned with that theme.

"The development of escape rooms dates back to 2007 in Japan, where they were implemented for commercial purposes. Since first being introduced to the U.S. in 2013, they have experienced fast growth in popularity (Nicholson, 2015)." (Martina, Richard & Göksen, Sultan, 2020)

The game normally begins with a brief introduction to the rules of the game, delivered in form of video, audio, or by a live gamemaster. The players then enter a room or area where a clock is started that limits the time they must complete the game, which typically is between 45 to 60 minutes. The players then explore, find clues, and solve puzzles that allow them to progress further in the game. These challenges are generally more mental than physical but different knowledge and skills are required for different types of puzzles. If players get stuck, there may be a mechanism in place by which they can ask for hints. Hints can be delivered in written, video, or audio form, or by a live gamemaster. The players loose if they are unable to complete all the puzzles within the allotted time. Good endings are usually represented by either escaping “alive” within the time limit, completing the room’s objective, or even stopping the threat or antagonist of the story, while bad endings usually represent the players getting “killed” by the main driving force of the story or an antagonist of the room coming to get the players once the timer has run out. Besides the entertainment factor, escape rooms can also be used to encourage collaboration, teamwork, and team building.

Virtual, digital, or online escape rooms are digital counterparts of escape rooms that take place through a computer and network. The team communicates and collaborates through an online synchronous platform like Zoom while using a software application that can be run by one player and shared to the others or that allows multiplayer involvement. Like for physical escape rooms, teams solve riddles and complete puzzles in a fixed amount of time. More complex digital escape rooms can use virtual reality to increase the sense of immersion of the players.

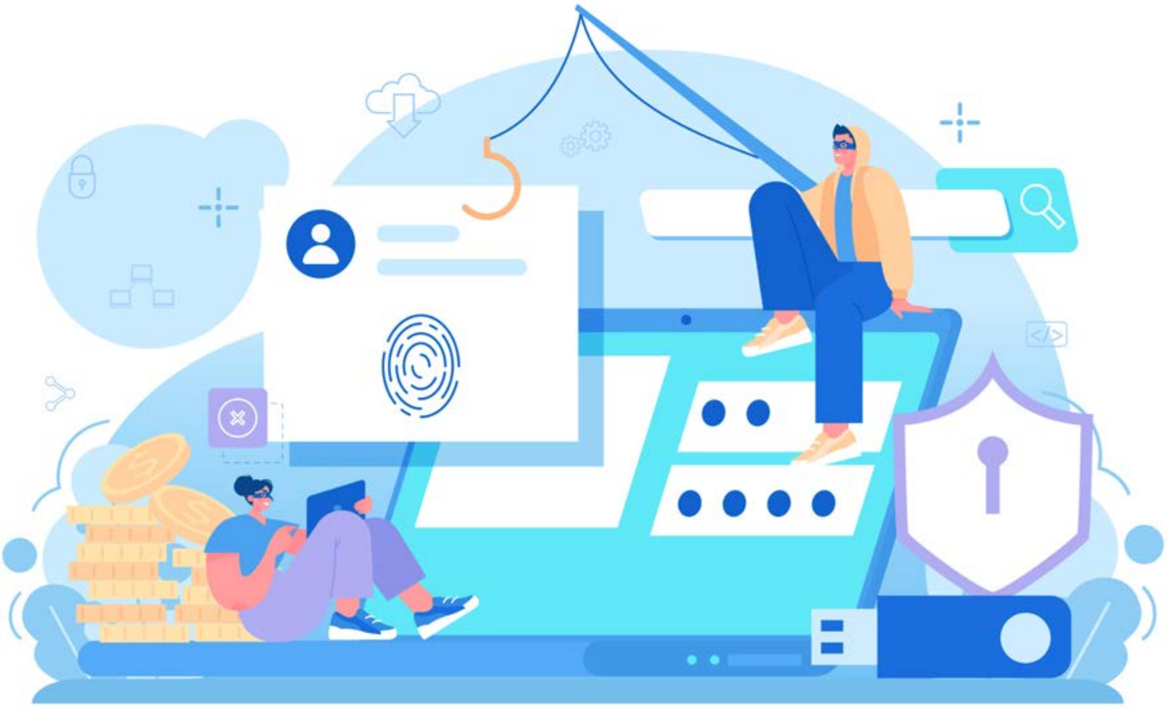
For several years now, the academic sector has also embraced the benefits of Escape Rooms and uses them for their purposes. For some time, there have been various scientific studies on the effectiveness and use of EERs around the world. In Europe, there is not yet too much research on the topic, but it is growing remarkably (Tercanli, H. et al. 2021). Escape Room models are used in different topic fields. The EyesOnCS project intends to support SME education in cybersecurity by adopting an escape room approach in a virtual environment. 22% of the EERs used so far have been in the field of Computer Science and thus already belong to the top 3 studies for which EERs have already been used (Tercanli, H. et al. 2021).

Educational Escape Rooms are used for different stages during the learning process. While some EERs do not require any prior knowledge and let you learn the basics, other EERs may require prior knowledge and deepen the knowledge with their teaching approach (Guckian et al. 2020; Mac Gregor, 2018; Tercanli, H. et al. 2022).

All in all, by using the Escape Room approach, soft-skills in general get promoted, but also the motivation is increased and skills such as problem-solving, team building, out-of-the-box-thinking, critical questioning are brought in. Besides the many different skills, also awareness of a certain topic is created while learning with the Escape Room approach. Thus, it is an extremely effective learning method that significantly increases the knowledge of the participants of the EER by about 53%. The consolidation of knowledge also plays an important role here and is given (Tercanli, H. et al. 2021).

The Escape Room Model approach can also be put to good use in companies. EyesOnCS and the resulting Escape Room about cyber security are intended to raise awareness and train (non-technical) employees in their knowledge of the subject. Here we already start with the basics and thus give the players a sense of security through playful learning. Here, too, as in the HEI, the steep learning curve will take effect and motivation will be given for a topic that still seems foreign to some.

5 Cybersecurity Cases



The perspective of cybersecurity especially for SME businesses and companies is worrisome. The level of protection of the companies is not related to the constantly growing digitalized innovation as well as the interconnection of digital devices. Many people are also too careless in their private use of end devices and thoughtlessly disclose private and personal information on the Internet. It is important to show the dangers and personal consequences of this behaviour and to explain on how to deal with professional information appropriately. Since small and medium-sized enterprises guarantee economic stability in many European countries, it is particularly important to sensitise employees to make Europe a little more resilient.

It is an important goal of this compendium to provide readers with experiences from cybersecurity practice. To achieve this goal, the project partners involved have compiled different security incidents. These security cases are described in detail in the following chapter.

Cases have been collected by all partner organisations in all partner countries: Italy, Portugal, and Germany. The following chapters provide detailed description of the cases.

5.1 Cybersecurity Cases from Italy

Case 1 – The importance of firewalls in cybersecurity

Title	The importance of firewalls in cybersecurity
Case source	Post e Italiane PST - National Postal service company (Italy)
Occurrence period	August 2021
Tags	Company, Identity Theft, Email-attack, Phishing
Status	closed by the end of August 2021 by login credentials modification
Applicability Escape Room	Highly applicable: It is a common case that can be easily understood

Eyes on Phishing:
Phishing attacks involve sending mass amounts of fraudulent emails to unsuspecting users, disguised as coming from a reliable source. The fraudulent emails often have the appearance of being legitimate but link the recipient to a malicious file or script designed to grant attackers access to your device to control it or gather recon, install malicious scripts/files, or to extract data such as user information, financial info, and more. Phishing attacks can also take place via social networks and other online communities.[18]

What kind of attack was it?

Phishing Attack

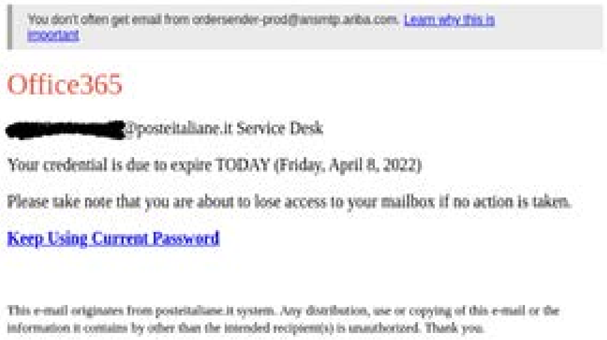
Weakness/Vulnerability:

Human mistake - victim´s incautiousness or ignorance led to the cyber threat.

What happened?

- Unknown cyber criminals managed to trace the email contact of the employee, the victim of the attack. The victim received an email asking to update his login credentials of Office 365 Teams (the online platform used within the company).
- The victim clicked on the fake link included in the mail sent by the cybercriminals and entered his company´s account login information.

[18] https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks



You don't often get email from ordersender-prod@ansmtp.ariba.com. Learn why this is important

Office365

[redacted]@posteitaliane.it Service Desk

Your credential is due to expire TODAY (Friday, April 8, 2022)

Please take note that you are about to lose access to your mailbox if no action is taken.

Keep Using Current Password

This e-mail originates from posteitaliane.it system. Any distribution, use or copying of this e-mail or the information it contains by other than the intended recipient(s) is unauthorized. Thank you.

Figure 1: E-Mail.

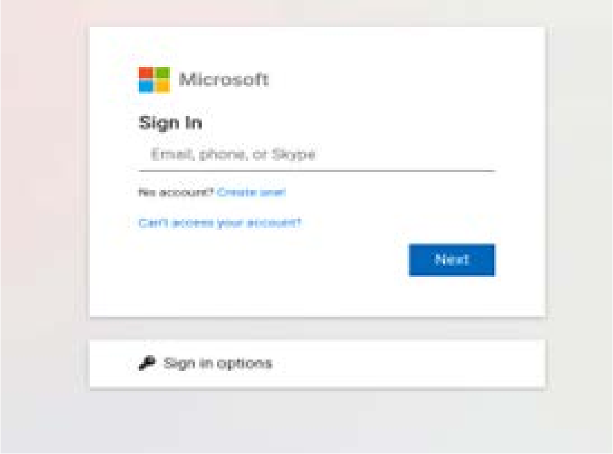


Figure 2: Microsoft Log-In.

How has it been noticed?

The Computer Emergency Response Team (CERT) of the company detected few suspicious accesses from other countries like UK, Algeria, United States while the victim used to log on from Milan, Lombardy, Italy. This aroused the suspicion and mistrust of the CERT.

What measures were taken?

- The CERT asked the victim to confirm if he logged into his account from those countries. The victim denied, so the CERT asked him to change his login credentials.
- Poste Italiane introduced an effective monitoring system operating on the national level. Overall, the company email software is equipped with a Firewall, namely a spam filter that intercepts and blocks most malicious emails.

What is the result of the defence measures?

When any of these spam mails manage to get past the filter, employees have a button on their mailbox for reporting the above-mentioned email directly to the CERT. Once the CERT has analysed the email and classifies it as malicious, it extracts the information and links it contains and places them on perimeter controls, by blocking access to the link.

Case 2 – Supply Chain attack

Title	Supply Chain attack
Case source	ERG Evolving Energies - Italian energy company
Occurrence period	August 2021
Tags	Company, Server-attack, Data Theft, Malware, Ransomware
Status	closed within the week of occurrence by login credentials modification
Applicability Escape Room	Not applicable: The information disclosed by ERG on the way the CS experts acted in handling the hacking attack are not detailed. Therefore, it would be difficult to create the narrative of the case, especially because the main technical aspects of the attack are missing.

Eyes on Ransomware:

A Ramsomware attack is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access.

in the case of Ransomwares, companies have limited options

- pay the ransom
- decrypt the stolen data
- lose/publicly disclose the stolen data.

What kind of attack was it?

Ransomware

Weakness/Vulnerability:

In the case of Ransomwares, it is not possible to identify a "human mistake", because they are targeted attacks perpetrated against companies whose protection systems have been monitored and studied over time by the offenders

What happened?

ERG is the Italian leading wind power operator and among the top ten onshore operators on the European market. The group operates in the wind energy, solar energy, hydroelectric energy, and high-yield thermoelectric cogeneration energy sectors. ERG relies on Engineering Ingegneria Informatica for its IT security services.

- According to the press' reconstruction of events, on July 30th, 2021 the LockBit 2.0 ransomware gang hit Engineering Ingegneria Informatica managing to infect its servers with a virus that had allegedly compromised the access credentials to some of its customer VPNs, including ERG's.
- Engineering Ingegneria Informatica reported the attack to its clients and initiated extensive audits, through which, on the night of August 5th, detected the matrix and extent of the attack, as well as the companies hacked in turn. The attack was conducted by a ransomware operation known as RansomEXX, which passed through Engineering Ingegneria Informatica till reaching ERG's computer system.
- As soon as they entered the system, the cyber criminals copied a part of the company's files proceeding to encrypt them. The criminals publicly blackmailed ERG sharing the message below on the homepage of ERG's website, threatening the company of leaking the stolen data within a few days if the company did not pay a ransom. The main purpose of hacking attacks is indeed to steal data as leverage in extortion attempts.

How has it been noticed?

During the attack, ERG experienced some limited disruptions to its information and communication technology (ICT) infrastructure.

What measures were taken?

- Immediate activation of the internal cybersecurity procedures: ERG did not share detailed information on the technical actions undertaken to tackle the damage caused by the attack. The only certain information available is that the CS society appointed by ERG, Engineering Ingegneria Informatica, asked the company to change the login credentials to accounts.
- Afterwards, ERG confirmed that all facilities were properly in operation and had not suffered any interruptions, thus ensuring business operations.
- To deny the cyber criminals' further access to company data, Engineering Ingegneria Informatica invited ERG to perform password changes on the accounts supported by its teams and report any other suspicion of inappropriate use of its credentials.

What is the result of the defence measures?

Due to the limited extent of damage, ERG refused to pay the ransom. According to the ERG's statement, hackers had encrypted data deemed quite irrelevant.

Case 3 – Denial of Service (DoS) Attack

Title	Denial of Service (DoS) Attack
Case source	Online Rental Company (Italy)
Occurrence period	October 2021
Tags	SME, Company, Data Theft, Denial-of-Service (DOS)
Status	closed within the week of occurrence, by closing the online platform and creating a new one.
Applicability Escape Room	Applicable with difficulties: although it is a common case, its consequences are not perfectly replicable.

Eyes on DoS:
DOS attacks work by flooding systems, servers, and/or networks with traffic to overload resources and bandwidth. This result is rendering the system unable to process and fulfil legitimate requests. In addition to denial-of-service (DoS) attacks, there are also distributed denial-of-service (DDoS) attacks.
DoS attacks saturate a system's resources with the goal of impeding response to service requests. On the other hand, a DdoS attack is launched from several infected host machines with the goal of achieving service denial and taking a system offline, thus paving the way for another attack to enter the network/environment.[19]

What kind of attack was it?

Denial of Service (DoS)

Weakness/Vulnerability

Human mistake – The head of the Company was ill-advised.

What happened?

- Before the problem occurred, the company presented had relied occasionally on Sync Security (SS), a private Cyber Security company specialized in data protection, compliance, and business continuity. Four months before the attack, SS detected on the online platform "Shutdown" the concerned company was ranked among the first 100 companies most vulnerable to cyber-attacks.
- Platforms like "Shutdown" report data – collected over time by web spiders – indicating

[19] https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks

the type and level of vulnerability of companies' domains and explain the ways such vulnerabilities can be exploited. These platforms are easily accessible to everyone, thus exposing even more the companies that are ranked among the first hundred.

- It is indeed statistically proven to suffer a cyber-attack within the first 12 months after the publication of such ranks. Since attacks perpetrated on the basis of the information disclosed by these platforms are not targeted (in un-targeted attacks, attackers indiscriminately target as many devices, services or users as possible. They do not care about who the victim is as there will be a number of machines or services with vulnerabilities[20]), therefore it is possible for companies to defend themselves against cyber threats and prevent economic or data loss.
- Sync Security's SOC (Security operation system) therefore reported to the head of the Company this risk, however he underestimated the issue and refused to make use of preventive defence measures.
- Four months later, the Company's website in the form-based customer interaction section suffered a first DOS: the unknown cyber criminals, from a – non-specified – European country, managed to block the website, thereby preventing its productivity.

How has it been noticed?

In a very short time, the attacks became more targeted and deeper, resulting in the compromise of both commercial and customers' personal data. Therefore, the head of the Company required the intervention of Sync Security's experts.

What measures were taken?

- The intervention was immediate: Sync Security's experts put containment measures in place. Within 3-4 hours the attack became even more aggressive, hence the measures put in place were no longer sufficient to contain the damage.
- Sync Security's experts, upon permission of the company's CEO, made the drastic decision to block access to the site for users outside Italy.
- In between the problem - an error related to the site code - was fixed and Anti-DOS presidiums were put in place. Moreover, in the following days, Sync Security's experts made use of a platform to monitor the IP rating of every user.

What is the result of the defence measures?

- Shutting down the website and reopening it once the threat has been neutralized.
- Shutting down the website from Google through the hosting society resulted in the disappearance of the company and its rental platform from the browsers. Therefore, the company had to undertake promotional campaigns, marketing activities and DEM (Direct Email Marketing) that further weighed on the loss budget.

Lessons Learned:
After this experience, the company decided to invest 0,5% of revenue in Cyber Security, by entering a contract with Sync Security.

[20] National Cyber security center, https://www.ncsc.gov.uk/information/how-cyber-attacks-work, accessed on Juanuary 20 2023.

Case 4 – SQL Injection

Title	SQL injection
Case source	Insurance Company (Italy)
Occurrence period	October 2021
Tags	SME, Company, Payment information Theft, SQL injection
Status	closed by the end of November 2021 after a technical audit.
Applicability Escape Room	Not applicable: The information on how CS experts acted in handling the hacking attack are not detailed. Therefore, it would be difficult to create the narrative of the case, especially since it was a false alarm.

Eyes on SQL:
This occurs when an attacker inserts malicious code into a server using server query language (SQL) forcing the server to deliver protected information. This type of attack usually involves submitting malicious code into an unprotected website comment or search box. Secure coding practises such as using prepared statements with parameterized queries is an effective way to prevent SQL injections.
When a SQL command uses a parameter instead of inserting the values directly, it can allow the backend to run malicious queries. Moreover, the SQL interpreter uses the parameter only as data, without executing it as a code.[21]

What kind of attack was it?

SQL injection

Weakness/ Vulnerability

Human mistake: website user produced an technically inaccurate report.

What happened?

In the months leading up to the attack, the Cyber Security Agency appointed by the company performed several penetration tests to evaluate the security level of the company system. Although these security tests were conducted thoroughly in the course of ten days in November 2021, while the company was running a sales promotion, it received a report from a consumer organisation, which ended up blocking the campaign.

[21] https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks

How has it been noticed?

A member of the consumer organisation claimed to have lost his money while entering his payment information on the company website.

What measures were taken?

- The company attorney suggested the head of the company to take the website offline. It was thought to be a case of SQL injection, allegedly a cyber-criminal inserted a malicious code into the company server using Server Query Language (SQL), hence forcing the server to deliver protected information.
- The head of the company required an explanation from the Cyber Security Agency: how was it possible that right after a penetration test the company suffered a cyber-attack? Especially since for this kind of Agencies, cyber-attacks such as SQL injections are quite easy to detect.
- The Cyber Security Agency took immediate action, also conducting – in private – a passive analysis about the report.
- The customer who reported to have lost his money while entering his payment information on the company website was an undergraduate student of computer engineering, who, having some knowledge on the topic, was misled by the fact that he read “injection” within the source code HTML of the Company website, when it is just a feature of Java programming language.

What is the result of the defence measures?

- The static program analyses determined the attack never occurred. Therefore, the theft suffered by the user was not related to the company's website. While it was unlikely that a system that had only recently undergone pressure testing would have a vulnerability; this had to be officially verified by technical audit.
- Having taken the website offline was costing the company a large loss of revenue.

Lessons Learned:

In this case there is less a mistake, but rather a merit. The company – however small – by entrusting a professional Cyber Security Agent to perform security tests, proved to be foresighted. Indeed, the investment done on cyber security, helped the company prevent the risk of a major loss of profits. Indeed, having had professionals to rely on, the company website was put back into operation immediately after the result of the technical analysis carried out within a few hours. On the contrary, without prevention, this report made by the user, which eventually turned out to be inaccurate, would have cost the Company three times as much in lost profits, in addition to the cost of emergency intervention by CS specialists.

Case 5 – Smishing

Title	Smishing
Case source	Small retail enterprise
Occurrence period	occurred March 2021
Tags	Enterprise, Identity Theft, SMS attack, Phishing, Smishing
Status	closed by the end of March 2021 by login credentials modification.
Applicability Escape Room	Highly applicable: It is a common case that can be easily understood and can be transferred into the escape room model.

Eyes on Smishing:
Smishing is a form of phishing that uses mobile phones as the attack platform. The criminal executes the attack with an intent to gather personal information, including social insurance and/or credit card numbers. Smishing is implemented through text messages or SMS, giving the attack the name "SMiShing.". When cybercriminals "phish," they send fraudulent emails that seek to trick the recipient into clicking on a malicious link. Smishing simply uses text messages instead of email. In essence, these cybercriminals are out to steal your personal data, which they can then use to commit fraud or other cybercrimes.

What kind of attack was it?

Smishing

Weakness/Vulnerability

Human mistake - the victim fell into a trap. He did not realize that his bank already had his personal details, therefore there was no reason to ask the customer to fill in a form. The customer obviously did not know that a bank would never ask a customer to fill in forms/ logins via Email.

What happened?

- The unknown cyber criminals managed to trace the personal number of the employee, the victim of the attack. The victim had applied for mortgage subrogation, i.e., had initiated the process of transferring the mortgage from one bank to another, however, he was still waiting for his old bank to send him all the necessary documents.
- The victim received a SMS informing him that his documents had been uploaded on his

mobile banking account and asking to click on a link to proceed to the download from the personal area of the bank website. The victim used the enterprise computer to perform this procedure, to download and print the papers in the office. He clicked on the link and was redirected to a website, a perfect copy of the original one, so he did not bother checking the website URL. Here he was requested to fill in a form with his personal data: Name, surname, phone number, tax code.

- Once done, a notification “we have sent your documents” popped-up, this time asking to click on the link and insert his log-in credentials. Although the victim was sure to have inserted the right credentials, yet the password was “wrong”. The page which apparently was just refreshed was the real page of the Bank.
- The criminals have stolen the login credentials of the Bank and so had access to the victim's personal data. They used the credentials and succeeded to overcome the multifactor authentication system, allowing them to control the mobile token device and to authorise bank transfers directly from the personal area of the bank website.

How has it been noticed?

After a few hours, when the victim logged in on the mobile app of the bank with his smartphone, he immediately realized he had a lower account balance.

What measures were taken?

- The victim changed the log-in credentials and notified the banking institution he fell victim to a phishing campaign.
- He reported about the attack also inside the company. The enterprise appointed a cybersecurity specialist to conduct deep analysis of the system if one of the links, the victim clicked on, downloaded malware or any further threat to the Company database. The technical analysis did not detect any virus: the company data was safe.

What is the result of the defence measures?

The situation has been solved by changing the log-in credentials. However, the victim was unable to get the money back. He should have contacted the Bank to make sure of the veracity of that SMS. Furthermore, he should not have used the company computer to take care of his personal matters, even if urgent. In this case it also has to be considered the psychological side of the situation: mortgages are sensitive matters, so it is also understandable that the victim felt the urge to take care of the paperwork as soon as he received the SMS - in this case a malicious one – in this regard.

Case 6 – Spam phishing

Title	Spam phishing
Case source	Government body
Occurrence period	occurred in 2018
Tags	government body, Identity theft, Social engineering, Email attack, Phishing
Status	closed by login credentials modification
Applicability Escape Room	Applicable with difficulties: This is a very sophisticated phishing campaign, so it would be difficult to reproduce certain elements.

Eyes on Social Engineering:
Social engineering attack technique consists of psychological manipulation to trick users into making security mistakes or giving away sensitive information. In this case the unknown cyber criminals first investigated the intended victims to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack.

What kind of attack was it?

Spam phishing

Weakness/Vulnerability

Human mistake - Social engineering. The victims fell into a very sophisticated scam, carefully detailed and developed over time. When cyber criminals put in place processes to retain the victims, it is very difficult to distinguish malicious emails from truthful ones. This is one of the major risks associated with social engineering, that leverages victims' weaknesses, in this case a psychological reward linked to a passion, to extort sensitive information.

What happened?

- At the time of the attack, the emails of employees of this government body were generated in the same way: first name + last name + domain. Thus, the information of the email address holders was not obscured, as they were not considered sensitive data.
- This made it easier for criminals to trace the identities of a group of employees. The perpetrators began spying on the social profiles - Instagram, Facebook, Twitter, LinkedIn -

of these employees, and by looking at the photos and videos posted, pages followed, and followers, they identified a common passion of about 20 employees: bodybuilding. Thus begin a very sophisticated phishing campaign.

- At first, the criminals started a phishing test activity: they sent empty emails to the victims to see who was most likely to fall into the trap. Afterwards, these employees received an email regarding a new agreement between the government body and a famous brand of workout supplements, on which occasion this brand was launching a sales campaign. By entering their purchase and shipping information at the link on the email, they would have joined this sales campaign, receiving the products at their doorstep at a very special price. Of these 20 employees only two have been deceived.
- By clicking on the link, they have been redirected to the - FAKE - log-in page of the government body, where “being a promotion exclusively for employees of that government body”, they were required to sign-in with their log-in credentials: username and password.
- Once the payment was "finalised” on the FAKE brand website - in which even a customer service number was available - the criminals put in place a process to retain the victim, by sending the purchased goods. The criminals made sure to make the shipment plausible: taking care of every detail, such as the packaging, labels, etc.
- Having received the purchased goods, the two victims spread the word among their colleagues of the alleged veracity of this sales campaign. Thus, the malicious link resulting from the phishing campaign began to circulate among the employees - at different levels - and in a few days as many as 300 people fell into the trap.

How has it been noticed?

Only when a superior learned what was going on, knowing there was any agreement with this brand, he figured it out that the personnel had fallen victim to a scam. The employees not only recklessly gave away their personal info and payment details, but also exposed at risk the body they work for, which as a government owns a huge number of citizens' personal data, the uses of which for malicious purposes could be innumerable.

What measures were taken?

- To batten down the hatches, all accounts of victims of the scam were blocked and passwords were subsequently changed.
- The government today then proceeded to replace usernames as well.

What is the result of the defence measures?

- The situation has been solved by changing passwords and gradually usernames.
- Today, four years after the attack, all email addresses have been changed: it is not possible anymore to trace back the identity of the email address holders, since name and surname have been replaced with a code.

5.2 Cybersecurity Cases from Germany

Case 1 – Spam E-mails

Title	Spam E-mails
Case source	Media technology Consulting, German/ Bielefeld local SME
Occurrence period	occurred March 2022
Tags	SME, Identity theft, Email-attack, Scam
Status	closed by 25.3.22 by password modification
Applicability Escape Room	Applicability and transferability to the Escape Room Model Very easily applicable: The simple case is easy to be understood and can be transferred to a limited escape room model.

Eyes on Identity theft
Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed in many different ways and its victims are typically left with damage to their credit, finances, and reputation.

What kind of attack was it?

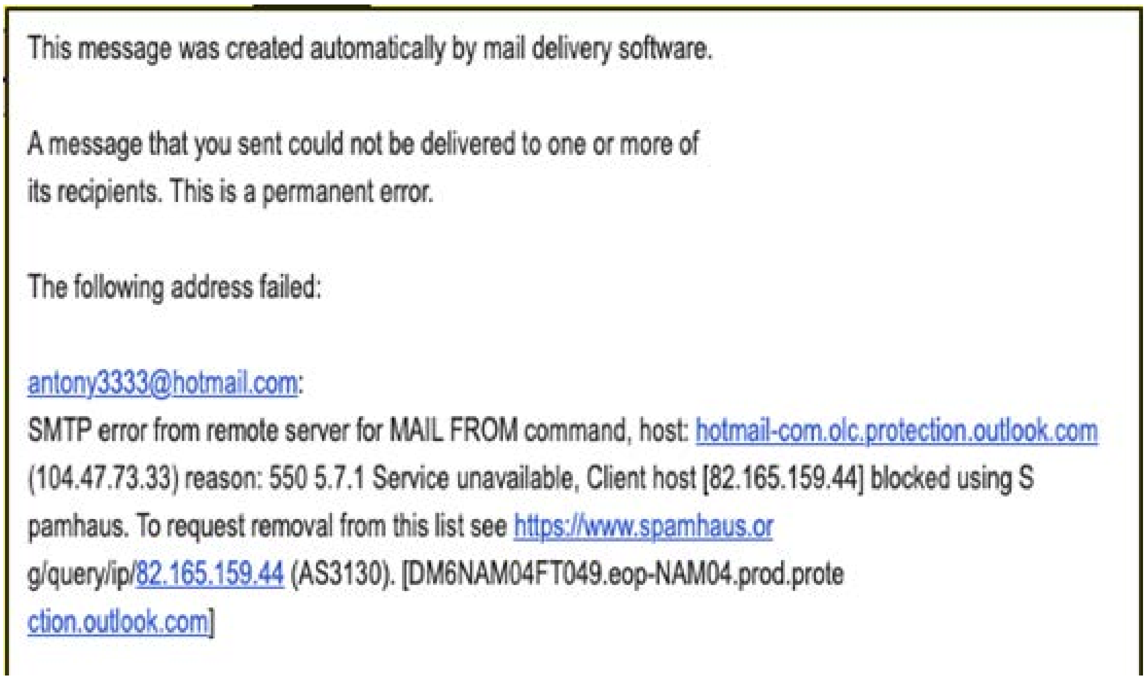
Identity theft

Weakness/Vulnerability:

Human mistake – Password too simple or not changed recently.

What happened?

The perpetrator apparently obtained the password of the victim's account. From this account, the cybercriminal sent spam emails, presumably in large numbers to addresses unknown to the victim.



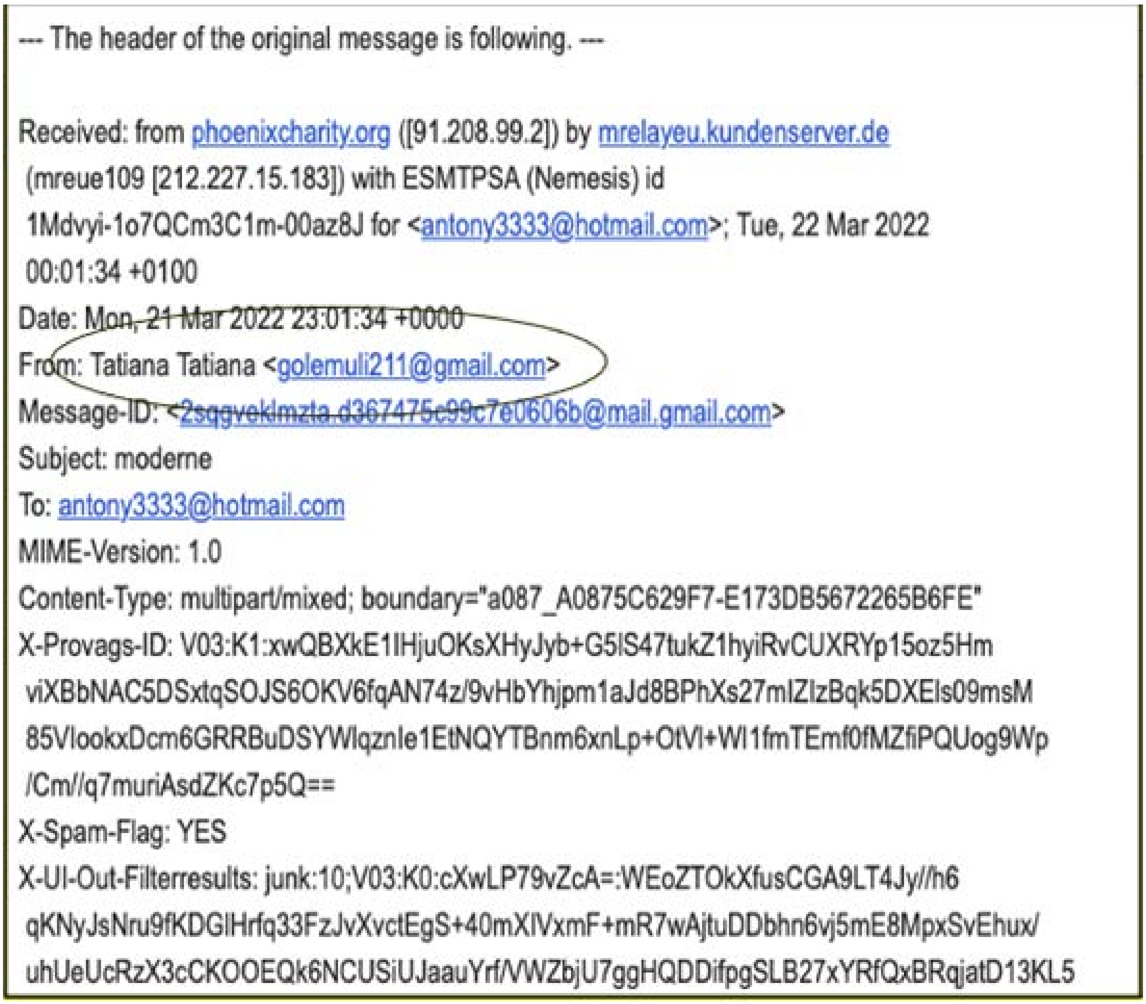
```
This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of
its recipients. This is a permanent error.

The following address failed:

antony3333@hotmail.com:
SMTP error from remote server for MAIL FROM command, host: hotmail-com.olc.protection.outlook.com
(104.47.73.33) reason: 550 5.7.1 Service unavailable, Client host [82.165.159.44] blocked using S
pamhaus. To request removal from this list see https://www.spamhaus.or
g/query/ip/82.165.159.44 (AS3130). [DM6NAM04FT049.eop-NAM04.prod.prote
ction.outlook.com]
```

Figure 3: Failure Notification Mail from Receiving mail Server.



```
--- The header of the original message is following. ---

Received: from phoenixcharity.org ([91.208.99.2]) by mrelayeu.kundenserver.de
 (mreue109 [212.227.15.183]) with ESMTPSA (Nemesis) id
 1Mdvyi-1o7QCm3C1m-00az8J for <antony3333@hotmail.com>; Tue, 22 Mar 2022
 00:01:34 +0100
Date: Mon, 21 Mar 2022 23:01:34 +0000
From: Tatiana Tatiana <golemuli211@gmail.com>
Message-ID: <2sqgveklmzta.d367475c99c7e0606b@mail.gmail.com>
Subject: moderne
To: antony3333@hotmail.com
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="a087_A0875C629F7-E173DB5672265B6FE"
X-Provags-ID: V03:K1:xwQBXkE1IHjuOKsXHyJyb+G5lS47tukZ1hyiRvCUXRYp15oz5Hm
 viXBbNAC5DSxtqSOJS6OKV6fqAN74z/9vHbYhjpm1aJd8BPhXs27mIZIzBqk5DXEls09msM
 85VlookxDcm6GRRBuDSYWlqznle1EtNQYTBnm6xnLp+OtVl+Wl1fmTEmf0fMZfiPQUog9Wp
 /Cm//q7muriAsdZKc7p5Q==
X-Spam-Flag: YES
X-UI-Out-Filterresults: junk:10;V03:K0:cXwLP79vZcA=:WEoZTOkXfusCGA9LT4Jy//h6
 qKNyJsNru9fKDGIHrfq33FzJvXvctEgS+40mXlVxmF+mR7wAjtuDDbhn6vj5mE8MpxSvEhux/
 uhUeUcRzX3cCKOOEQk6NCUSiUJaauYrf/VWZbjU7ggHQDDifpgSLB27xYRfQxBRqjatD13KL5
```

Figure 4: Header of the Spam Mail.

- According to Figure 3 this mail was blocked by the receiving mail server based on spam detection. It can be assumed that a high number of spam emails sent automatically from the victim's account, reached the addresses specified by the attacker. This is the primary impact of the attack. Only assumptions can be made about the contents sent.
- Further research[22] discovered that often spam/scam mails with the return address golemuli211@gmail.com distributed the content shown Figure 4. It must be noted that the scammer did not use the return address of the victim.
- The damage thus seems to be limited to sending spam/scam from the victim's account. No money was requested from the victim.

How has it been noticed?

The victim's email provider obviously recognized the account abuse and sent the following warning to the victim (see fig. 4). At the same time, the victim of the attack noticed that emails that were apparently sent from his account were rejected by receiving mail servers. The number of these mails was very high, about 200.

What measures were taken?

Measure: Change to a more save password
To solve the present problem we conducted the following checks and measures:

- **Check 1: Was the e-mail(s) sent without users' knowledge?**
  - Check their end devices (PC, smartphone, or tablet) with an up-to-date virus scanner.
  - Update the software on users end devices and activate automatic updates.
  - Use the firewall on your router, PC or internet security software.
  - If a virus was found and successfully removed, change your passwords.
- **Check 2: Did the user send the mail on purpose?**
  - Check whether the email software you are using is configured correctly.
- Making sure that the recipient addresses are reachable by regularly maintaining users mailing lists.
- If user send newsletters or other mass mailings, attention to the following standards would have been taken:
  - Did sender have the recipient's consent (double opt-in)
  - The newsletter contains a link that allows the recipient to unsubscribe with just one click (opt-out)
  - E-mail recipients for whom the user receives an undeliverable message is automatically deleted from the address database (bounce management)

What is the result of the defence measures?

- In this case the Email password was changed by the victim within a short period of time
- The block was automatically removed by the provider within a few minutes.

[22] https://www.django-hurtig.com/jagdzentrum/jagd_vorgang_mainstream_id.php?id2=21727

Case 2 – Installation of Crypto Miner software

Title	Crypto Miner software was installed
Case source	Undisclosed customer/Germany
Occurrence period	occurred June 2019
Tags	SME, crypto miner, crypto jacking, scam
Status	closed and technically solved
Applicability Escape Room	Very easily applicable: The simple case is easy to be understood.

Eyes on Crypto miners:
Cryptocurrency mining is a process of creating new digital "coins." However, that is as far as simplicity goes. The process of recovering these coins requires solving complex puzzles, validating cryptocurrency transactions on a blockchain network and adding them to a distributed ledger to locate them.

What kind of attack was it?

Crypto Miners

Weakness/ Vulnerability:

Human mistake – Downloading and installing open-source software from the Internet was the trigger for this attack. It was not downloaded from "safe" or "official" manufacturer sites.

What happened?

- At a customer's site, crypto miners were installed as a result of an arbitrary software download by the employees. When the crypto miners were uninstalled, an encryption of the network structure (servers, clients, backups, shadow copies, etc.) started. This was followed by an extortion of the client.
- The customer's employees had local admin rights and were allowed to install software on the clients. As a result, crypto miners had installed themselves as well.
- The crypto miners started working immediately after the installation and used the full client resources for mining.

How has it been noticed?

The performance of the clients became worse and worse. Simple processes took a very long time. Furthermore, the utilization of the CPU and RAM was consistently at 99%.

What measures were taken?

- The network structure was disconnected from the Internet
- The clients and servers were removed from the network
- The entire technical infrastructure was reinstalled
  - Uniform virus protection, externally stored backups, admin rights were withdrawn from users
  - Firewall system was installed

What is the result of the defence measures?

- As a result of the security measures implemented, there was no renewed infestation.
- Malware that had already been downloaded was removed by the virus protection system before it could be executed.
- During the uninstallation, the software started an encryption of the network structure. Here, all devices available on the network were encrypted.
- The backups and shadow copies were deleted and could not be restored. The customer was reset from 01.07.19 to 31.12.18.
- The data had to be maintained manually. There was no response to the extortion.
- The infrastructure was reinstalled and partially restored from the existing old backups.

Lessons learned:

This type of attack can happen again. However, it can be prevented by a uniform, up-to-date virus protection with additional modules such as an Intercept X or a sandbox. Furthermore, the admin rights can be withdrawn from the users, so that not just any software can be installed.

Case 3 – Phishing Mail/Attack

Title	Phishing mail /attack
Case source	Undisclosed customer / Germany
Occurrence period	occurred February 2022
Tags	SME, phishing, fraud
Status	The case was technically solved.
Applicability Escape Room	Case easily applicable: The simple case is easy to be understood and can be transferred to a limited escape room model.

What kind of attack was it?

Phishing

Weakness/Vulnerability:

Human mistake – the customer's username and password for online banking were entered following the link of a phishing mail and transmitted to the phishing perpetrator.

What happened?

Phishing mails with updated terms and conditions or cost changes were sent to a customer. Afterwards, the online banking login had to be performed to view the changes.

How has it been noticed?

The internal IT administrator of the reporting company was contacted. He analysed and checked the mail.

What measures were taken?

- The mail domain was blocked via the firewall.
- However, about 3000€ were transferred to another bank account by this fraud. Currently, the reimbursement via the bank is still pending.

What is the result of the technical / organizational / social defence measures?

- Employee training in the area of awareness was carried out.
- Employees received an "info sheet" with information on how to recognize phishing mails. Afterwards, phishing mails were no longer clicked on and deleted directly.

Lessons learned:
This type of attack can happen again at any time. A sustainable solution is difficult to implement. Official mail domains like Gmail or similar can be used. If you block them, among other things, "official/correct" mails will no longer arrive. The links are also regenerated each time of an attack. Here blocking only provides a temporary protection.

Case 4 – Phishing Mails/Attacks

Title	Phishing Mails in order to obtain mail login data
Case source	Admin of educational institution / Germany
Occurrence period	occurred March 2022
Tags	SME, phishing, login data, spam
Status	The case was successfully processed and closed.
Applicability Escape Room	Case easily applicable: The simple case is easy to be understood and can be transferred to a limited escape room model. Since the case is a very often occurring standard case, it is not very interesting for the model.

What kind of attack was it?

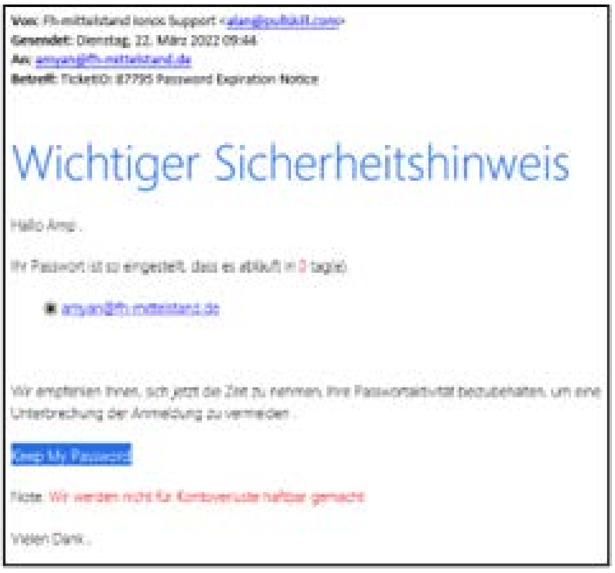
Phishing

Weakness/Vulnerability:

There was no incorrect behaviour on the part of the colleague, she acted correctly and reported the incident. The spam and scam protection allowed the mail through in this case, as the score for a mail defence was not reached.

What happened?

- The employee of the educational institution received a phishing e-mail saying that her mail password has expired, and she should set a new password.
- The sender of the mail was the alleged provider: Ionos (1&1) support.



Von: Fh-mittelstand Ionos Support <[illegible]>
Gesendet: Dienstag, 22. März 2022 09:44
An: amyan@fh-mittelstand.de
Betreff: TicketID: 87795 Password Expiration Notice

Wichtiger Sicherheitshinweis

Hallo Amy ,

Ihr Passwort ist so eingestellt, dass es abläuft in 0 tag(e)

- amyan@fh-mittelstand.de

Wir empfehlen Ihnen, sich jetzt die Zeit zu nehmen, Ihre Passwortaktivität beizubehalten, um eine Unterbrechung der Anmeldung zu vermeiden .

Keep My Password

Note: Wir werden nicht für Kontoverluste haftbar gemacht

Vielen Dank .

Figure 5: safety notice

How has it been noticed?

- Due to the alertness and informedness of the employee the problem was noticed, and the colleagues proactively informed the admin of the IT department. The employees were aware of the fact, the various service providers would never send mails with this content. Passwords do not expire at the institution.
- Additionally, upon closer inspection, the sender could be identified as not legitimate.

What measures were taken?

- The colleague forwarded the mail to the IT-admin.
- The IT department then began taking the usual regular safety measures:
  - First, an entry was formulated in the message centre to warn all other colleagues that phishing attacks had occurred at the given time.
  - In parallel the sender was blocked so that no background communication can take place (blacklist).

What is the result of the defence measures?

- Since the victims and IT departments are virtually powerless against such phishing attacks and no sustainable defence mechanisms can be installed without noticeably restricting the user, no further actions could be taken.
- No damage was done, except for working time invested in clarifying the incident.

Lessons Learned:
After evaluating the incident, additional preventive campaigns and employee training were planned to increase alertness.

Case 5 – Malicious code in mail attachment

Title	Malicious code in mail attachment
Case source	University / Germany
Occurrence period	occurred June 2016
Tags	SME, mail, attachment, spam, ransomware
Status	The case was successfully processed and closed.

Applicability Escape Room	Case very easily applicable: The simple but instructive case is easy to be understood and can very well be transferred to an interesting escape room model. In addition, it is possible to develop a scenario for an instructive and exciting story from the case.

Eyes on Locky attack:
Locky is a type of ransomware. It was released in 2016 while security experts found that the malware authors delivered this ransomware via email asking for payment through an attached invoice of a malicious Microsoft Word document that runs infectious macros. Locky Ransomware is a piece of malware that encrypts important files on your computer, rendering them inaccessible and unusable. It holds them 'hostage', and in the meanwhile, demanding a ransom payment, in exchange for the encrypted files.

What kind of attack was it?

Locky attack - Ransomware Trojan.

Weakness/Vulnerability:

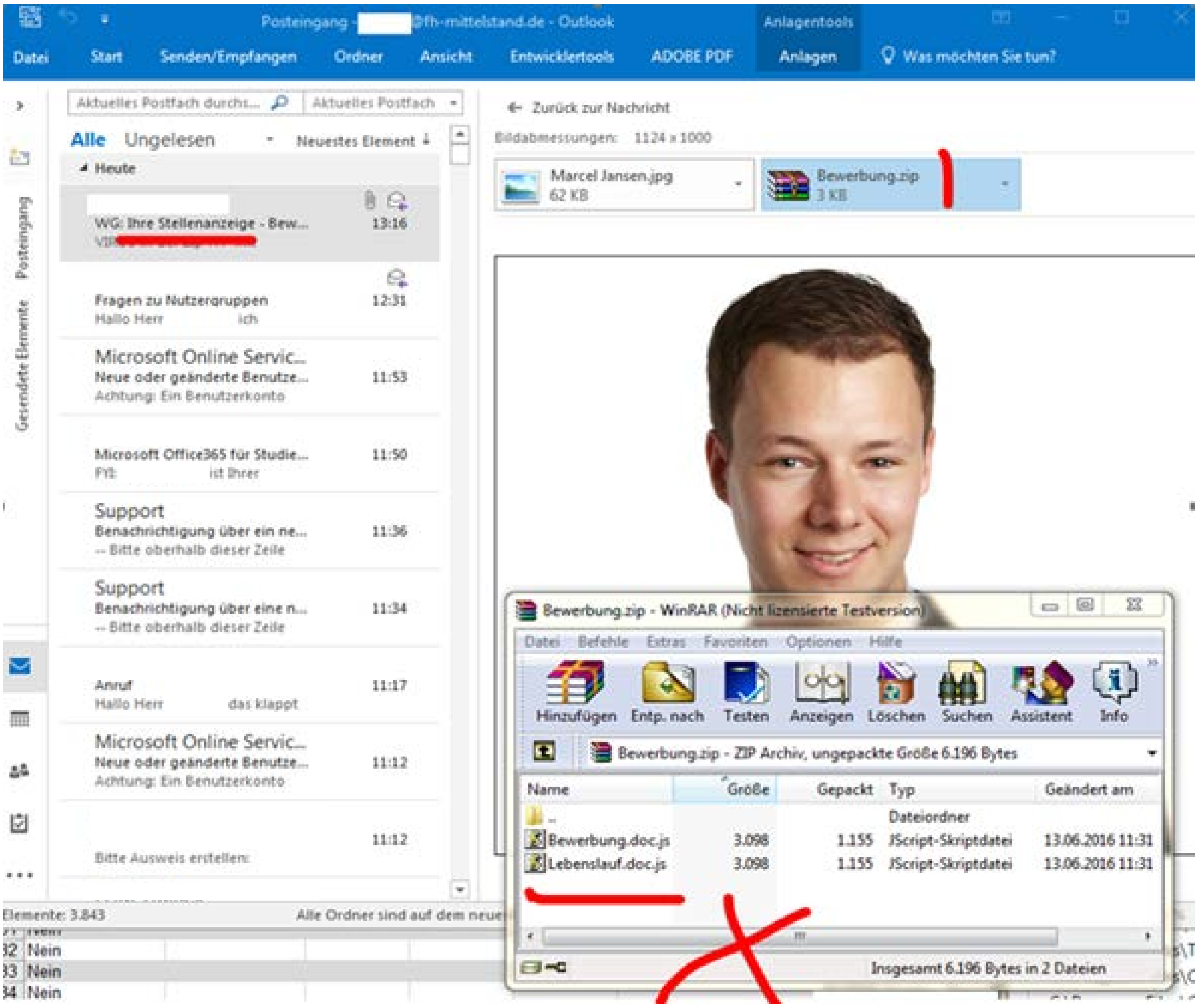
Human mistake - Opening an unknown email attachment. The successful attack was favored by the victim's carelessness and the zero-day variant of this Trojan.

What happened?

- A mail with a zip file that was supposed to contain invoices was sent to a team member (the victim).
- This zip file was encrypted, which made it impossible for antivirus systems to scan it.
- The password for the zip file was in the text of the email.
- The victim opened the zip file without further verification, unzipped the xlsm file and opened it. Afterwards, the victim took his lunch break.
- The virus protection (Kaspersky) - the zero-day variant of this Trojan - and the colleague's lunch break meant that the application had enough time in the background to compromise all the data.

How has it been noticed?

- When the victim returned to his workplace, he wondered about the changed background screen and informed the IT department.
- At this point, about an hour had passed since the victim clicked on the attached macro-Excel file.
- The moment the admin appeared at the victim's computer to help in an emergency, the admin immediately unplugged the LAN and disconnected the WLAN.
- Unfortunately, it was already too late, and the attack had been successfully executed.



[redacted]
WG: Ihre Stellenanzeige - Bew... 13:16
[redacted]

Fragen zu Nutzergruppen 12:31
Hallo Herr ich

Microsoft Online Servic...
Neue oder geänderte Benutze... 11:53
Achtung: Ein Benutzerkonto

Microsoft Office365 für Studie... 11:50
FYI: ist Ihrer

Support
Benachrichtigung über ein ne... 11:36
-- Bitte oberhalb dieser Zeile

Support
Benachrichtigung über eine n... 11:34
-- Bitte oberhalb dieser Zeile

Anruf 11:17
Hallo Herr das klappt

Microsoft Online Servic...
Neue oder geänderte Benutze... 11:12
Achtung: Ein Benutzerkonto

11:12
Bitte Ausweis erstellen:

Elemente: 3.843 Alle Ordner sind auf dem neue

Bewerbung.zip - WinRAR (Nicht lizensierte Testversion)

Bewerbung.zip - ZIP Archiv, ungepackte Größe 6.196 Bytes

Name	Größe	Gepackt	Typ	Geändert am
..			Dateiordner	
Bewerbung.doc.js	3.098	1.155	JScript-Skriptdatei	13.06.2016 11:31
Lebenslauf.doc.js	3.098	1.155	JScript-Skriptdatei	13.06.2016 11:31

Insgesamt 6.196 Bytes in 2 Dateien

Figure 6: The dangerous attachment.

- The admin found a catastrophic situation: all documents were encrypted and no longer usable. Besides the local documents, all the documents accessible on the network drives had been encrypted as well.

What measures were taken?

- To start decryption, the criminal demanded $500 in the form of Bitcoins.
- As about 50% of the staff members could no longer access the work-related documents on the network drive.
- The admin then dismantled the laptop in question. At the same time, a notice was posted in Customer Management System (CMS) about this incident so that telephone accessibility could be restored.
- The IT department immediately ensured that the causing laptop was no longer accessible on the network and then no further files on the network drive were encrypted.

- The laptop was completely formatted, and Windows was reinstalled. There were no local work files.

What is the result of the technical / organizational / social defence measures?

- The IT department, in consultation with the management, imported a full backup of the previous day. As a result, all the processes of all employees from the last 24 hours were no longer available. For some employees this was very critical, but for most the damage was limited.
- The victim was given special training to prevent this case from happening again.
- One day later, information was received from the antivirus vendor at the time that Locky threats are now also detected and prevented.

Case 6 – CEO-Fraud

Title	CEO-Fraud
Case source	University / Germany
Occurrence period	occurred April 2020
Tags	SME, mail, fraud, spam, scam
Status	The problem still exists. (At least similar attempts are still detected, but they are now limited to a limited number of examples, e.g. Apple Gift cards).
Applicability Escape Room	Case is good applicable: The simple but instructive case is easy to be understood and can very well be transferred to an interesting escape room model. In addition, it is possible to develop a scenario for an instructive and exciting story from the case.

Eyes on CEO-Fraud:
Attacker claims to be the CEO of a particular company and tries to force the victim to conduct malicious actions or/and fraud in the name of the real CEO.

What kind of attack was it?

CEO fraud is a highly targeted form of spear-phishing in which attackers research potential victims and their companies online, learning everything they can from the organization's website, as well as information from social media sites such as LinkedIn, Facebook and Twitter. Typically, the attacker aims to trick you into transferring money to a bank account owned by the attacker, to send confidential HR information, or to reveal other sensitive information.

Weakness/Vulnerability:

- It is a CEO fraud. The sender claims to belong to the management with intent to conduct a fraud.
- The spam/scam protection on the part of the mail provider failed or did signalize “fraud”.
- The employee was not trained in order to immediately recognize not legitimated requests. The employee was also very new to the company and had little contact with other colleagues due to Covid19. The employee was also very new to the company and had little contact with other colleagues due to Corona.

What happened?

- An email, supposedly from the management, reaches colleagues: A transfer of money to a foreign country was requested.
- This is not an automated mail; the person being contacted would have been able to initiate this transfer.
- As the real mail address of the attacker is difficult to recognize for the recipient, the user did not really notice this.

How has it been noticed?

- Due to the fact that the transfer of money follows specific rules and a control mechanism inside the organisation, the legitimacy of the transfer could not be confirmed. It quickly became clear that this was a case of fraud.
- If the user had hovered over the mail address directly with the mouse, it would have been quickly noticed that it was a fraud attempt.

What measures were taken?

- The attack was handled by blocking the sender's mail account (Gmail account of the attacker).
- The case was reported to the police, but no perpetrator was identified.

What is the result of the defence measures?

It is not possible to protect oneself sustainably without restricting mail sending too much, so proactive protection continues to be strengthened.

Case 7 – Backdoor in Software – Spy Attack

Title	Backdoor in Software – Spy Attack
Case source	Ministry of the Interior NRW/ Düsseldorf/Germany
Occurrence period	Undisclosed
Tags	Spy attack, backdoor
Status	Resolved
Applicability Escape Room	Case very easily applicable: The interesting case is easy to be understood and can very well be transferred to an interesting escape room model. In addition, it is possible to develop a scenario for an instructive and exciting story from the case.

Eyes on Spy Attack

The theft of research results, product development information, balance sheet figures and customer data cause long-term damage to the companies concerned: foreign competitors obtain the data free of charge. A hard-won competitive advantage can be lost, so that product sales fall. Foreign intelligence services have excellent IT skills and conceal their access. The discovery of an attack often occurs only when an external whistle-blower alerts the company to the attack.

What kind of attack was it?

Spy attack, backdoor

Weakness/Vulnerability:

The third-party software should not have been used unchecked in the company network. Instead, a security concept should have been used to test whether the software could be used in isolation.

What happened?

- Companies with business relations abroad are often obliged to use certain software, e.g. for processing tax obligations.
- A special backdoor software was installed on various computers in the globally networked victim's company.
- Via a hidden backdoor, an attacker was able to access documents in the victim's network.

How has it been noticed?

In the aftermath of the installation, it becomes known that the mandatory software contains a backdoor for the foreign intelligence service.

What measures were taken?

The system got completely re-installed and the backdoor got closed.

What is the result of defence measures?

Further attacks were prevented.

Case 8 – Extended Social Engineering – Spy Attack

Title	Extended Social Engineering – Spy Attack
Case source	Ministry of the Interior NRW/ Düsseldorf/Germany
Occurrence period	Undisclosed
Tags	Spy attack, social engineering
Status	Resolved
Applicability Escape Room	Case very easily applicable: The Interesting case is easy to be understood and can very well be transferred to an interesting escape room model. In addition, it is possible to develop a scenario for an instructive and exciting story from the case.

What kind of attack was it?

Spy Attack

Weakness/Vulnerability:

- Attackers cleverly know how to create fear in the victim that they will miss out on a good offer. Moreover, telephone contact reduces the mistrust towards the attacker. Nevertheless, the malicious document should not have been opened in the company network. Once again, the "human weakness" is exploited.
- What happened?
- In many high-tech fields, it is common for individuals to be contacted by recruiters with offers to change jobs.
- When an employee of a well-known company receives a call on his cell phone from a head-hunter, this does not seem out of the ordinary. After a brief conversation, the supposed

agent announces that he will forward a lucrative job offer. A short time later, the document arrives in the employee's WhatsApp account. When he tries to open it on his cell phone, the process interrupts with an error message.

- The next day, the head-hunter contacts the employee again and promises exceptional earning potential with attractive working conditions. However, feedback on further interest in the offer made must be given immediately. Without further ado, the employee transfers the document received at the presentation to his business email account. After a brief confirmation to use a special format template, he can open the file on his company computer. Since the offer does not meet his expectations, he cancels the job with the head-hunter. After that, the process is forgotten.
- Later it turns out that by opening the document, remote access was established in the employee's company PC. This access enabled the attackers to spread further in the company network and leak sensitive data. The data theft was not noticed until the attackers had long since disappeared.

How has it been noticed?

No further information, because the case is undisclosed by the Ministry of the Interior NRW.

What measures were taken?

No further information, because the case is undisclosed by Ministry of the Interior NRW.

What is the result of the defence measures?

No further information, because the case is undisclosed by the Ministry of the Interior NRW.

Case 9 – Phishing Mail

Title	Phishing Mail
Case source	IT news company, Germany
Occurrence period	Occurred May 2019
Tags	Company, phishing, email attack, ransomware
Status	The status of this case is: closed within several weeks of the problem's occurrence, by creating a new network and replacing all computers connected to the network during the attack.
Applicability Escape Room	Highly applicable: Emotet and trojans are commonly known as well as phishing.

Eyes on Phishing
We have already described phishing attacks, but it is important to note that phishing attacks have adapted over the years and are becoming increasingly "better" and more sophisticated. It is therefore important to keep up to date with the latest phishing methods.

What kind of attack was it?

Phishing attack

Weakness/Vulnerability:

The employee activated macros for the infected file.

What happened?

- An employee opened an email from a spoofed sender posing as a business partner. The email contained an infected Word document.
- When the employee opened this file, an error message appeared prompting the employee to “enable” the edit.
- The employee clicked on this message and Emotet infected his system and started spreading across the network.

How has it been noticed?

Several infections were detected, and several infected computers were found across the network.

What measures were taken?

- Connections from various computers to the outside were established.
- The virus was removed with Avira and Windows Defender.
- Afterwards, the admins tried to prevent the malware from communicating to the Emotet infrastructure. Since this did not work as intended, the whole network was disconnected from the internet.
- External service providers and several IT forensics companies were contacted.

What is the result of the defence measures?

- The whole intranet was restored and all computers that were connected to the intranet during the attack were replaced.
- The security concept was reviewed to prevent this case in the future.

Case 10 – Blackmailer Phishing Mail

Title	Blackmailer Phishing Mail
Case source	Electrical wholesaler (Germany)
Occurrence period	Occurred February 2020
Tags	Company, phishing, email attack, SME, ransomware
Status	Closed within three weeks after the problem occurred by paying the ransom.
Applicability Escape Room	Highly applicable: Missing backups are a great problem and the loss of data without a working backup is catastrophic.

Eyes on Backups

A backup is a copy of data that is made and stored separately from the original data. This copy can be used to restore the original data in the event that it is lost or damaged. It is highly recommended to create and test backups on a regular basis within a company.

What kind of attack was it?

Phishing attack

Weakness/Vulnerability:

The infected email was inadvertently opened by an employee. The ransomware encrypted all files. A negligent opening of suspicious emails and attachment lead to the successful attack. Furthermore, the company had no regular backup strategy. The lack of backup checks forced them to pay the ransom.

What happened?

- An employee opened an infected email attachment. All ads were white and displayed an email address. The malware strain Emoted infected all computers and therefore encrypted all files within reach.
- An external service provider, who was entrusted with creating the backups, had not yet created these. No recent backup was available and the only ones available were too old to work with.
- Nobody oversaw the backups and had checked the date of the last backups. Communication with the external service provider was also unregular.

Additional information: Macros are often used in Office applications such as Word, Excel, and PowerPoint. These macros are saved as part of the document file and are written in a programming language called VBA (Visual Basic for Applications). Macros can be used to infect a system with malware.

How has it been noticed?

Files were encrypted quickly, and the system was not usable.

What measures were taken?

- The company contacted the police and the blackmailer.
- The Blackmailer demanded 21 Bitcoins. Without a functioning backup, their very existence was at risk. Therefore, the ransom of 120.000€ was paid, and all systems were decrypted.
- Communication by mail and no digital billing for three weeks, which resulted in huge financial losses.

Additional information: Not every company which pays the ransom gets their files back decrypted. Even if they get their files back, it is necessary to examine all files for hidden malware.

What is the result of defence measures?

- The email system was then switched to a cloud solution from Microsoft.
- External backups are now created weekly.
- Regular backup and security plans were enabled.
- Cyber-Security trainings

Case 11 – Phishing mail with Malware

Title	Phishing mail with Malware
Case source	Machine safety company (Germany)
Occurrence period	Occurred May 2020
Tags	company, phishing, email attack, ransomware
Status	Closed within two weeks after shutting down the intranet.
Applicability Escape Room	Highly applicable: Emails are dangerous, tips by public authorities have to be taken seriously and be verified.

Eyes on Malware
Malware, short for malicious software, is any software designed to harm or exploit a computer system or network. There are different types of malware, including viruses, worms, Trojan horses, ransomware, and spyware. It is often attached and hidden within other software or links.

What kind of attack was it?

Phishing attack

Weakness/Vulnerability:

Negligent opening of an infected email attachment. The employees were not trained properly so that they were able to detect a suspicious email.

What happened?

Email with malware has been opened.

How has it been noticed?

- Company was informed by a public authority (Landeskriminalamt) about an imminent cyber-attack, using infected mails.
- The company verified this call and decided to disconnect its network seven minutes after the call.

What measures were taken?

- Disconnection of the network.
- Examination and disinfection of all systems of the network. After the disconnection, the malware was identified. Production came to a halt.
- Each computer had to be disinfected individually.
- Replacement server provided email communication.

Additional Information: individual disinfection of every computer is very expensive regarding time and costs for the company / Attack could have been prevented with proper training.

What is the result of the defence measures?

Two weeks later, the IT system and production were up and running again.

Case 12 – Ransomware and Phishing

Title	Ransomware and Phishing
Case source	IT service provider
Occurrence period	Occurred October 2021
Tags	company, SME, ransomware
Status	In progress, 95 % of the systems have been restored.
Applicability Escape Room	Highly applicable: Recovery after a successful attack has to be trained to be fast and efficient.

Eyes on DeepBlueMagic
DeepBlueMagic apparently originates from China. Like several ransomware strains in the past, it encrypts files using common encryption tools such as Bitlocker and BestCrypt, which users often trust and use for encryption themselves.

What kind of attack was it?

Malware "DeepBlueMagic" installed via phishing mail.

Weakness/Vulnerability:

Negligent opening of an infected email attachment. The employees were not trained properly so that they were able to detect a suspicious email.

What happened?

- Providers for public authorities were attacked. An Infectious email attachment containing malware has been opened.
- No personal data was stolen.

How has it been noticed?

The users got emails from the cyber-criminals that their files were encrypted and not usable.

What measures were taken?

- The regional administrative office had to close.
- All systems were shut down.
- In addition to the main systems, 4000 end devices had to be scanned for malware.

- The backups have been restored, but the recovery is still in progress.
- No ransom was paid.

Additional information: This example shows how important a functioning backup system is. Even after the attack they were able to restore the data without paying the ransom. Keep in mind: no backup - no pity.

What is the result of the defence measures?

By the end of 2021, 95 % of all data had been restored.

Case 13 – Malware

Title	Malware
Case source	Investment start-up (Germany)
Occurrence period	Occurred October 2021
Tags	company, SME, ransomware, social engineering
Status	Closed after a few days by closing the exploited vulnerability.
Applicability Escape Room	Applicable with difficulties: Exploiting vulnerabilities needs a certain level of knowledge or they must be very easy to detect. Nevertheless, they require a deeper understanding of IT

Eyes on Social Engineering
Social engineering is the use of psychological manipulation to influence individuals or groups to divulge sensitive information or perform actions that may be harmful to them or their organization. This can include tactics such as phishing, vishing (voice phishing), and manipulation on the phone. The goal is always the same: to deceive people into giving up confidential information or access to systems or networks.

What kind of attack was it?

Ransomware attack supported by social engineering phone calls.

Weaknesses/Vulnerability

Stolen data was used to support and provide credibility to social engineering phone calls.

What happened?

- Phishing attacks which were supported by social engineering phone calls towards the customers.
- The vulnerability in the IT-system was not found in time.
- System vulnerability was used to leak customer data.

How has it been noticed?

During a scan of the system the security leak / attack was localised quickly.

What measures were taken?

- Customers were informed three days later.
- Authorities have been informed.
- Vulnerability has been closed.

Additional Information:

If you have a user who wants to change a password, it is recommended that the responsible IT department publishes requirements regarding secure passwords.

What is the result of the defence measures?

After the vulnerability was closed, customers were notified and prompted to change their passwords.

Case 14 – Malware in Company

Title	Malware in company
Case source	Industrial machinery producer (Germany)
Occurrence period	Occurred July 2021
Tags	Company
Status	Recovered after a few months.
Applicability Escape Room	Applicable with difficulties: The case was very elaborated and by no means a fault of the company - learning lesson: no matter how good your security is, there can always be an attack.

Eyes on Spoof Mails
A spoof email is one in which the sender's email address and other parts of the email header have been altered to appear as though the email originated from a different source. This is often used in phishing scams and other forms of fraud, as it can make the email appear more legitimate to the recipient.

What kind of attack was it?

Elaborated and long planned attack, using a service provider from abroad as an entry to the company via a phishing mail and fake website.

Weaknesses/Vulnerability

Service provider was used as a weak spot - although IT-security and staff from the company was well prepared.

What happened?

The hackers send a spoof mail to a service provider abroad. The mail was linked to a perfectly faked website so that the service provider could not recognize the fraud.

How has it been noticed?

The system completely shut down / was useless, and all files were encrypted.

What measures were taken?

- All systems were switched off.
- All business processes were stopped.
- Blackmailing attempt with conti group.
- External cybersecurity provider was engaged to help restore the systems.

Additional Information: Even if a security system runs well and the staff is trained properly it is always possible to get hacked. Unfortunately, there is no 100% safety of attacks.

What is the result of the defence measures?

- A taskforce was founded. Establishing new communication channels with daily news.
- Public authorities have been notified.
- Different business areas have been prioritized.
- The infrastructure was rebuilt, external IT consulting and support were involved.
- Backups were restored and the recovery was divided into three categories: red (still infected), orange (in quarantine) and green (clean data).

5.3 Cyber security Cases from Portugal

Case 1 – Denial of Service in communication services

Title	Denial of Service in communication services
Case source	Wikipedia[23], Diário de Notícias[24]
Occurrence period	Occurred February 2021
Tags	Company, telecommunications
Status	The status of this case is closed.
Applicability Escape Room	The case might be transferred to the Escape room model because it shows the importance of cyber security for the society. However, the company did not disclose enough information to provide a scenario for the game.

What kind of attack was it?

The company and the police did not reveal much information. It is suspected that a highly sophisticated group of hackers conducted the attack by exploiting some security holes in software that was not updated, but the exploit used was not revealed. The attack envisaged ensuring that the company could not provide its communication services.

Weaknesses/Vulnerability:

The weaknesses resulted from the lack of update of all the software that managed the communication services. It is unclear if there was some inside collaboration as well.

What happened?

Hackers exploited the software vulnerability to gain access to the communication servers and systems and to cause failures in the communication.

How has it been noticed?

- Lack of 3G and 4G network mobile data.
- Lack of services of SMS, TV and fixed Internet customers.
- Lack of voice service.
- 112 (emergency services number) could not be reached.
- SIBS [owner of the Multibanco brand] is a Vodafone customer. Their ATM network was

[23] https://pt.wikipedia.org/wiki/Ciberataque_%C3%A0_Vodafone_Portugal
[24] https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html

supported on the Vodafone network. Some of the ATMs, as they have an interconnection network to the mobile data network, were unavailable until around midnight, so:

- Shops could not sell their products online as the connections to the main banking operator were not working.
- Clients could not use the ATMs.
- Clients could not pay in shops with cards.

What measures were taken?

Emergency and health services were rerouted to other communication companies. The company had to stop all the systems and then had to go back to older communications systems. Then gradually it had to check and restart all the affected systems. This took about two weeks.

What is the result of the defence measures?

The services have not been attacked since the incident thanks to the new security measures implemented.

Mistakes and reaction:

This break in Vodafone happened due to the work of hackers that exploited a software vulnerability. People were very upset, and some started to panic, because they could not reach other people or emergency contact such as 911, some businesses lost a lot of money and people were afraid that the hackers had access to private information. However, the CEO of Vodafone guaranteed there was no access to private information. The company has since reinforced the security measures.

Case 2 – Phishing in retail store clients

Title	Phishing in retail store clients
Case source	Diário de Notícias[25]
Occurrence period	Occurred November 2019
Tags	Company
Status	The status of this case is closed.
Applicability Escape Room	Easily transferable to the Escape Room Model

What kind of attack was it?

Phishing attack on clients of a large retail store.

Weaknesses/Vulnerability:

The social engineering approach was very well done and took advantage of the unsuspecting customers.

What happened?

People received fake texts from someone pretending to be employees of the Continente retail store asking for personal information. Some people believed in the messages and gave their personal data to the hackers.

How has it been noticed?

People started seeing items being bought with their retail store card and account.

What measures were taken?

Clients were informed and warned about the attack. Affected clients were given new cards.

What is the result of the defence measures?

The information campaign prevented a large number of customers from being affected.

Mistakes and reaction:

The clients of the retail store (Continente) were victims of phishing, and they did not check the veracity of the information in the email messages.

[25] https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html

Case 3 – Data stolen from public entities

Title	Data stolen from public entities
Case source	RTP NOTICIAS[26]
Occurrence period	Occurred between May and December 2017
Tags	Companies, public institutions, private persons
Status	The status of this case is closed
Applicability Escape Room	The case might be transferred to the Escape room model because: • It's a relevant case to be explored, especially given its wide impact and the high profile of the victims (which could have led to serious consequences, and to the sharing of confidential information). • We have information on the technical aspects of the attack (the passwords were stolen through registrations on social media channels, and the data was published on two online lists - "Exploit.in" and "Anti Public" -, circulating on the dark web. • We can divide the narrative into different moments: from when the first warning sign was given, and the first data was shared (around 2016), and when the final lists were found, and the attack was made public.

What kind of attack was it?

Hackers exploited software vulnerabilities in public institution servers that were not maintained adequately from a cyber-security point of view.

Weaknesses/Vulnerability

Several major errors that can be highlighted in this situation are:

- professional and official email addresses were used by individuals for registration on social media channels and other platforms.
- no measures were taken after the event to protect the accounts revealed (e.g. by changing the exposed passwords).

What happened?

- According to the source, a document with 20.416 pages (with a total of almost 32,5 million passwords) was circulating on the Internet, revealing data belonging to employees and representatives from almost all areas of public administration, such as ministries, armed

[26] https://www.rtp.pt/noticias/pais/pj-confirma-ataque-informatico-milhares-de-passwords-roubadas_n1047761

forces, public security forces, tax authorities, and the national electoral commission.

- The victims were multiple and diverse: public entities, big companies, governmental bodies, public employees, and football teams.
- Moreover, passwords and emails from individuals working in private and public places, such as banks, hospitals, and media outlets, were also revealed. According to the information revealed at that time, the personal data of the users was already being stolen for years before it was published, and hackers had collected it through attacks on social media accounts, such as Facebook, LinkedIn, Twitter, and on storage platforms, such as Dropbox. This attack was known as the greatest cyber-attack ever registered in Portugal, and the biggest information theft ever recorded.

How has it been noticed?

On the 20th of December 2017, a Portuguese news magazine published an article revealing that thousands of emails and passwords had been stolen by a group of hackers.

What measures were taken?

- The criminal police promptly started an investigation into the attack. However, a representative of the security forces admitted that the information was not recent and was, in fact, known for a while (since 2016).
- No measures were taken after the event to protect the accounts revealed (e.g. by changing the exposed passwords).

What is the result of the defence measures?

In that sense and given that a lot of the revealed passwords were still active around a year after the data breach[27] it can be concluded that there is still a lack of knowledge about online security in several public and private Portuguese institutions.

[27] https://tictank.pt/2017/12/22/contexto-sobre-a-maior-fuga-de-informacao-pessoal-em-portugal

Case 4 – Denial of Service in a SME

Title	Denial of Service in a SME
Case source	Internal Source
Occurrence period	Occurred between January until February 2022
Tags	SME
Status	The status of this case is closed.
Applicability Escape Room	The case might be transferred to the Escape room model because it shows a simple problem that can affect most SMEs. The technical aspects of the case can be easily accessed.

What kind of attack was it?

Denial of service in a SME

Weaknesses/Vulnerability

The identified cause was a password attack that allowed to capture one staff email account that did not use an appropriate password generation scheme.

What happened?

- A password attack that captures one account. Hackers then used that account to generate bogus mail messages.
- Some email accounts and the email server were being used to spam some addresses and cause Denial of Service. The SME domain was also blacklisted in some services.

How has it been noticed?

The system administrator started receiving hundreds of warnings about messages not sent or sent to wrong addresses. Then the Internet Service Provider contacted, warning about the situation.

What measures were taken?

The internet provider that supports the SME closed up all access to the websites and online environments except the ones used for the administration. Passwords were changed and the files were cleaned. Better password definition schemes were adopted.

What is the result of the defence measures?

There has not been a repetition of the break-in although attacks are still frequent.

Case 5 – Code injection on websites

Title	Code injection on websites
Case source	Internal Source
Occurrence period	Occurred between October 2021 and March 2022
Tags	SME
Status	The status of this case is closed.
Applicability Escape Room	The case might be transferred to the Escape room model because it shows a simple problem that can affect most SMEs. The technical aspects of the case can be easily accessed.

What kind of attack was it?

Software exploit of some WordPress plugins. Code was injected in those files.

Weaknesses/Vulnerability

SME staff was not using appropriate measures to protect forms on the websites.

What happened?

Hackers used unprotected forms in the hosted websites to:

- Inject code in some pages to install trojans.
- Execute software.
- Generate log registers entries to fill up disk space.

How has it been noticed?

The ISP runs regular security checks on the servers that detected the injected code.

What (technical) measures were taken?

Files were cleaned and all the plugins were updated.

What is the result of the defence measures?

There has not been a repetition of the break-in although attacks are still frequent.

Case 6 – Data stolen from football club

Title	Data stolen from football club
Case source	All news media in Portugal
Occurrence period	Occurred between 2018 and 2019
Tags	Company
Status	On the courts
Applicability Escape Room	The case might not be transferred to the Escape room model because the technical aspects of the case are not easily accessed.

What kind of attack was it?

It is not clear if the cybercriminal got access through phishing or password attack.

Weaknesses/Vulnerability:

Lack of effective security measures in systems that were used by people with low digital skills.

What happened?

- Hackers got access to the emails of the board of a major football club in Portugal.
- An archive with several terabytes of email messages were then made available to a news channel that made them public. Some of the messages indicated corruption and bribery of diverse sport agents by the club officials.

How has it been noticed?

A public news channel received the database with the email messages and made them public.

What measures were taken?

The responsible hacker was identified and arrested. The case is currently on trial. The affected club hired a new solution for their messaging needs.

What is the result of the defence measures?

The club is no-longer dependent on in-house cyber-security technicians that were clearly not up to the challenge.

6 Conclusion

Most of the cases illustrated in this compendium affirm that the degree of protection in SMEs is not related to the continuously expanding digitalized innovation and progress. Weaknesses and vulnerabilities persist among staff members who often use end devices without due care and attention to cybersecurity. The lack of competencies and knowledge about cyber threats, as well as the extent of possible damage to the company or own personal, still exists.

The examples gathered in three European countries have revealed that the problems and challenges faced by European SMEs are comparable. This similarity allows to elaborate collaborative solutions to improve the existing state. In a general sense, it is important to highlight the risks and individual repercussions of unaltered, incautious, and heedless behaviours, and provide guidance on acting and reacting correctly. Given that small and medium-sized enterprises contribute to economic stability in all European nations, it becomes especially crucial to sensitize employees, and thereby contributing to Europe's resilience and digital security.

The nature and type of vulnerabilities are consistent and comparable across SMEs – encompassing phishing, social engineering, ransomware, and insecure passwords. A significant portion of these attacks can be attributed to human errors. Many companies applied similar approaches to counter the attacks and rectify the situation through the implementation of technical and organizational security measures.

Nevertheless, not all SME leaders consistently internalized the lessons learned. In several companies, leaders established preventive systems against cyberattacks and threats, and only a handful have chosen staff training as a subsequent security measure. This option appears to be less prioritized and less commonly pursued, so far.

The reactions and responses arising from cyberattacks in the showcased SMEs reveal a deficiency in understanding and recognition of the significance and value of education and training in this area. These results once again emphasize the pressing necessity to create and provide educational opportunities and programs aimed at mitigating competence gaps among non-technical personnel. Equipping companies and organizations with essential knowledge and skills is crucial for ensuring effective and secure business process operations.

This compendium has been published to support SMEs in dealing with relevant cyber security attacks. The EyesOnCS project itself wants to contribute to cyber security trainings of personnel in European SMEs and of vocational students.

7 References

- Abt, C., Serious Games (1987): University Press of America.

- Agrawal, S.; Simon, A.; Bech, S.; Bæntsen, K.; Forchhammer, S. (2020): Defining immersion. Literature review and implications for research on audiovisual experiences. J. Audio Eng. Soc., 68, 404–417.

- ACN Italy: National Cybersecurity Strategy 2022 – 2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf, seen 29.7.22.

- Bundesamt für Sicherheit in der Informationstechnik: Computer Emergency Response Team für Bundesbehörden (CERT-Bund), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html , seen 28.7.22.

- Cyber security intelligence: National Cyber Security Centre Portugal (CNCS), https://www.cybersecurityintelligence.com/national-cyber-security-centre-portugal-cncs-2730.html , seen 29.7.22.

- ENISA (2022): Consolidated Annual Activity Report 2021, Attiki, 2022.

- ENISA (2021): Cybersecurity for SMES- Challenges and Recommendations, European Union Agency for Cybersecurity (ENISA), Attiki, 2021.

- European Commission: The EU cybersecurity certification framework, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework , seen 29.7.22.

- EUR-Lex: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 32019R0881 - EN - EUR-Lex , seen 28.7.22.

- EyesOnCS Projektteam (2023): Cyber Alert Scenario_0x_nn, Preliminary report of the project team, to be published, FHM Düren, Düren, 2023.

- Guckian,. J., Sridhar, A. & Meggitt, S. J. (2020): Exploring the perspectives od dermatology undergraduades with an escape room game. Clinical and Experimental Dermatology, 45 (2), 153-158. https://doi.org/10.1111/ced.14039.

- Juzeleniene, S., Mikelioniene, J., Escudeiro, P., Vaz de Carvalho, C. (2014): GABALL project. serious games-based language learning. Procedia-Soc. Behav. Sci. 136, 350–354.

- Mac Gregor, M. (2018). Campus Clue: Habituating Students to the Information Search Process via Gaming. Pennsylvania Libraries: Research & Practice, 6 (2), 86-92. https://doi.org/10.5195/palrap.2018.172.

- Martina, Richard & Göksen, Sultan. (2020). Developing Educational Escape Rooms for Experiential Entrepreneurship Education. Entrepreneurship Education and Pedagogy. https://www.researchgate.net/publication/346548119_Developing_Educational_Escape_Rooms_for_Experiential_Entrepreneurship_Education , seen 10.1.23.

- Michael, D.R., Chen, S.L. (2006): Serious Games. Games That Educate, Train, and Inform. Thomson Course Technology PTR, Oshawa.

- N.N.: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/ , seen 28.7.22.

- N.N.: About ENISA - The European Union Agency for Cybersecurity, https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity, seen 28.7.22.

- N.N.: https://www.django-hurtig.com/jagdzentrum/jagd_vorgang_mainstream_id.php?id2=21727, seen 28.7.22.

- N.N.: https://www.dn.pt/sociedade/servicos-de-voz-movel-da-vodafone-registam-recuperacao-progressiva-14568590.html , seen 28.7.22.

- N.N.: https://www.dn.pt/dinheiro/fraude-marca-continente-alvo-de-phishing-11487091.html, seen 28.7.22.

- N.N.: https://www.rtp.pt/noticias/pais/pj-confirma-ataque-informatico-milhares-de-passwords-roubadas_n1047761, seen 28.7.22.

- N.N.: https://tictank.pt/2017/12/22/contexto-sobre-a-maior-fuga-de-informacao-pessoal-em-portugal/, seen 28.7.22.

- N.N.: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/, seen 28.7.22.

- N.N.: Deutschland sicher im Netz, https://www.sicher-im-netz.de, seen 28.7.22.

- Oblinger, D. (2006): Simulations, games, and learning. ELI White Paper, vol. 1, no. 1.http://net.educause.edu/ir/library/pdf/ELI3004.pdf.

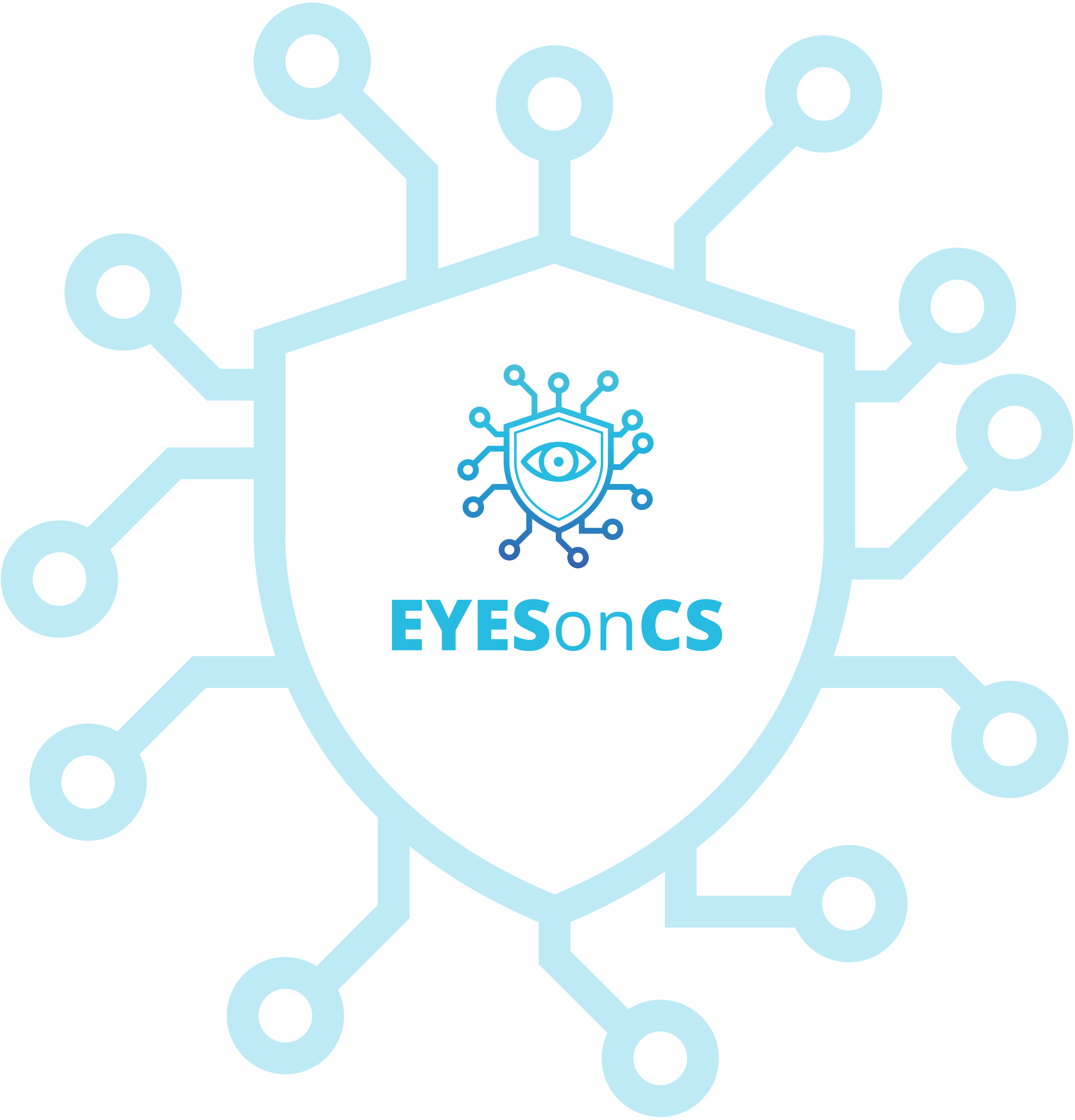
- Prensky, M.(2003): Digital Game-Based Learning. Comput. Entertain. (CIE) 1(1), 21.

- Streim, A., Mann, S. (2021): Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, bitkom, https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr, seen 2.3.23.

- Tercanli, H., Martina, R., Ferreira Dias, M., Reuter, J., Amorim, M., Madaleno, M., Magueta, D., Vieira, E., Veloso C., Figueiredo, C., Vitòria, A., Wakkee, I., Gomes, I., Meireles, G., Daubariene, A., Daunoriene, A., Mortensen, A., Zinovyeva, A., Rivera-Trigueros, I., Lòpez-Alcarria, A., Rodrigìguez-Dìaz, P., Olvera-Lobo, M.D., Ruiz-Padillo, D.P., And Guitièrrez-Pèrez, J. (2021), Educational escape rooms in practice: Research, experiences and recommendations. UA Editoria. https://doi .org/10.34624/rpxk-hc61.

- Zyda, M. (2005): From visual simulation to virtual reality to games. Computer 38(9), 25–32.

Notes



Stay tuned!

Follow us and learn more
about the project here:

www.eyesoncs.eu

Co-funded by
the European Union