Law of the internet safety and Industry 4.0

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Index

List of abbreviations

APT: Advanced Persistent Threats

CERT: Computer Emergency Response Team

CNCS: Centro Nacional de Cibersegurança

CSC: Cyber Security Center

CSIRT: Computer Security Incident Response Team

DDOS: Distributed Denial of Service

DSN: Digital Supply Network

EU: European Union

GDPR: General Data Protection Regulation

ICT: Information and Communication Technology

IDSA: Czech Institute of Informatics, Robotics and Cybernetics

IT: Information Technology

ÖSCS: Österreichischen Strategie für Cyber Sicherheit

NCBI: NarodniCentrumBezpecnejsiholInternetu

SIC: Safer Internet Center

SME: Small and Medium Enterprise

Figures

Key definitions

Advanced Persistent Threats: complex and target attacks on critical IT infrastructures of companies and public authorities.

Botnet: collection of internet-connected devices, which may include computers, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware.

Cybersecurity: the practice of protecting systems, networks and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing or destroying sensitive information, extorting money from users or interrupting normal business processes.

Data breaches: an intentional or unintentional release of secure or private/confidential information to an untrusted environment. Data breaches may involve personal health information, personally identifiable information, trade secrets and/or intellectual property.

Denial-of-service attack: a security event that occurs when an attacker prevents legitimate users from accessing specific computer systems, devices, services or other IT resources.

Internet safety: knowledge of maximizing the user's personal safety and security risks on private information and property associated with using the internet and the self-protection from computer crime in general.

Hoax/chain letter: a false report that is spread via e-mail, instant messenger, social networks or other means. Malicious hoaxes are intended to lure users into traps by sending additional promising links which, however, only cause viruses or malware or lead to fraudulent websites.

Malware: any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan and spyware. These malicious programs can perform a variety of different functions such as stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users computer activity without their permission.

Phishing: phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in an email or other communication channels. The attacker use phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.

Ransomware: malicious software that aims to block the access to archives and systems requiring payment of a value to return access.

Slander: false spoken statement about someone that damages their reputation.

Spam: electronic messaging systems to send out unrequested or unwanted messages in bulk. The most common form of spam is email spam but the term also applies to any message sent electronically that is unsolicited and bulk.

Trojan: type of malware that is often disguised as legitimate software. Trojan can be employed by cyber-thieves and hackers trying to gain access to users systems.

Virus: a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.

Warez: pirated software such as illegally copied, often after deactivation of anti-privacy measures that is distributed via the internet.

Worm: type of malicious software program whose primary function is to infect other

computers while remaining active on infected systems.

1. Introduction

Industry 4.0 will promote several changes either in businesses, because it will affect all levels of production and supply chains, including business and production managers, workers, cyber-physical systems, costumers among others as well as citizens in their private life.

Although the amount of benefits that arise with Industry 4.0 the information and assets owned or used by the organizations and people become more and more important. Because of this, with the new industrial revolution the existence of attacks increases exponentially and also brings new risks that must be considered and addressed both for organizations as well as in the overall society. Therefore cybersecurity should become an integral part of the strategy, design and operations and the implementation of measures is very important from now on. There are plenty of measures/practices to implement in companies and in citizens private life in order to improve the security and the safety to gather, protect and provide information. In addition, although there are some initiatives and institutions involved in the internet safety there are still much work to do specially because the world nowadays is extremely dynamic and, as a consequence, new threats are always emerging, new vulnerabilities are discovered and the lack of development/training of workers is a key challenge.

The new era of digitization is bringing the increasing use of digital technologies in even more areas of business and society and the growing connectivity of everything. This situation is, as well, responsible for significant socio-cultural, economic, greater challenges and threats on the level of security and some policy changes in the European territory. Having this in mind, it is absolutely necessary to make society more aware and more prepared for this reality and include some strategies at a national level to help to achieve a safer community in a daily basis globally.

In this report we have a brief overview of the main challenges that people face everyday in some of European country, the main risks/difficulties that people are facing everyday, the most common incidents regarding cybersecurity and we safety.

2. Industry 4.0: a brief overview

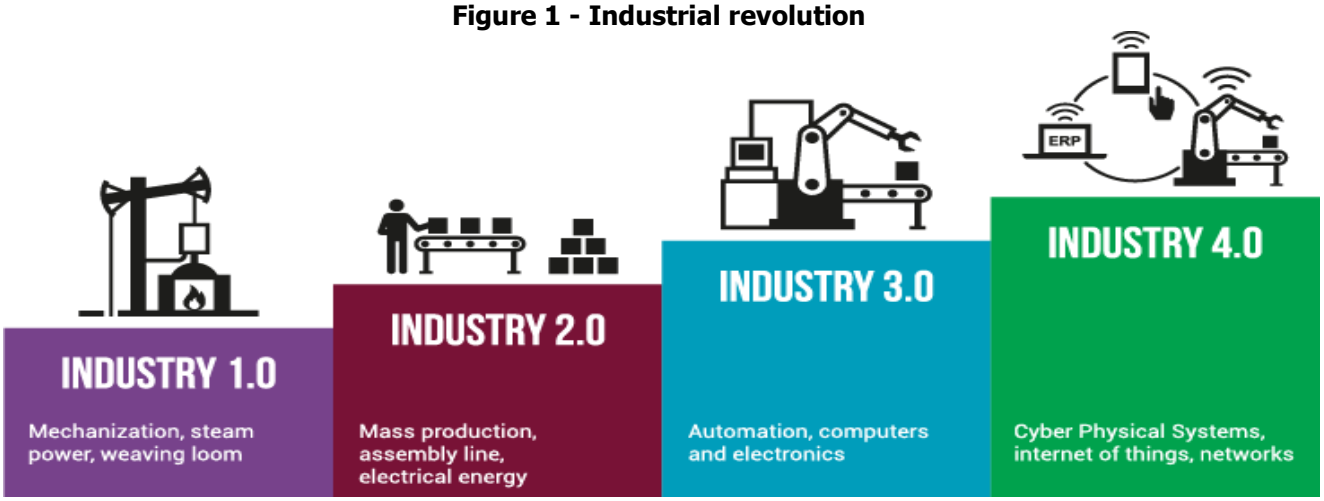
The forth industrial revolution, commonly referred to as Industry 4.0, is characterized by the decentralized intelligence which helps to create intelligent object networking and independent process management, with the interaction of the real and virtual worlds representing a crucial new aspect of the manufacturing and production processes.

Indeed, the industrialization of the world began in the late 18th century with the first industrial revolution and it was defined by the introduction of mechanical production facilities with the help of water and steam power.

The forth industrial revolution is characterized by the digital transformation with the development of cyber-physical technologies that allow disruptive changes in production and business models.

The Industry 4.0 is a natural outgrowth of the third industrial revolution which fully transformed the nature of commerce in the second half of the 20th century with an array of computerization and Information Technology (IT) advances. It was a period of big changes for retail and consumer goods companies, marked by the emergence of credit cards, back-office and warehouse automation, just-in-time supply chains and the first online business models. As a matter of fact, the concept of Industry 4.0 is relatively recent and has grown in importance during the last few years within the different companies.

Figure 1 - Industrial revolution



Source: (Simio, n.d.)

Industry 4.0 is a combination of several technological advancements:

- **Information and Communication Technology:** Digitalization and the widespread application of Information and Communication Technology (ICT) allow the integration of all systems throughout the supply and value chains and enables data aggregation on all levels. Information is digitized and the corresponding systems inside and across companies are integrated at all stages of both product creation and use lifecycles;

- **Cyber-physical systems:** Cyber-physical systems improve the capability of controlling and monitoring physical processes, with the help of sensors, intelligent robots, drones, 3D printing devices (some of which will be more detailed further into this report). In cyber-physical systems the physical components are aggregated into a network of interacting elements. While the initial inputs and final outputs are customarily physical, information often transposes between physical and digital states during manufacturing process;

- **Network communication:** All these devices, both within the manufacturing plant and across suppliers and distributors, are connected through different wireless and Internet technologies. Reliable high-quality communication networks are a crucial requirement Industry 4.0 and therefore it is important to expand the broadband Internet infrastructure where needed. This high level of networking of interconnected components allows for a decentralized and self-organized operating of the cyber-physical systems;

- **Big data and cloud computing:** With the use of big data and cloud computing, the information retrieved through these networks can be used to model, virtualize and simulate products and manufacturing processes;

- **Modelling, virtualization and simulation:** Simulation is a core functionality of systems by means of seamless assistance along the entire life cycle, for example, by supporting operation and service with direct linkage to operation data;

- **Improved tools for human-computer interaction and cooperation:** To control these processes, human workforce is supplied with state-of-the-art ICT tools that make use of advancements in augmented reality and intelligent robotics. The cyber-physical systems of Industry 4.0 have the primary aim of assisting humans in their everyday jobs. The key features of such systems are non-intrusiveness, context-adaptiveness, personalized, location-based and mobility.

In addition, it is important to be aware that there are also some important challenges associated with Industry 4.0 and internet safety. The two main important challenges are:

- **Security:** Perhaps the most challenging aspect of implementing Industry 4.0 techniques is the IT security risk. This online integration will give space to **security breaches, data leaks** and might even involve **cyber theft**. As data is collected throughout the supply chain questions of ownership will arise and it is important for companies to make sure that their data won't end up in the hands of a competitor. On the other hand, it must be ensured that the production facilities themselves do not pose a threat to humans or the surrounding environment and that the workers receive continuous safety trainings;

- **Privacy:** This issue concerns not only the customers but also the producers. In one hand, the customer needs to collect and analyze data which is relevant for the development of his business. On the other hand, the costumer might feel that his privacy is being threatened. Also, small and large companies who haven't shared their data in the past will have to work their way to a more transparent environment. Bridging the gap between the consumer and the producer will be a huge challenge for both parties.

2.1. To what extent have Industry 4.0 been adapted to the challenges created by internet safety in your country?

2.1.1. Austria

The concept of Industry 4.0 drives the networking of machines via the Internet and thus opens up previously closed systems to new dangers such as cyber-attacks or malwares. The protection of IT systems requires a comprehensive security concept and strategic information security management.

The association "Platform Industry 4.0" is aware of the importance of the safety aspect in connection with Industry 4.0 and has newly identified the focus "Security and Safety" in the strategy meeting 2017.

With the establishment of the expert group Security and Safety the platform Industry 4.0 Austria wants to increase the perception of the importance and significance of the topic Security for Industry 4.0, network relevant actors in Austria and contribute to establish Security & Safety as an Austrian competitive advantage. Interested members and experts from research and industry will be offered a forum for the exchange of experience and the opportunity to develop a common understanding of security in relation to digitization. As first joint projects the creation of an Austria-wide security competence catalogue of science, private research institutions and companies as well as an "industrial security" guideline for companies is planned, with the aim to sensitize especially Small and Medium Enterprises (SMEs) to the topic to point out critical points in the area of security and safety in business decisions and to offer first assistance.

The implementation of Industry 4.0 is not possible without guaranteeing data and software security. Therefore, it is necessary to use existing international safety standards, which allow professional testing of systems and software used, in addition to the further development of safety systems relevant for industry 4.0. IT-Security in Industry 4.0 gets a special meaning with the intensive use of the Internet also for automation control functions, virtualization and cloud computing, through SelfX technologies (self-configuration, self-healing, self-optimization) and the agent-based networking of intelligent functions between each other.

The standard family ISO/IEC 27000ff (developed in ISO/IEC JTC 1/SC 27, IT Security techniques) offers in addition to a generic management system for information security, a variety of generally accepted and field-tested tools and topic-specific solutions such as

ISO/IEC 27036-4 for security in cloud services.

The IEC 62443 standard "*Industrial communication networks - Network and system security*" developed in IEC /TC 65, Industrial-process measurement, control and automation, is based on the ISO/IEC 27000 standard family (Verein Industrie 4.0 Österreich, 2016).

Therefore, we can confirm that in Austria there are multiple initiatives that aims to improve the challenges imposed by Industry 4.0. and internet safety.

2.1.2. Czech Republic

In the case of Czech Republic the Industry 4.0 will move the core business of most companies into the digital world. The main challenges identified in companies in Czech Republic are as follows:

- **IT security and reliability of key systems:** in a company that is managed by machines, it will be essential that data from individual sensors inside the machines is truly authentic. Furthermore, it is important that the setup of the network is not compromised. Companies become dependent on their ICT infrastructure;
- **Business process integrity:** pressure on the lowest price and the shortest time to implement project changes within Industry 4.0 can lead to a negative effect. Incorrect process settings can be essential in production and delivery. These problems can lead to a financial loss or even an existential problems of the company;
- **Sensitivity to software flaws:** in many businesses, the production process is largely software-dependent, but there is still participation by people who are involved in the operation of equipment. In addition, machines or lines usually operate autonomously (not linked to the global system). In the future, the machines will be managed by central software, which will depend on the functioning of operating systems, firewalls, IDS / IPS protection, management tools, and so on.

2.1.3. Portugal

In Portugal there are some initiatives in the last few years in order to promote the Industry 4.0 in companies. In this context, the national government in Portugal has a program called "i4.0" that aims to promote the national reindustrialization. This strategy has more than 50

public and private measures and the statistics said that these measures will have an impact in more than 50.000 companies that operate in Portugal and, in an initial phase, will allow the requalification and also the development of digital competences of more than 20.00 workers.

In addition, the main challenges of the Portuguese companies regarding the adaptation to the Industry 4.0 and the internet safety are:

- **The lack of digital competences and the requalification of human resources** and these factors are contributing to the delay of the development of digital transformation, the development of digital maturity and can promote some security risks;
- The **lack of human resources capable to plane, execute and guarantee the implementation and maintenance of Industry 4.0 solutions**. To solve this situation managers of the enterprises can develop partnerships with external organizations, secondary or technical schools and universities;
- The **lack of capabilities and competences to detect security failures** and how to solve them. Regarding to this topic, the majority of the companies recognize that they need to implement security measures/plans because with this they will promote a digital transformation process;
- The **reconversion of old systems to the technologies of Industry 4.0 can bring some security risks** because the old systems are not designed to have such a high level of connectivity. This means that in order to managing the security risks, the companies need to guarantee the protection of their systems they have to be aware to avoid new threats they have to be resilient to limit some damages and to restart their operations. Therefore, when companies are stablishing a strategy for Industry 4.0 all the themes related to security must be in the top of the priorities.

2.1.4. Spain

In the case of Spain, the creation of an environment of digital trust that allows reinforcement of the protection of institutions and promotes the implication of citizens in the

digital environment is vital for the development of a connected society. In order to achieve this cybersecurity industry must act as the key enabling element.

In connection with this, the Spanish Digital Agency, focused on the aforementioned goal and, in particular, by means of the Digital Trust Plan, is studying the possibility of carrying out a feasibility study in collaboration with the main reference agents and with the National Forum for Digital Trust with the purpose of developing an integration proposal to start up a Cybersecurity Industry.

After the implementation of the GDPR the goal is none other than to guarantee a safer environment for personal data and information. However, this process has been a challenge for companies. The new standard introduces tools such as the right to be forgotten, the obligation to inform in a concise, intelligible and simple language or the fact of facilitating the data portability to another company assigned without any obstacles. In particular, technological development is associated with a greater exposure to new threats, particularly those associated with cyberspace. The hyper connectivity of today's world exacerbates some of the security system's vulnerabilities and requires greater protection of networks and systems, as well as the public's privacy and digital rights. Spain must adapt to this permanent transformation by stepping up its efforts to digitalize and technify the State and society, based on an educational and training system adapted to this new reality.

In order to adapt to the change required by the new European Data Protection Regulation, it has been necessary to draw up a plan developed within a National Cybersecurity Strategy that has involved an enormous change in relations between companies, citizens and public institutions in order to promote the society's development. This has been possible through the creation of:

- **Cybersecurity Strategic Plan:** The main objective of this strategic plan of the Spanish Government focuses on ensuring a safe use of information systems and networks through a system of prevention, analysis, recovery and detection of any cyberattack in the field of New Technologies. In this way, national legislation is complied with the regulations established within the framework of international law in accordance with the commitments made by Spain. On the other hand, the challenges

of achieving a global, complete and flexible response are focused on the risks and threats identified.

- **Safety regulations and standards:** As defined from Europe, data protection will be regulated and compulsory from 25 May 2018. It establishes the implementation of new security measures for freelancers, companies and the Public Administration. These measures include the implementation of encryption and double-factor basic authentication systems if the level of risk requires it. In this sense, it is crucial to adapt to the LOPD and to know the LSSICE content, as well as to assist a data protection consultancy to verify how the computer security measures are implemented and to know what level of security and protection you must guarantee against any attack.

- **General Data Protection Regulations:** The New Technologies right represents a great advance in terms of documentation, but we should understand that we are living a new conceptual and legal reality. On the other hand, by means of computer attacks it must be considered that a huge amount of confidential information can be stolen on a daily basis. Companies have implemented preventive and protective tools to keep any intruder away from accessing their information. In summary, General Data Protection Regulations state that companies must report attempted intrusions and successful unauthorized access, as well as affected data. These cybersecurity measures guarantee a greater control and protection of private information.
    - Some technological/systemic/organizational challenges are:
        - **Improvement of cybersecurity capabilities** of governments, public agencies, organizations, universities, etc., in order to move up to reach the state of the art in Industrial Cybersecurity;
        - **Raise general awareness and provide specialized training** suitable to every type of user;
        - **Development of tools to facilitate public-private partnerships** at all levels;

- Increase research on Industrial Cybersecurity;
- **Development of cybersecurity strategies** for the industry;
- **Development of best practice guidelines** and reference standards;
- **Foundation of testing laboratories**;
- **Development of evaluation schemes**;
- **Development of ICS-CERTs**;
- **Support for the development of regulatory frameworks**;
- **Development of systems that include cybersecurity** from design;
- **Development of a cybersecurity culture** within the pillars of traditional industrial safety.
- **Approach and training** of those persons in charge of control systems in ICT security systems and vice versa;
- **Improvement of legislative compliance**;
- **Dissemination of products and solutions** in industrial cybersecurity among all stakeholders.

2.2. How has been the adaptation for the companies and the overall society regarding cybersecurity?

2.2.1. Austria

In the second quarter of 2015, PwC and Strategy& jointly published the study "Industry 4.0 - Austria's industry in change". In this study, Austria-wide 100 companies from five industries (automotive suppliers, electrical engineering and electronics, mechanical and plant engineering and the process industry) were questioned. For a successful, timely implementation of Industry 4.0 concepts, companies still must master numerous challenges. For one third of the respondents, the focus is on high investments and an often-unclear profitability calculation as well as missing standards and norms for new Industry 4.0 applications. Many companies have not yet drawn up concrete implementation plans for Industry 4.0 solutions or approved investments because the solutions are new for many companies, require considerable changes and the potential is difficult to quantify. There is

an acute need for more transparency and a cross-industry exchange of experience. International standardization in the area of Industry 4.0 applications must also be promoted and this is the only way to intensify cooperation between companies and increase efficiency in the future. The main challenges are:

- **Inadequate qualification of employees;**
- **Data protection;**
- **Data security.**

Digital change will change the demands placed on employees at all stages of the value chain from development to production to sales and the increasing digitization will make processes and business models more agile and data driven. This demands completely new skills and qualifications from employees. The demand for software developers and data analysts in industry will also increase significantly over the next five to ten years (Busch et al., 2015).
The adaptation of companies and the overall society regarding cybersecurity is already in progress, but further adaptations and commitment are needed not only from public authorities, but also from individual companies and each individual living in this society. Various initiatives, such as the Platform Industry 4.0 association and the Information Security Commission are helping in this regard by providing advice. As the digital possibilities continue to evolve and change, there is also a need for continuous development in terms of security.

2.2.2. Czech Republic

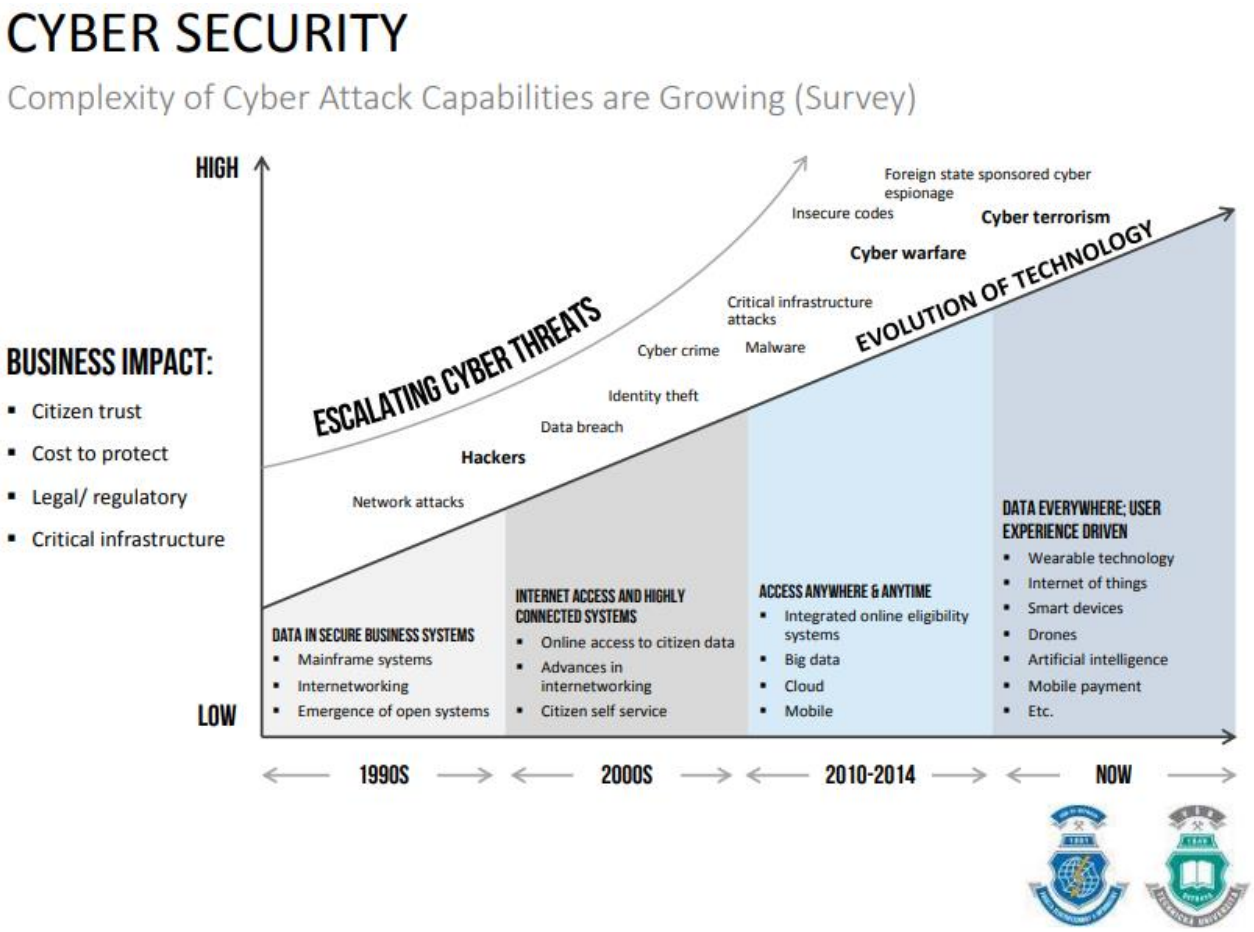
Regarding the adaptation of companies and the overall society regarding cybersecurity there are some business impact which affect the companies for example:

- **Citizen trust;**
- **Cost to protect;**
- **Legal/regulatory impact;**
- **Critical infrastructure.**

The Faculty of Electrical Engineering and Computer Science of VŠB-TUO in Czech Republic

analyzed escalating cyber threats during evolution of technology since 1990-2018 and it was found the complexity of cyber-attack capabilities are growing. In the next figure we can see the results of these threats.

Figure 2 - Threats in cyberspace



Source: (VŠB-TUO, n.d.)

As we can see in the figure above the number of cybersecurity issues are increasing since 1990. With the evolution of technology the cyber threats are escalating and after 2010-2014 the main critical cyber threats are:

- **Malware;**
- **Critical infrastructure attacks;**
- **Cyber warfare;**
- **Insecure codes**;
- **Cyber terrorism;**

- **Foreign state sponsored cyber espionage**.

2.2.3. Portugal

The fast digital transformation brings one a new problematic related to cybersecurity.

The Centro Nacional de Cibersegurança (CNCS) aims to assure a secure national cyberspace and works in different phases, specially the reaction phase which means, when something goes wrong and is the formal entity responsible for the national cybersecurity. In addition, CNCS will create an instrument called "**Modelos de Maturidade para a Cibersegurança**" that will bring a set of measures and controls to applicate and will define some priorities in order to grow in the maturity of cybersecurity. This instrument will be divided into four documents: 1) how to react to incidents; 2) how to prevent incidents; 3) how to detect incidents; and, 4) management of security information. This instrument will be available in 2019 and will also include some good practices that will be certainly very helpful.

CNCS have a very active role when it comes to this subject also and in February 2019 launched a free online course that aims to increase knowledge and literacy in the area of security, addressing topics such as software update, use of pen drives and passwords, use in personal and professional context.

Also, CNCS is working with **cooperation programs national and internationally**. Actually, in this area, Portugal has one of the biggest cooperation networks to react to cybersecurity incidents in Europe and this center was only created in 2014.

The majority of cybersecurity events come from:

- **Internal incidents because sometimes workers have, without any bad intention, some behavior or attitude that can lead to some incidents**. Because of this, providing training activities to all the workers is crucial in order to avoid some of the incidents that can happen. In addition, although the investments in training are fundamental the digital infrastructures, such as software and hardware can't be forgotten because they result in more informatics system security;
- **Phishing attack.** Portuguese invest little in cybersecurity and they are, therefore, more vulnerable to attacks. This happens because the majority of companies still prefer to deal with things internally because they consider that this area is not yet a

priority. This can be explained by the fact that the majority of Portuguese companies are SMEs;

- **Outdated technology and cybersecurity** are two aspects that every manager considers that block the progression of their businesses. In addition, Portuguese organizations confirm that cybersecurity is acting as a brake on productivity with almost half of the technological and entrepreneur's leaders consider that cybersecurity has a bad impact;
- **Authentication security procedures are complex or consume more time**, when they to perform an urgent task or with a particularly tight deadline, they may feel encouraged to take non-compliant paths and follow "shortcuts";
- **Lack of digital competences and capabilities it is still a big issue** although there are more information and initiatives online and offline carried out by public and private institutions that aims to promote a more secure behavior and attitude. Nevertheless, especially the younger generation is becoming more comfortable and has more knowledge to deal with cybersecurity problems.

Because of these, companies **should adopt some clear security strategies that give security to clients** and they should have some resolutions plans when it comes to a cybersecurity crisis.

To conclude we can say that Portugal has some initiatives related to cybersecurity carried out in the last few years and there are also some initiatives that aim to promote a much safer behavior and attitude by the overall society. However, there is still much to do in order to have a better secure environment both in companies and in citizen's private life.

2.2.4. Spain

Cybersecurity projects in Spain aim at increasing the security of current applications, services and infrastructures and supporting the creation of leading markets in Europe, always with an end-user approach and including all competent bodies regarding compliance, critical infrastructure operators, ICT service suppliers, ICT distributors, market players and

citizens. All of these require strengthening capacities to deal with threats from cyberspace. Thus, it should be convenience to:

- **Reinforce the capacity to investigate and prosecute cybercrime**, to guarantee citizen security and the protection of rights and freedoms in cyberspace;
- **Promote the cybersecurity of citizens and companies**;
- **Foster the Spanish cybersecurity industry**, ensuring the generation and retention of talent personal, in order to strengthen digital autonomy;
- **Contribute and promote an open, plural, secure and reliable cyberspace**, supporting the national interests;
- **Develop a culture of cybersecurity**.

3. Internet safety and Industry 4.0: in companies

Industry 4.0 technologies are expected to prompt a further evolution in the traditional linear supply chain structure by introducing intelligent, connected platforms and devices across the ecosystem, resulting in a digital supply network (DSN) across the value chain to inform each other. The result may be better management and flow of materials and goods, more efficient use of resources and supplies that more appropriately meet customer needs. Although all the benefits that came with these the increasing interconnectedness of the DSN also brings with it cyber weaknesses that should be properly planned and accounted for in every stage, from design through operation to prevent significant risks.

But a responsive, agile network of this nature is made possible only by open data sharing from all participants in the supply network which creates significant problems and can lead to some difficulties between allowing transparency for some data and maintaining the information.

Therefore, organizations may thus want to consider ways to **secure that information to prevent unauthorized users** from accessing it across the network especially when it comes to supporting processes such as information sharing and system access.

The main important factor to be careful is trust. Organizations may need to **keep evolving their risk management to preserve integrity** and remain secure when transacting information or goods, as well as strengthening their monitoring capabilities and cybersecurity operations to remain vigilant and protecting processes that cannot be validated.

3.1. Which accidents concerning the internet safety were solved in your country in the recent years in companies?

3.1.1. Austria

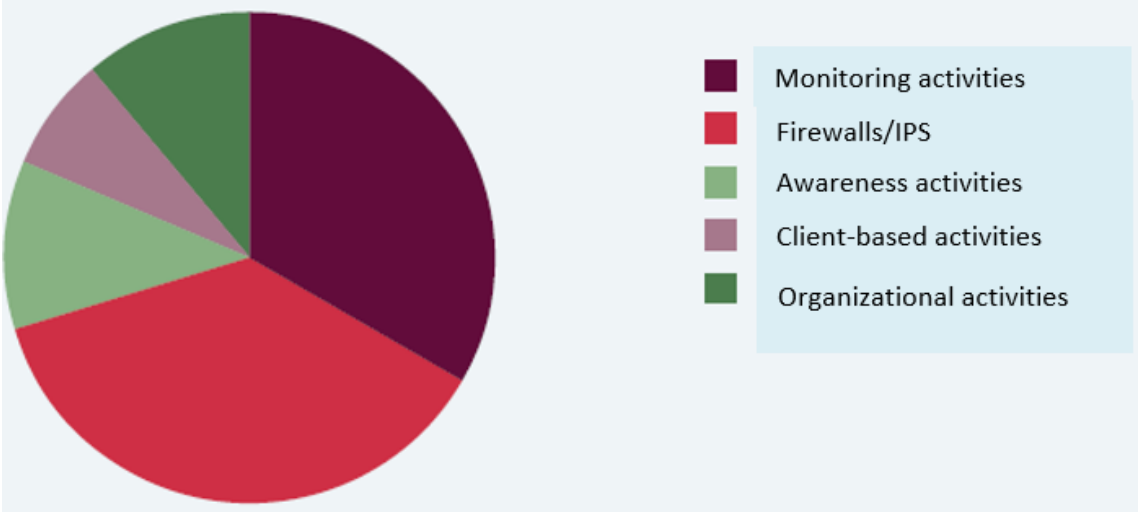
In Austria there are some examples of accidents concerning the internet safety like, for example, Advanced Persistent Threats (APT). In October 2018, Austria became a victim of such an attack, with the aim of endangering the security of the IT systems of public

authorities and institutions and stealing data on a large scale. The attackers used a variety of channels to attempt to infect victims with malware in order to compromise user data, with the ultimate goal of infiltrating computer networks and stealing confidential data.

The precautions taken by the attacked institutions and the good cooperation between GovCERT and Cyber Security Center (CSC) made it possible to fend off the attacks of all those affected and to prevent the outflow of data. The fact that the effects have remained minimal despite the effort of the attackers is a further sign of the effectiveness and importance of continuous cooperation between all relevant bodies at the national level (Cyber Sicherheit Steuerungsgruppe, 2019).

In the next figure, we have an overview of the security measures introduced.

Figure 3 - Measures taken (2018)

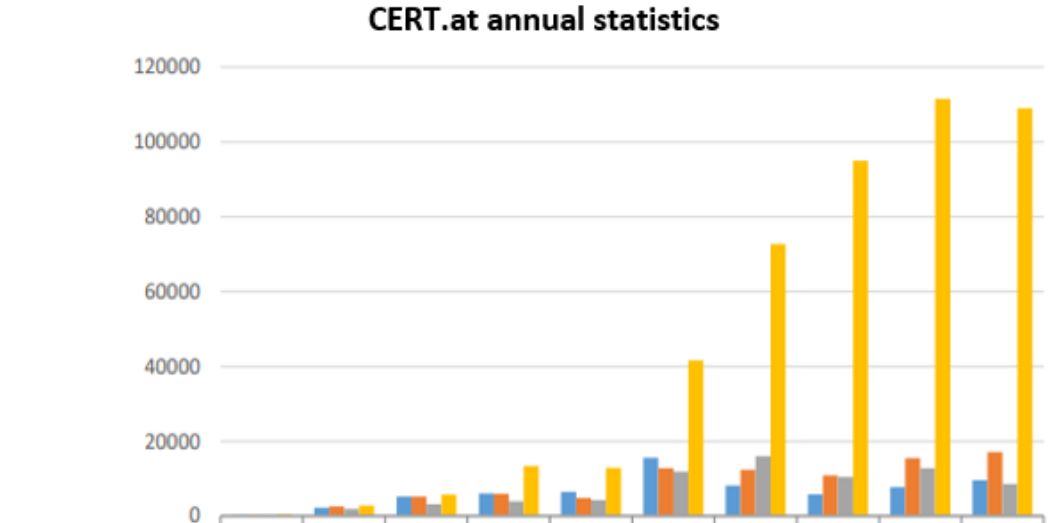


Source: (Cyber Sicherheit Steuerungsgruppe, 2019)

While technical progress in the areas of firewalls/IPS and endpoint protection has undoubtedly led to upgrades in defense measures, last year's trend is also continuing here: instead of focusing purely on isolation, more and more organisations are tending towards **monitoring measures to detect attackers in their own networks**. This also includes the **active search for current threats for the respective organization** and, in a second step, the targeted checking of systems for infections. In addition, preparatory measures were taken in many places to be able to analyze security incidents using forensic

methods (Cyber Sicherheit Steuerungsgruppe, 2019).

Figure 4 - CERT.at annual statistics with overview of reports, incidents and investigations over time



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
False alarms	187	2227	5209	6006	6460	15592	8178	5740	7701	9537
Relevant reports	210	2593	5190	5938	4878	12755	12346	10884	15499	17055
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809	8556
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550	109003

Source: (Nic.at GmbH, 2018)

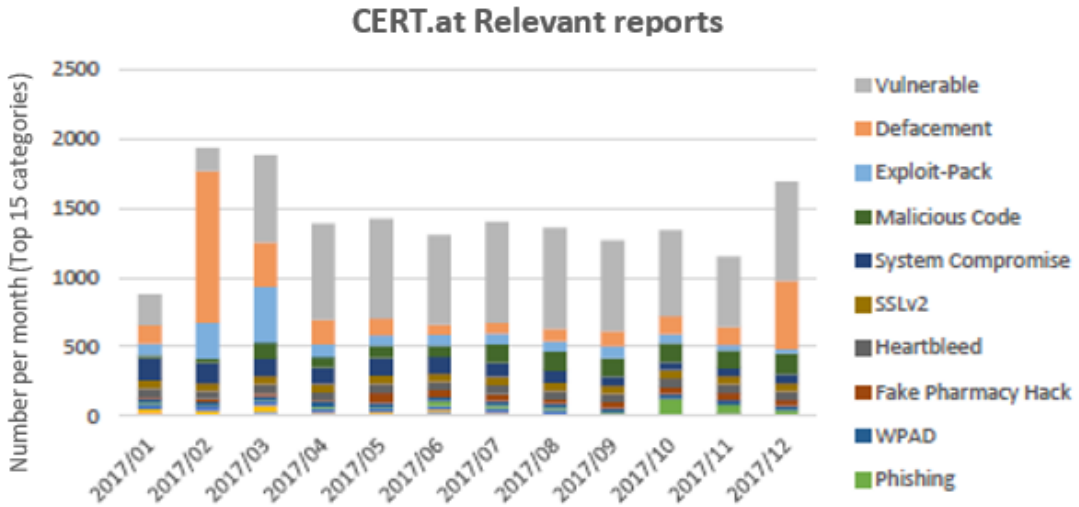
Since 2008, the Computer Emergency Response Team (CERT).at team has been leading overall annual statistics. These include the number of relevant reports, incidents and investigations as well as false alarms. Since 2008 until 2017 CERT.at is working to continuously improve cybersecurity in Austria. In figure 4, we can see that the number of reports, incidents and investigation over time and we can confirm that the number of relevant reports is significantly bigger than the rest of the categories. The explanation for each one of the following categories are described bellow.

"Relevant reports" refer to incoming reports to CERT.at not all of them describe a situation that CERT.at classifies as a relevant incident and requires active treatment.

"Incidents" are those cases that actually represent a security risk. In these cases CERT.at becomes active and informs affected companies, organizations or private users, for example, about IT security threats and, in special cases, supports them in solving problems.

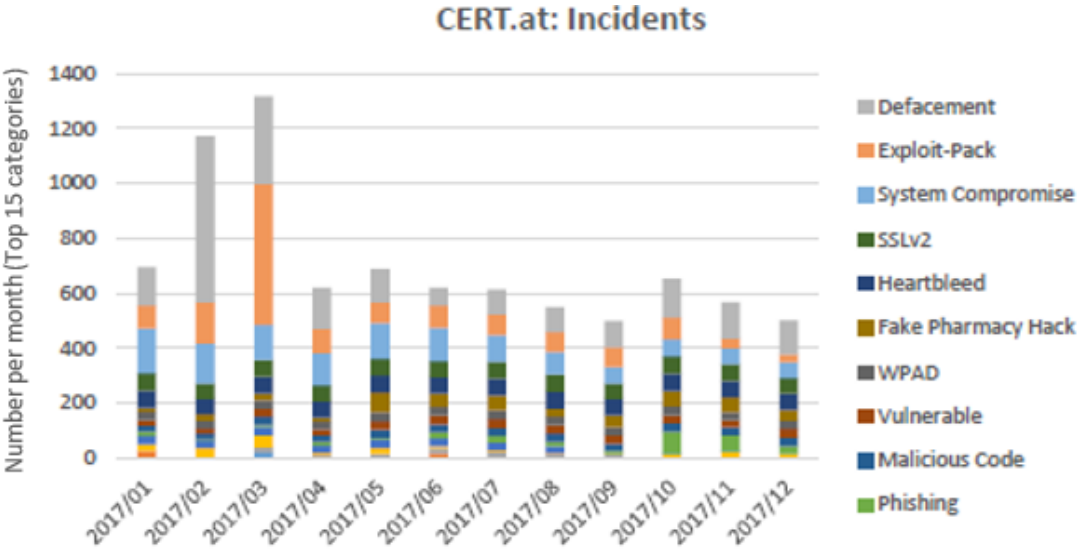
In the CERT.at ticket system, contacting the affected companies, organisations or private users is referred to as "Investigation". An investigation is usually an e-mail to the network operator, web host or domain owner. In figure 5, 6 and 7 we have an overview of the most common incidents that happen in 2017 by category.

Figure 5 - Classification of relevant reports by threat type over time (2017)



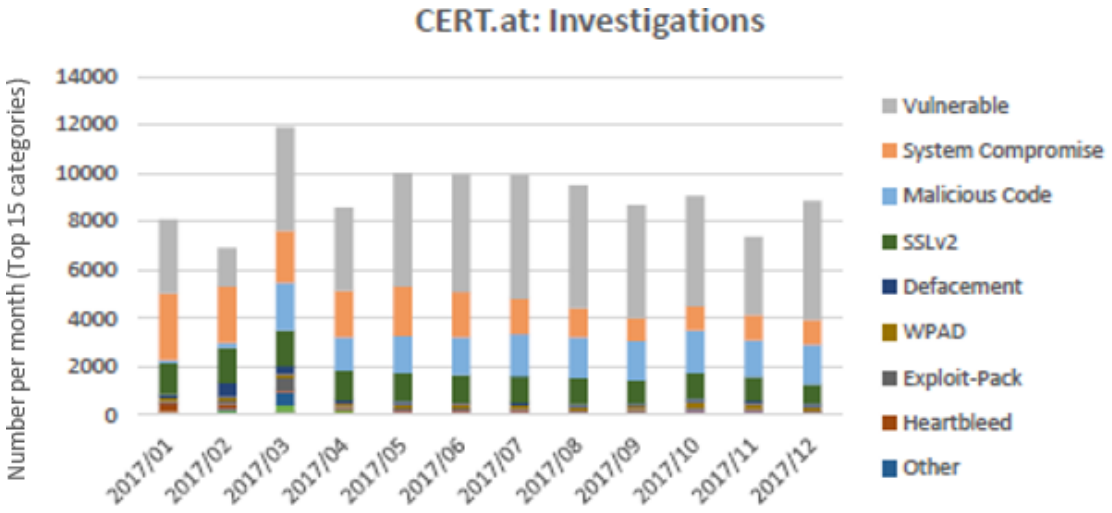
Source: (Nic.at GmbH, 2018)

Figure 6 - Classification of incidents according to threat types over time (2017)



Source: (Nic.at GmbH, 2018)

Figure 7 - Classification of the investigations conducted by CERT.at according to threat forms over time (2017)



Source: (Nic.at GmbH, 2018)

3.1.2. Czech Republic

From national analysis of cases of Internet crime in Czech Republic revealed that the most prominent manifestations of cybercrimes include:

- **Swindling and embezzlement;**
- **Forgery;**
- **Defamation;**
- **Electronic vengeance;**
- **Hoaxes;**
- **Warez;**
- **System penetrations;**
- **Computer bank robbery (phishing, pharming, IP spoofing).**

Cybercriminals have shifted again and their methods are more sophisticated than before and many companies and institutions are not prepared for the current modern electronic attacks. The Czech Republic Police have been monitoring the development of crimes committed in cyberspace (primarily within the Internet) since 2011. Cases of cybercrime have been steadily increasing since then (out of about 1500 crimes in 2011 to more than 5650 crimes in 2017) growth has slowed in recent years. CRIS.CZ incidents in 2017 show that the

biggest threats are:

- **Phishing;**
- **Malware;**
- **Spam;**
- **Trojan.**

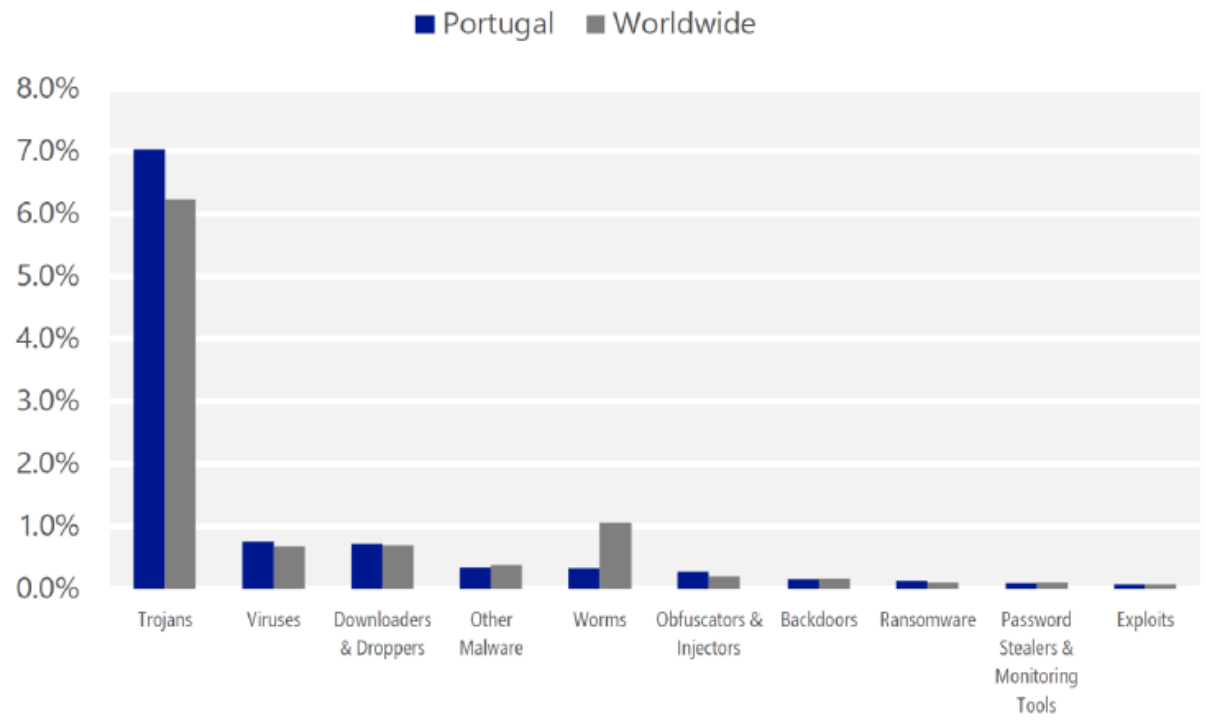
The most common attack is phishing through obtaining sensitive information such as credit card numbers or perhaps accounts passwords. However, fake e-mails from company directors are also common with the command to transfer a certain amount of money to a certain account.

3.1.3. Portugal

In Portugal, the most common attacks are:

- **Phishing attacks** that are, generally, followed by SPAM messages send to multiple users. While there may be phishing types that request the data directly in response to the email, they are most often articulated with a website where you fill in your data. In 2018 Portugal was the second country in the world with more phishing attacks according to the study "Spam and Phishing in 2018" carried out by Kaspersky Lab about online security;
- **Cybersecurity breaches (data stolen);**
- **"Ransomware" attacks** declined in Portugal in 2018 and phishing remains the favourite attack method. Also, Portugal is still slightly bellow the international average in detecting cybersecurity breaches, except for the identification of crypto-coin mining episodes.;
- **Malware and Trojans.** According to a report carried out by Gabinete de Estratégia e Estudos, Portugal is one of the countries that has one of the highest malware incidents rates and this is the malicious software more common in Portugal along with Trojans (see figure 8).

Figure 8 - Malicious software incident rate (march 2017)



Source: Microsoft (2018)

- **Cloud threat intelligence ("cloud" threat)** is one of the most recent threats to information security at the moment because the use of cloud is nowadays used by the majority of the companies and, with that, making it a growing target for attacks. When hackers enter in the cloud of the organizations through access credentials stolen from a user, largely due to the use of weak passwords followed by targeted phishing attacks and violations of third-party services. According to Microsoft (2017), attacks on cloud user accounts increased 300% in the first quarter of 2017 compared to the first quarter of 2016.

According to the results of the same study, Portugal is the 8th country with the biggest cybercrime vulnerability score and one of the countries with the biggest cybercrime victims in the EU (3th position).

Figure 9 - Cybercrime vulnerability score

EU COUNTRY	CYBERCRIME VULNERABILITY SCORE				
1. MALTA (MOST VULNERABLE)	42%	11. SLOVENIA	38%	21. SWEDEN	32%
2. GREECE	41%	12. CROATIA	37%	22. ITALY	31%
3. ROMANIA	41%	13. DENMARK	36%	23. FRANCE	31%
4. SLOVAKIA	40%	14. LATVIA	35%	24. UK	31%
5. SPAIN	40%	15. CZECH REP	35%	25. NETHERLANDS	30%
6. LITHUANIA	39%	16. POLAND	34%	26. GERMANY	30%
7. CYPRUS	39%	17. IRELAND	33%	27. ESTONIA	30%
8. PORTUGAL	39%	18. LUXEMBOURG	32%	28. FINLAND (LEAST VULNERABLE)	29%
9. HUNGARY	39%	19. AUSTRIA	32%		
10. BULGARIA	38%	20. BELGIUM	32%		

Source: Website Builder Expert (2017)

Figure 10 - Cybercrime victimhood rating

Biggest Cybercrime victims in the EU

	% OF POPULATION WHO HAVE EXPERIENCED CYBERCRIME	ANNUAL AVERAGE MALWARE ENCOUNTER RATE	CYBERCRIME VICTIMHOOD RATING
1. ROMANIA	18%	28%	23%
2. NETHERLANDS	27%	14%	21%
3. PORTUGAL	15%	24%	20%
4. POLAND	16%	23%	20%
5. ITALY	17%	21%	19%

Source: Website Builder Expert (2017)

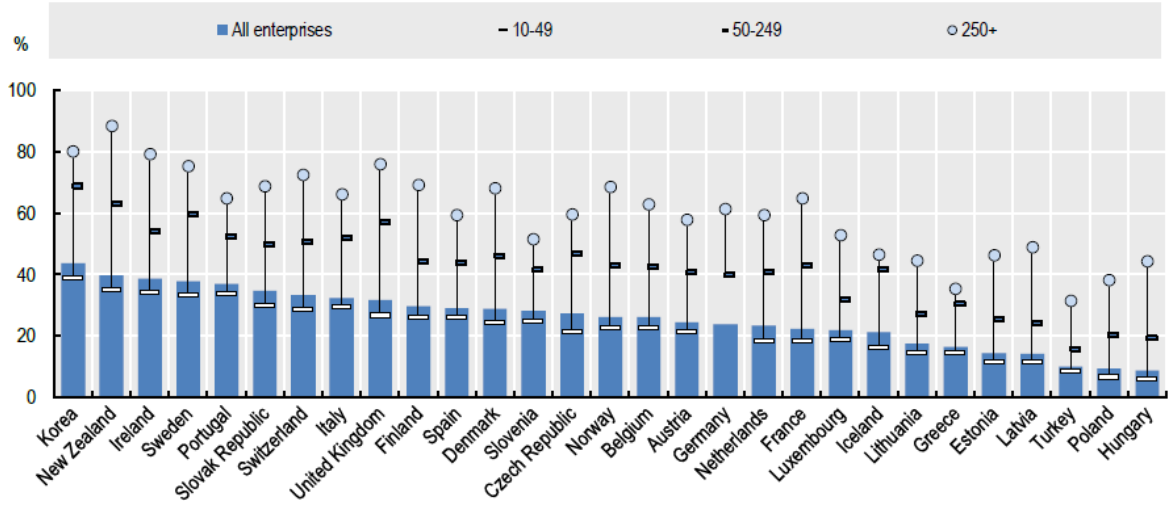
However, it is important to state that Portugal has a high percentage of computers with security software enabled but it still one of the countries that are more vulnerable to cybersecurity crimes.

In terms of the dimension of the companies, the most affected are those with between 50 and 249 workers (47.1%), followed by companies with more than 250 workers (42,6%) although companies between 10 and 49 workers are the ones that are less exposed to these

type of incidents (OECD, 2017).

When it comes to companies that have a formal policy to managing their digital privacy risks, Portugal is one of the countries that has more policies implemented in their companies.

Figure 11 - Companies that has a formal policy to manager digital privacy risks (2015) (% of all companies)



Source: OECD (2017)

In conclusion, the risk of cybersecurity incidents in Portugal is much higher than the medium of the rest of the companies in EU28.

When it comes to the data security, the biggest concerns of Portuguese companies are:

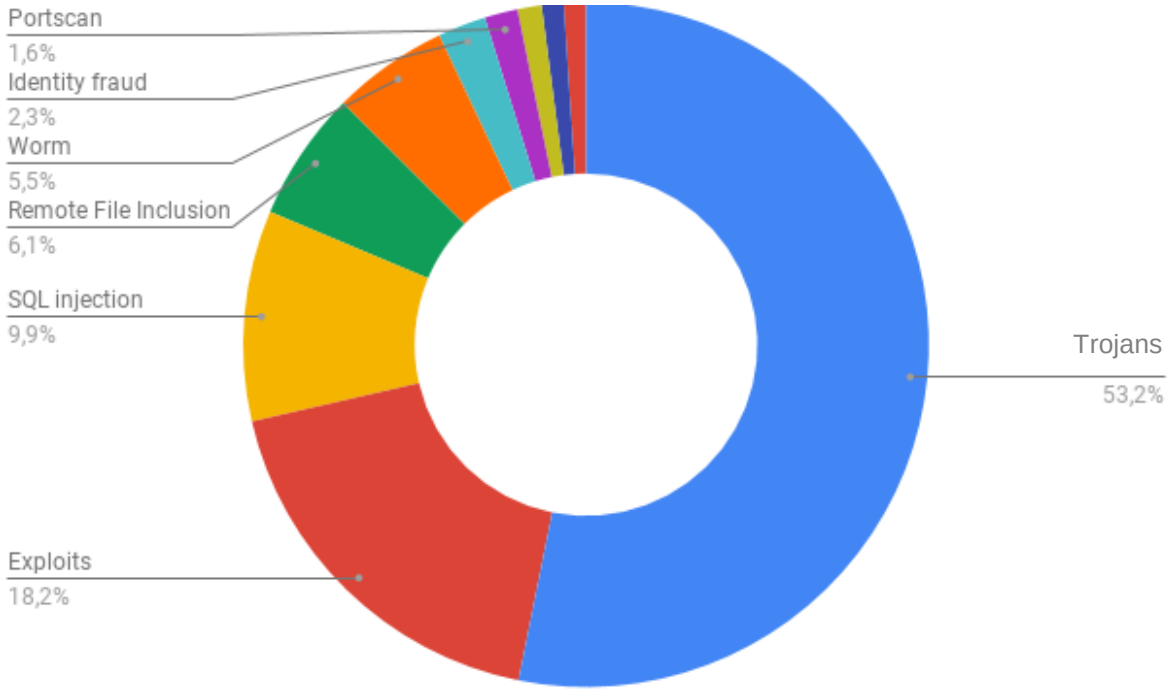
- **Internal data management** (61%), such as the risks inherent in data loss accountability (59%),
- **Infringements or cybersecurity failures** (43%)
- **Misuse of data during the exchange of data with partners** (43%).

3.1.4. Spain

As we can see in the figure above the most common attacks in Spain are:

- Trojans;
- Exploits and SQL injection.

Figure 12 - Most common incidents



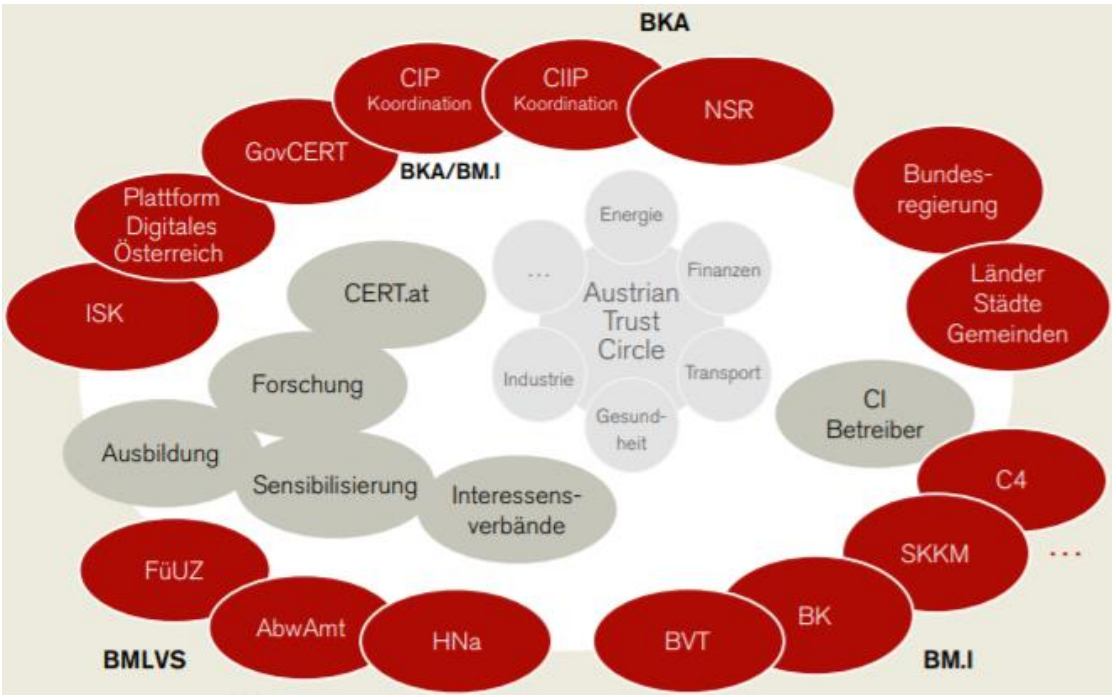
Source: Author's own elaboration from (ccn-cert.cni, n.d.)

3.2. Are in your country any teams to monitor the internet safety and cybersecurity regarding companies?

3.2.1. Austria

In the area of cyberspace there are many Austrian structures and stakeholders who are working with cybersecurity on a very distributed basis. Several organisations work exclusively in cybersecurity are already playing an important role in Austria, such as the established CERTs.

Figure 13 - Stakeholders in Austria in cases of cyber attack



Source: (Bundeskanzleramt, Digitales Österreich, 2012)

CERT.at is the Austrian national Computer Emergency Response Team, which was established in 2008 together with GovCERT Austria by the Federal Chancellery (BKA) in cooperation with nic.at, the Austrian domain registry, as a project at nic.at. As such, CERT.at is the contact for IT security in the national environment and is responsible for all cases that are not covered by a more specific CERT.

CERT.at networks other Computer Emergency Response Teams and Computer Security Incident Response Teams from the areas of critical infrastructure and Information and Communication Technology (ICT) and gives warnings, hints on concrete cases and solutions for companies and private individuals.

GovCERT Austria is the Government Computer Emergency Response Team for the public administration sector in Austria. It thus serves as the primary contact point at national level for the individual bodies of public administration in the event of a cyber-attack.

On an international level, GovCERT Austria acts as the Austrian contact point for foreign governments and international organisations on ICT security issues. It exchanges information and warnings with them and, if necessary, forwards them to domestic interested parties (Nic.at GmbH, 2018).

CERT.at and GovCERT support, within the scope of their possibilities and specifications, in security incidents. While this support is, in most cases, limited to the provision of information such as technical notes or references to commercial providers for Internet Service Providers or domain owners, CERT.at and GovCERT act as a coordination point and interface between the affected parties and other relevant actors on a national and international level in the event of major incidents. It also provides instructions for action and shares information on how to eliminate threats (Nic.at GmbH, 2018).

CERT.at must not only ensure security on the Internet in Austria but it must also protect the security of one's own IT systems and infrastructure is a decisive factor.

A certification according to ISO 27 001/2017 is the proof that IT security in a company is dealt with comprehensively and, in addition to the examination of the safety of the technical systems and the security of the physical infrastructure, including organizational aspects. The ISO 27 001 certification is a seal of quality to the outside world and on the other hand also to an ongoing incentive to ensure one's own internal security. Annual audits at CERT.at ensure that this standard is maintained (Nic.at GmbH, 2018).

The most important CERTs in Austria are: A1-CERT; ACOnet-CERT; Austrian Energy CERT; BRZ-CERT; CERT.at; CERT-Verbund Österreich; GovCERT Austria; MilCERT; Raiffeisen Informatik CERT; sCERT; SV-CERT; TSA CERT; WienCERT; WILICERT.

3.2.2. Czech Republic

There are many organizations in the Czech Republic that are actively involved in the protection of cyberspace. Examples include CERT or Computer Security Incident Response Team (CSIRT.CZ). CERTs are found in the predominate computer security organizations and various global sectors of government, commerce and academia. It addresses technical issues of cybersecurity including solving of security incidents of subjects that manage important communications and information systems for the government, then the malware analysis, collection and evaluation of information on cyberattacks and threats and so on. CERT.CZ performs tasks such as ensuring the prevention of cyber threats and attacks against crucial information infrastructure operators and public authorities and ensuring and coordination of solutions of cybersecurity incidents of crucial information infrastructure

operators and public authorities.

CSIRTs are usually services responsible for receiving, reviewing and responding to computer security incident reports and activities. Their services are usually performed for a defined constituent that could vary from a corporation to a paying client.

In the Czech Republic, the Czech Institute of Informatics, Robotics and Cybernetics (IDSA) was set up to provide a unified environment for sharing data between users in different industrial and manufacturing environments. IDSA goal is to create an ecosystem for secure data sharing that is built on a unified data exchange standard between international business partners.

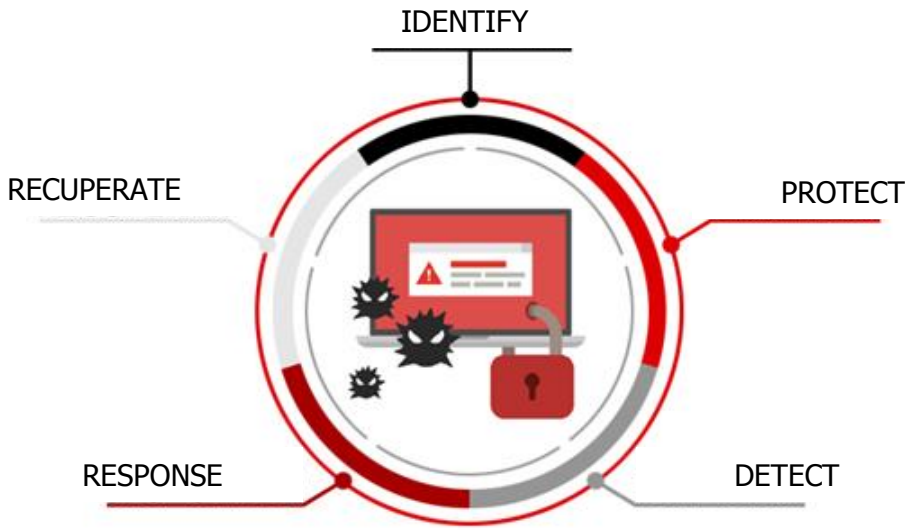
3.2.3. Portugal

In Portugal there are private companies and a CNCS that help Portuguese companies with cybersecurity issues with some services/solutions to evaluate and to have a more responsible behavior and attitudes online.

When it comes to private companies there are some services regarding online protection that are mostly provided by insurance and security companies. Some of these solutions include services that analyze the whole lifecycle of cybersecurity. In the next figure, we can see one example of one service provided by a technological group.

The service is divided into five stages: 1) identify; 2) protect; 3) detect; 4) response; and 5) recuperate.

Figure 14 - Cybersecurity services/solutions



Source: Gmv (n.d.)

In Portugal there is, as well, CERT.PT that is an integral part of the CNCS that coordinates the response to incidents involving state entities, essential service operators, operators of critical infrastructures and digital service providers. Through this service CNCS coordinates the response to cybersecurity incidents involving state entities, essential service operators and digital service providers, operators of critical national infrastructures and other national computer security incident response team.

The complexity and transnationality of a large number of cybersecurity incidents requires an aggregate view and coordinated action between the various entities involved.

Also, private security companies in Portugal are more active when it comes to the presentation of services related to digital security and managed security services in the market. Nevertheless, there majority of the organizations still don't face the protection and the security as an integrated part in their strategy.

3.2.4. Spain

In 2018, two new technical safety instructions were published in Spain:

- Resolution of 27th March, 2018, from the Secretary of State for the Civil Service, approving the Technical Instruction on Security Audits for of the Security of Information Systems;
- Resolution of 13th April, 2018, from the State Secretariat of Public Function, approving the Technical Instruction on Security for the Notification of Security Incidents.

Both come in addition to the ITS in accordance with the National Security Framework (ENS) and the previously published Security Status Report. On the other hand, the transposition process is being completed for Directive (EU) 2016/1148, of 6 July, the NIS Directive, which will also affect the public sector, and which, among other issues:

- Will identify the Essential Service Operators.
- The security measures to be applied.
- The competent authorities.

- Will identify the reference CSIRTs.
- Will assign the CCN-CERT the coordination and technical response in particularly severe cases.

In addition, and as a result of fully applying Regulation (EU) 2016/679 of 27 April on processing and free movement of personal data (GDPR), a new draft Organic Law on Data Protection has been drawn up which, repealing the current law, will regulate any issues which the General Data Protection Regulation leaves to the Commission.

Ccn-cert attending the different activities of the national cryptology center has developed:

- ATHENEA is the new cybersecurity challenge training instrument which aims to raise awareness on the importance of this field.
- GLORIA is a platform form an aging cybersecurity incidents and threats, which has also been interoperable with into the Carmen, Lucía and Reyes tools to make it easier to detect, analyze and exchange incidents.
- SAT_ICS- The main function of the Early Warning System for Industrial Control Systems is early detection of security incidents. It also allows access to a greater number of detection rules and the correlation of events, favoring support for incident resolution.

3.3. What those teams do when they face a cybersecurity incident regarding companies?

3.3.1. Austria

In the case for IT security for SMEs they can use the it-safe online guide to assess the security of their own IT infrastructure. The IT Security Handbook for SMEs provides practical information on possible dangers and the right technical measures to counter them. In this manual we can find the following contents: risk management; compliance with legal requirements; IT strategic considerations; personnel measures; computer security and virus protection; network security; data backup and emergency preparedness; construction and

infrastructure measures; IT security experts group; and, police - crime prevention.

Figure 15 - it-safe-at manual

Source: (WKO Bundessparte Information und Consulting, 2019)

In the case for EPU checklist for one-person companies, one can determine in just a few minutes whether and where there might be security problems in the IT area. In an emergency (e.g. a cyber-attack or encryption of your data by a blackmail Trojan), the Cyber Security Hotline at 0800 888 133 can provide free assistance around the clock.

The cyber-security-hotline is a three step system:

1) The call center offers 24 hours/day, 7 days a week on 0800 888 133 (free of charge for members) initial telephone information and emergency assistance;

2) The call center offers simple initial measures etc. but neither technical remote diagnostics, nor legal assistance or questions on prevention, coordinates (free of

charge for members) but gladly - if necessary and desired - the contact to a company of the UBIT ExpertsGroup IT-Security specialized in IT security and cybercrime from your proximity. It is advisable to take advantage of this free initial consultation with the IT security company;

3) The IT security enterprise contacts the damaged ones and accomplishes a free first meeting on basis of the data raised by the call center. Although remote diagnoses can never give a complete picture, these specialists can assess their situation better and, if necessary, provide information about more concrete immediate measures and coping measures for the establishment of normal operations. It also helps to determine whether and in what form the IT security company can help with a possible on-site deployment, which goes beyond the initial consultation and is subject to a charge. Any further assignment must then be agreed directly with the IT security company; the costs (hourly rate, etc.) for further activities must also be agreed directly with the IT security company.

3.3.2. Czech Republic

There are many organizations in the Czech Republic that are actively involved in the protection of cyberspace. Examples include CERT or CSIRT.CZ.

CERTs are found in many computer security organizations and various global sectors of government, commerce and academia. It addresses technical issues of cybersecurity including solving of security incidents of subjects that manage important communications and information systems for the government, then the malware analysis, collection and evaluation of information on cyberattacks and threats and so on. CERT.CZ performs tasks such as ensuring the prevention of cyber threats and attacks against crucial information infrastructure operators and public authorities and ensuring and coordination of solutions of cybersecurity incidents of crucial information infrastructure operators and public authorities.

CSIRTs are usually services responsible for receiving, reviewing and responding to computer security incident reports and activities. Their services are usually performed for a defined constituent that could vary from a corporation to a paying client.

In the Czech Republic, IDSA was set up to provide a unified environment for sharing data

between users in different industrial and manufacturing environments. The main goal of this institute is to create an ecosystem for secure data sharing that is built on a unified data exchange standard between international business partners.

3.3.3. Portugal

In the case of Portugal, CNCS act as an operational coordinator and national authority specialized in cybersecurity along with entities of the National Critical Infrastructures operators. In other words, CNCS promotes the use of cyberspace in a free reliable and secure way through the continuous improvement of national cybersecurity and international cooperation. The role of this institution is to give information and raise awareness not only of public entities and critical infrastructures but also of businesses and civil society. On the other hand, it is important that the country be equipped with qualified resources to deal with qualified human resources to deal with the complex challenges of the security of cyberspace.

This institution has, therefore, a crucial role in this field in Portugal and is responsible to organize and give different types of tools to spread a security culture that promotes to all the knowledge, awareness and confidence needed to use information systems, reducing exposure to the risks of cyberspace.

The CNCS mission is to implement measures and instruments necessary to anticipate, detect, react and recover situations that, due to the imminence or occurrence of incidents or cyber attacks, may jeopardize the functioning of state agencies, critical infrastructures and national interests.

The teams that works in this organizations organize:

- **Events** such as C-DAYS that is a national reference event that focuses one big themes related to information security and cyberspace. This event happens every year and has multiple actors (industry, society, government, industry, academy,…) involved;
- **Awareness sessions in multiple themes** regarding cybersecurity that can be seen in the website of the CNCS;
- **Seminars** designated by "Cibertemas" related to cybersecurity and also promotes

project promotion, debate and the share of ideas.

- **Awareness and training program in cybersecurity** in different parts of the country, from north to south, passing through the island counting with the support of partners;
- The possibility to **notify and get help in the eventual presence of some incident**;
- **General courses** of cybersecurity that lasts two days. The majority of these types of events are free but need a registration.

Like mentioned before, CERT.PT is an integral part of the CNCS that coordinates the response to incidents involving state entities, essential service operators, operators of critical infrastructures and digital service providers. The coordination of incident response includes:

- The screening of incidents reports, their technical and forensic analysis;
- The articulation with the national and international entities involved;
- Coordination of incident response may be initiated by the CNCS for example in a large-scale incident situation or may be requested by channels designated for that purpose.

In the case of necessity the CNCS coordinates its action with other national authorities. This service can be solicited in the website of CNCS, by email or by telephone contact.
But, the companies that face a cybersecurity incident and that have some support especially from security and insurance companies are more protected and can solve their cybersecurity issues more easily because they can count with a specialized team that knows what to do and to solve cybersecurity issues. Each company that has services/solutions related to this area have their own methods, tools, controls, analysis, tests and each case is a case.

3.3.4. Spain

The cybersecurity world is extremely dynamic. New threats are always emerging and new vulnerabilities discovered, even when short time ago they were not considered as such. These facts have made that the IT and network communication systems evolve to face

these alarming circumstances. For this reason, there is an increasing demand of new systems to detect and manage security incidents that could have an impact in industrial facilities. Each cybersecurity incident that is captured allows identifying the system's vulnerabilities as well as the management process to respond to it. As a consequence, the experience provided by the teams in CERTs are very valuable.

One of the first challenges to overcome will be the inconvenience and impact that security measures may have in the day-by-day operations. This is particularly relevant when there is the need of an emergency response. If, in this case, there is a delay caused by the applied security measures, the result could be catastrophic. In addition, cyberattack techniques evolve permanently. This fact requests from the facilities operators to be technically updated even if such challenges are not directly related to their jobs. As a consequence, it should be developed new automatic response procedures to detect and to prevent cybersecurity incidents. Nevertheless, there is an additional difficulty because real time operating systems have a limited capacity to register and store data on the situation before and after a threat, reducing the forensic evidence when there is an incident. Managing each incident may be extremely useful to prevent future events, to answer to them in shorter time and to manage more efficiently their effects. Considering all of this, new tools and procedures to get and use this knowledge must be put in place, in a way that the contributing companies are not damaged from such a fact.

CERTs role and experience in Spain has a key to develop this item because of the knowledge and capabilities already acquired that can be applied to this new environment, and support the development of tools to:

- Detect the incident;
- Evaluate its relevance and size;
- Report about the incident itself;
- Enable the communication between all the involved entities;
- Technically assistance in the recovery of the implied systems;
- Identify the root cause of the incident;
- Avoid future similar incidents;
- Develop improvements and a knowledge base on the learnt lessons;

- Support the forensics study of the incident.

These services must be supported by others that will, as well, sustain the rest of initiatives such as:

- To announce and report on-going attacks;
- To identify, to study, to classify and to publish new vulnerabilities;
- To recommend new actions to improve general cybersecurity;
- To develop and catalogue cybersecurity solutions available for the general market;
- To develop forensics technologies and capacities.

3.4. Identify the main risks/difficulties that people face everyday in their work regarding cybersecurity?

3.4.1. Austria

The assessment of the trends for 2018 revealed a very broad spectrum of observations and assessments. After categorization and grouping, the most frequently cited trend assessments can be summarized as follows:

- The danger situation is on the rise and **attacks are becoming more complex** and frequent and the main motivation behind attacks is monetization;
- **Cloud security is becoming a critical issue** and companies are expected to become increasingly dependent on cloud providers;
- The **Network and Information Systems Security Act and the Basic Data Protection Ordinance will place considerable demands on companie**s;
- The importance of **organizational measures (e.g. risk management) will increase in future** compared to purely technical measures;
- One assumes that one cannot completely protect oneself from attacks and it is important to recognize attacks quickly and to react correctly;
- The **dependence of companies on hardware and software products** also represents an increasing threat.

3.4.2. Czech Republic

The main threats that people at work most often face are:

- **Increasing volumes of data (Big Data) and the issue of governance and security of such amount of data.** Protection and data security are very important for the Czech Republic, especially those that are a matter of public interest. In public and private sector the amount of data which is growing and that it is necessary to continue to store more data. Therefore, they began to use new forms of data storage, for example cloud storage. Increased use of these online services and cloud, however, often leads to non-transparent security solution whose credibility can be questionable;
- **Diversity of mobile devices ("bring your own device").** Significant internal threat is a worrying trend of growing acceptance of model "bring your own device". With the "bring your own device" target companies are initially infect personal employee's devices who did not implement strict security measures and then through them puts Trojan that infects the network. Policies on the use of hardware owned by employees must be thoroughly examined and, where necessary, updated and expanded;
- **Security and privacy of cloud services.** Attacks on cloud services are gaining strength and it is expected a great breach of security in the cloud in the near future. Nowadays, three-quarters of a security breach last for days, weeks or even months before they were discovered, and thus greatly increase the damage attackers;
- **Need for tracking the movement of data within the organization.** Behavioral analysis technologies enable companies and institutions to monitor users within companies and end users. This may bring to them the warning about suspicious behavior that could be data theft or attacks by malicious software;
- **Attacks to destroy.** Some ideologically profiled hacktivist group upheld that they will continue to try to destructive attacks against the interests of certain companies or public institutions;
- **Safety risks associated with computerization of public administration (eGovernment).** For example, electronic procurement process will entail new risks

that may threaten the credibility of the procurement procedure and safety risks associated with the fact that electronic tools for procurement are connected to the public network.

The best way to determine the appropriate incident response in any given situation is to understand **what types of attacks are likely to be used**. There is provided the list of the different attack vectors that people face in their work regarding cybersecurity:

- **External/removable devices:** An attack executed from removable media (e.g. flash drive, CD) or a peripheral device;
- **Email:** An attack executed via an email message or attachment (e.g. malware infection);
- **Attrition** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services;
- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories
- **Web:** An attack executed from a website or a web-based application (e.g. drive-by download);
- **Loss or theft of equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.

3.4.3. Portugal

In Portugal, the main risks and difficulties that workers can face in their professional life are as follows:

- **Web attacks that the main motivation behind is related to monetization and the spread of confidential/private information**;
- **Phishing**;
- **Spam**;
- **Malware infections through email**;
- **Web based attacks**;
- **Cloud security and privacy**;

- **Data privacy management**;
- **Exposition to informatics attacks, system failures and data violation**;
- **Global risk profile of the companies** (some activity sectors are more exposed than other);
- The **lack of knowledge to detect fake information** that can lead to, for example, infections and data robbery;
- A **web attack** executed from some untrusted source;
- The **increase use of hardware and software** products also represents an increasing threat as well.

3.4.4. Spain

The main risks/difficulties that Spanish people are facing nowadays are:

- **Malware**;
- **Web based attacks.** With majority of the business operations are being conducted online, web based attacks are continually on the rise. Cyber criminals are becoming more innovative and use sophisticated techniques to exploit unpatched vulnerabilities in the web applications. The motive behind these attacks may be different, to steal a company's sensitive information, display spam advertisements on the website or download malware to the user's computer;
- **Web applications attacks** raise a number of security concerns stemming from improper coding. Serious weaknesses or vulnerabilities allow criminals to gain direct and public access to databases in order to churn sensitive data. Many of these databases contain valuable information (e.g. personal data and financial details) making them a frequent target of attacks;
- **Data breaches**;
- **Phishing**;
- **Spam**;
- **Denial of service**;
- **Botnets**.

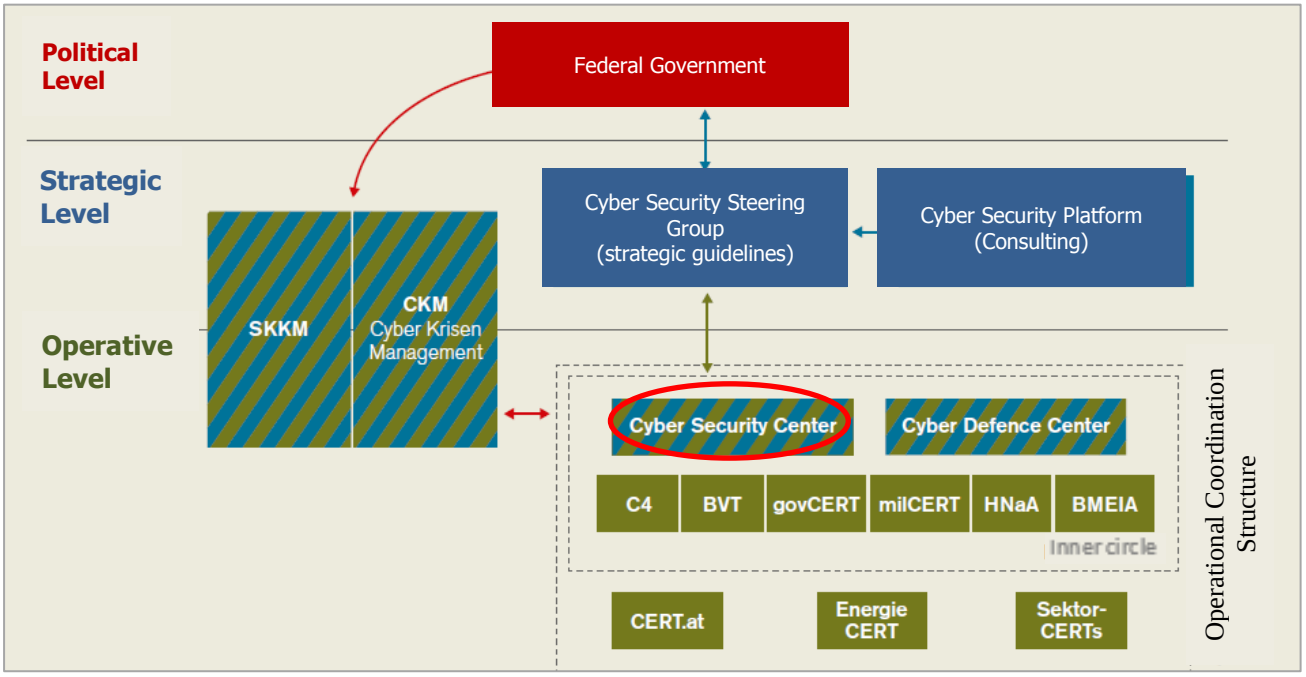
3.5. What is being applied in your country in order to improve internet safety of the citizens in their work?

3.5.1. Austria

In order to protect cyberspace and people in virtual space, the Österreichischen Strategie für Cyber Sicherheit - Austrian Strategy for Cyber Security (ÖSCS) provides, among other things, for the creation of a structure for coordination at the operational level. The strategy INNEN.SICHER also cites cybersecurity as a key challenge.

As a result, the INNEN.SICHER project "Cyber Security. BVT" was launched in June 2014, the central element of which is the establishment of a CSC in the Federal Ministry of the Interior. This project was successfully completed in December 2017 with the transfer of the CSC to regular operation. The importance of the project is underlined, among other things, by the fact that the EU has provided considerable funding from the Internal Security Fund.

Figure 16 - Cybersecurity in companies



Source: (Cyber Sicherheit Steuerungsgruppe, 2018)

The central tasks for the CSC are based on four pillars: network and information security authority; prevention and protection of critical infrastructures; coordination and cyber crisis

management; and, technical competence and contact persons.

An essential central task is the implementation of comprehensive prevention work trough:

- **Awareness events;**
- **Lectures;**
- **Counselling interviews;**
- **Good cooperation with industry and the existing structures** in the field of cybersecurity in Austria.

The ICT security portal onlinesicherheit.gv.at is an initiative in cooperation with the Austrian economy and functions as a central internet portal for topics related to security in the digital world. As a strategic measure of the national ICT security strategy and the Austrian strategy for cybersecurity, the initiative pursues the goal of promoting and sustainably strengthening the ICT and cybersecurity culture in Austria by:

- **Sensitizing and raising awareness among the target groups** concerned and by providing them with target-group-specific recommendations for action;
- **Provide a range of information and services** on offer is continuously expanded within the framework of regular editorial meetings with the 39 cooperation partners (federal ministries, provincial governments, authorities, universities of applied sciences, research institutes, companies, associations and interest groups). It contains the latest news and warnings, advice and further information for both beginners and experts;
- **Information through news articles, publications and event entries**. In 2018, each month, a focus topic on current trends was defined, with a total of 34 specialist articles published;
- **Training activities (courses);**
- **Preventive measures and intensive investigative work;**
- **Increased preventive work and police projects such as "CyberKids" and "Click & Check**".

3.5.2. Czech Republic

As digitization continues each company is naturally less resilient to virtual security risks. Experts in the Czech Republic defined five cybersecurity rules for companies:

- **Companies should create a special security team and include it in strategic measures**;
- **Involving employees to participate** in results can be one of the most reliable steps that can be taken;
- **Customer Protection.** Due to the interconnectedness of the offices of the future, companies should help their clients to understand how they can protect themselves not only from legal problems. Organizations should actively seek to understand the implications of both new and forthcoming legislation so that they can advise clients properly;
- **Companies should work with their partners, suppliers and other third parties** to share knowledge, products, and services related to cybersecurity;
- **Companies are rarely willing to share information or collaborate with others** but the information that they can give about a cyber-attack that they suffer is very important for multiple stakeholders to know and to think about what they can do to avoid a similar cyber attack.

Today, a common part of company's management is Information Security Management System. The basic elements used in internal business network protection systems are:

- **Workstation-level antivirus protection** for example, at the level of internet gateways;
- **Antivirus protection for file servers and groupware environments**;
- **Antivirus protection for internet gateway communication**;
- **Email antispam protection**;
- **Intrusion detection and prevention systems**. These are rather sophisticated security tools that can detect (IDS) an ongoing attack and take action to eliminate it (IPS). Implementing these systems is longer and more demanding, which often discourages administrators from using them consistently.

3.5.3. Portugal

The most common good practices that people have in their work are:

- **Participation in events** such as C-DAYS that is a national reference event that focuses one big themes related to information security and cyberspace;
- Use of **antivirus software in computers;**
- Access to **information through journals, websites and the general media**;
- **Awareness sessions in multiple themes** regarding cybersecurity;
- **Seminars** related also to cybersecurity that also promotes project promotion, debate and the share of ideas;
- **Awareness and participation in training program in cybersecurity** through CNCS which it is intended to massif the training and awareness;
- **Use of special security teams** present in the own company (not so frequent) and through subcontracted specialized company in security;
- The **possibility to notify and get help** in the eventual presence of some incident;
- **General training activities** (courses and workshops) that happens once in a way;
- **Internal training by some team member**.

3.5.4. Spain

In order to improve safety it is being implemented several responsibilities that are outlined below:

- **Involvement of companies in all the initiatives** in such a way that it may contribute with its experience and knowledge;
- **Develop enablement programs, tools, techniques, and reference documents that may support the performance of the cybersecurity professionals**. Among such reference techniques, it must be developed implementation methodologies, cybersecurity policies and procedures, as well as best practice guides for each industrial sector;
- **Organize training initiatives, free manuals and workshops** that take into account the different needs of all the related roles, special emphasis should be for the IT professionals that want to get involved in the protection of automation plants

and control systems. It must be considered the training needs of the professionals and control engineers that want to design in a secure way the new control and automation infrastructures;

- **Publish executive level in-depth analysis reports on the cybersecurity benefits**;
- **Supervision and constant monitoring on the milestones and advances that may have an effect on industrial cybersecurity** to assure the effectiveness of the executed actions.

In this regard, we can highlight the trajectory of the Telefonica Group, which at the beginning of the century began to form the line of Cybersecurity and now has 16 CSIRTs spread around the world. In addition, the subsidiary company expert in engineering "Next" that belong to BBVA group will drive the technological transformation of the BBVA bank. For this purpose it has advanced experts in mass analysis and macrodata, AI, blockchain and cybersecurity. As far as cybersecurity is concerned, they have a solvent team which will offer advanced professional security services including infrastructure and application solutions, development of secure software and cybersecurity solutions for both the BBVA Group and leading companies.

4. Internet safety and Industry 4.0: in private life

4.1. Which accidents concerning the internet safety were solved in your country in the recent years in the citizen's private life?

4.1.1. Austria

There was no information about these topic for Austria.

4.1.2. Czech Republic

The most common attacks in citizen's private life are:

- **Virus:** the most common virus can be spread through email and text message attachments, internet file downloads and social media scam links;
- **Worm:** email worms are usually spread by creating and sending outbound messages to all the addresses in a user's contacts list;
- **Scam:** some of the most common scams are: phishing; donation scam (a person claiming they have or have a child or someone they know with an illness and need financial assistance); catfish (a person who creates a fake online profile with the intention of deceiving someone); and, chain mail that is usually harmless and spread through e-mail and tells people to forward the e-mail;
- **Spam**: most email spam messages are commercial. Whether commercial or not, many are not only annoying but also dangerous because they may contain links that lead to phishing web sites or sites that are hosting malware or include malware as file attachments;
- **Phishing**.

4.1.3. Portugal

The most common incidents that are faced by people in their private life are:

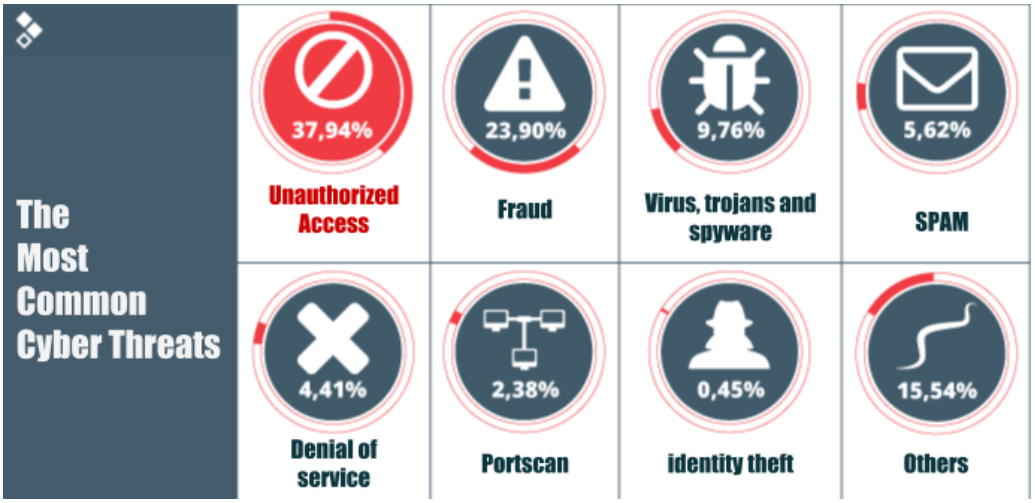
- **Virus**;

- **Phishing**;
- **Spam**;
- **Unauthorized access**;
- **Identity deft especially in social media.**

4.1.4. Spain

The most common cyber attack, as we can see in the next figure are: unauthorized access and fraud.

Figure 17 - Most common incidents



Source: (INCIBE, n.d.).

4.2. Are in your country any teams to monitor the internet safety and cybersecurity regarding citizens in their private life?

4.2.1. Austria

In Austria the team that is responsible to monitor the internet safety and cybersecurity for citizens is the Cyber Crime Competence Center (C4). The Cyber Crime Competence Centre (C4) is the national and international coordination and reporting centre for fighting cybercrime. The Centre is made up of technically and professionally highly specialised experts from the fields of investigation, forensics and technology. The Cyber Crime

Competence Center C4 was established in 2011 to combat computer crime as a separate unit within the Criminal Investigation Department of the Federal Criminal Police Office. Cyber Crime Competence Center C4 is divided into four units: "Central Tasks"; "Safeguarding IT Evidence"; "Investigations"; "Development and Innovation"; and, the Reporting Office.

Figure 18 - Logo cyber crime center

Source: (Bundeskriminalamt[1], 2019)

The Cyber Crime Reporting Office of the (C4) is on the one hand the contact point for the population. This enables new phenomena to be identified at an early stage. On the other hand, it is also the interface to the CSC and an international contact point in Cyber Crime matters. Another important task is the contact point for all police services in connection with Cyber Crime (Cyber Sicherheit Steuerungsgruppe, 2018).

4.2.2. Czech Republic

The association NarodniCentrumBezpecnejsiholInternetu (NCBI) is a member of the pan-European network of national safer awareness centers INSAFE. In collaboration with its partners NCBI organizes conferences, seminars, lectures and training sessions related to safer internet use and internet crime prevention in the Czech Republic.

Figure 19 - Logo NCBI

Source: (S@ferinternet.cz, n.d.)

Centre for prevention of risky virtual communication is an institute dealing with risky forms of online communication of children and adults. It focuses on cyberbullying, cyberstalking, hoaxes and spamming; sexting; social engineering in the online community; the risk of sharing personal data in social networks; and, other hazardous communication phenomena.

4.2.3. Portugal

In Portugal there are a few institutions that can help the Portuguese society to prevent cybersecurity incidents. The institutions can be seen as follows:

In Portugal, there are two entities that promote web security and personal data protection:

- **CNPD:** the first one and the most well-known is CNPD that is an independent administrative entity with powers of authority which works with the Assembly of the Republic. The CNPD cooperates with the data protection supervisory authorities of other states, namely in the defense and exercise of the rights of the persons that live abroad. In addiction, the CNPD is the empowered body to supervise and monitor the compliance with the laws and regulations within the area of personal data protection with strict respect for human rights and freedom. CNSC wants to guarantee freedom, security and a justice cyberspace for everyone. In the short term this consortium gives some answers to prevent adverse events. In a medium/long term the goal is to develop good practices regarding cybersecurity.

Figure 20 - Logo CNPD

Source: (CNPD, n.d.)

- **Association "Associação dos Profissionais de Proteção e de Segurança de Dados":** this is a professional association that represents individuals and organizations that deals with protection and data security, privacy and electronic communication regulation or who hold the position of data protection officers in organizations operating in Portuguese territory.

4.1.4. Spain

INCIBE-CERT is one of the reference incident response teams that improve the efficiency in the fight against crimes involving networks and information systems, reducing their effects on public security. INCIBE's mission is to strengthen cybersecurity, trust and the protection of privacy with respect to services offered within the information society, providing value to the public, businesses, the Spanish government, the Spanish academic and research network, the information technology sector and strategic sectors in general.

INCIBE is the reference security incident response center for citizens and private law entities in Spain, operated by The Spanish National Cybersecurity Institute, under the Ministry of Economy and Business through the Secretary of State for Digital Advancement. As a center of excellence, INCIBE is a service offered by the Spanish government to work towards the development of cybersecurity as an instrument for social transformation and for developing new fields of innovation. To this end with its activities focused on research, the provision of services and cooperation with the relevant actors, INCIBE heads a range of initiatives directed to cybersecurity at a national and an international level.

Figure 21 - Logo incibe

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

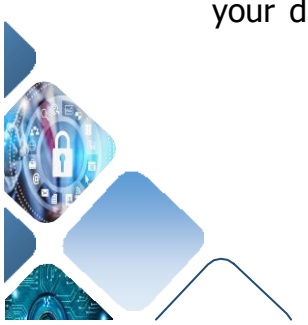
Source: (Incibe.es, n.d.)

4.3. What citizens do in your country when they face a cybersecurity incident?

4.3.1. Austria

In Austria there are various and topic-specific hotlines to which you can turn if you have become a victim of IT-related crime. Depending on the type of the cybersecurity incident people can rely on different authorities. There are also some institutions that provide important information (e.g. tips) to avoid cybersecurity incidents.

- **The Watchlist Internet:** this institution lists on its website numerous articles about various fraud attempts, such as fake shops, phishing, fake bills and subscription traps. This is also a list of fraudulent online shops, which is always kept up to date. This is the institution that Austria people can be in touch if they have a rip-off and fraud incident;
- **Internet Ombudsman:** this reporting office offers help with dispute resolution as well as free online advice on all aspects of shopping on the Internet. The Internet Ombudsman is a state-approved conciliation body for disputes arising out of online contracts under the Alternative Dispute Resolution Act. It also offers free arbitration and advice on other internet-related topics (copyright, data protection law, the right to one's own image, personal rights, etc.) (Bundesministerium für Digitalisierung und Wirtschaftsstandort[1], 2019);
- **Criminal police work:** a special reporting office has been set up to provide information to the citizens if they have to fight a cybercrime situation. Also, if a person has a suspicion or concrete indications of cybercrime, they can contact the relevant reporting office of the Federal Ministry of the Interior (Bundesministerium für Digitalisierung und Wirtschaftsstandort[1] , 2019).
- **Saferinternet.at:** Saferinternet.at is the Austrian information and coordination point in the Safer Internet Network of the EU. It supports internet users with tips and assistance in the competent and safe use of the internet, mobile phones and computer games. The initiative is aimed specifically at children, young people, parents and teachers (Bundesministerium für Digitalisierung und Wirtschaftsstandort[1] 2019);
- **Cyber-Security-Hotline:** in an emergency (e.g. a cyber attack or encryption of your data by a blackmail Trojan), the Cyber Security Hotline at 0800 888 133 can



provide free assistance around the clock;

- **Information security commission**: in the Federal Chancellery acts as a national and internationally recognized contact point National Security Authority for all questions in the field of information security and the relevant areas such as personnel security, physical security, document security or register management and information security, as well as a national accreditation body for domestic institutions in connection with the processing of classified information (Bundesministerium für Digitalisierung und Wirtschaftsstandort[2] , 2019).

4.3.2. Czech Republic

Cybersecurity is a global phenomenon representing a challenge for all individuals. Although cybersecurity is one of the most important challenges faced by governments today, the visibility and public awareness remains limited. Almost everybody has heard of cybersecurity, however, the urgency and behavior of persons do not reflect high level of awareness. Some main measures following by public:

- **Have a legal and regularly updated operating system**;
- **Use antivirus and firewall software**;
- **Update your web browser regularly**;
- **Use the domain name system security extensions** which provide origin authentication of data;
- **Use a secure password**.

4.3.3. Portugal

If there is a situation where people face a cybersecurity incident they can contact some institutions. These institutions are mentioned bellow:

- **Association "APDPO Portugal - Associação dos Profissionais de Proteção e de Segurança de Dados":** this is a professional association that represents individuals and organizations that deals with protection and data security, privacy and electronic communication regulation or who hold the position of data protection officers in organizations operating in Portuguese territory;

- **Contact telephone line "internet segura":** The association Associação Portuguesa de Apoio à Vítima is responsible for the management and operationalization of this line. The main purpose of this telephone and online line is to help and respond to doubts and problems related to online security, cyberbullying, bullying and unworthy exposure for young people, adults, teachers and children. The full support is confidential and anonymous;
- **Contact the telephone line "Linha aberta":** this telephone line is focused on illegal content (child porn, violence and racism) and criminal prosecution of those who publish this type of content;
- **Contact the policy officers,** if required.

However, it is important to say that people have free access to some initiatives (e.g. measures, workshops, courses, tutorials…) to prevent cybersecurity incidents.

4.3.4. Spain

The early incident detection is the corner stone to support actions and procedures to stop their expansion and effects and to make the recovery easier. To detect these harmful actions in a systematic way it will be needed to develop and deploy detection agents, as well as the implementation of centralized event management tools. An incident, once it is detected, should be identified and valued in its type and impact. It should trigger a response procedure that allows in an automated way; to aware the potential harmed personnel or facilities about the incident's nature and main features. It should offer as well, detailed information to take the appropriate decisions for its management and deploy the following appropriate stopping measures:

1. Replant safety parameters;
2. Secure confidential data;
3. Prevent attacks, in an integrated way by implementing ciber-measures;
4. Incorporate key functionalities to interact with these devices without risk. These functionalities will ensure accessibility, integrity, confidentiality and access control;
5. Classify possible risks and threats;

6. Include highly reliable software.

4.4. Identify the main risks/difficulties that people face everyday in their private life regarding cybersecurity?

4.4.1. Austria

The main risks/difficulties that people face everyday in their private life are:

- **Phishing** through data theft;
- **Ransomware (blackmailstrojan, cryptotrojan):** it practically takes the infected computer hostage and either encrypts individual data and folders or encrypts them;
- **Trojans:** are mostly unnoticed on the computer and work in the background to send spam mails or DDoS attacks against certain websites or companies;
- **Viruses and worms:** what a virus or worm ultimately do with its own computer cannot be predicted or limited. In the beginning, there were often joke viruses that fade in messages or shut down the PC. Nevertheless, such an offender can simply delete or encrypt all data;
- **Online harassment** through cyber bullying, cyber-stalking;
- **Fraudsters in online shopping** (fake shops, brand counterfeiting);
- **Subscription traps, hidden terms and conditions**;
- **Classified ad fraud**: non-existent companies that send fake messages and then pay money without receiving the goods;
- **Privacy and data protection settings**;
- **Hoax/chain letter**.

4.4.2. Czech Republic

Cyber-crime trends were drawn from the annual reports published between 2011 and 2016, which are published annually by the Ministry of the Interior, Department of Security Policy. Each report on the situation in the field of internal security and public order in the Czech

Republic (until 2016) describes, among others information crime and cybersecurity for the previous year, e.g. for the period 2010 to 2015 with the exception of 2010 there are in all reports the quantified data about information crime.

The most common manifestations of this crime identical are:

- **Copyright violations;**
- **Spread of extremist and terrorist propaganda;**
- **Disseminating of prohibited pornography;**
- **Fraudulent conduct;**
- **Threats;**
- **Blackmail;**
- **Scaremongering;**
- **Slander;**
- **Attacks on information systems and data;**
- **Stalking;**
- **Copyright violations;**
- **Threats;**
- **Extortion and swindling;**
- **Unauthorized data manipulation;**
- **Swindling** (cases of fraud in the information technology and especially the Internet).

The total number of cyber incident are growing since 2011 (please see the table above). In 2015 the number of cyber incident was 5023 cases.

Figure 22 - Number of Cyber Incident (characteristics of time series)

year	number of incidents	absolute growth	relative growth	growth coefficient
2011	1502	-	-	-
2012	2195	693	0.461385	1.461385
2013	3108	913	0.415945	1.415945
2014	4348	1240	0.39897	1.39897
2015	5023	675	0.155244	1.155244

Source: Sociálno-Ekonomická revue (2017)

4.4.3. Portugal

Nowadays, the main risks that people face everyday in their private life regarding cybersecurity are:

- **Virus and computer worms**;
- **Malware infections through email**;
- **Malicious software**;
- **Phishing**;
- **Trojan**;
- **Worm**;
- **Virus**;
- **Spam**;
- **Fraudulent links**;
- People that **easy provide personal information online** such as identity card number, payment details, credit/debit card or bank account number;
- The **abusive utilization of personal information**;
- Children **access to inappropriate digital content**;
- The **lack of limitation to cookies** due to the lack of knowledge.

4.4.4. Spain

The lack of knowledge about the digital information environment constitutes a vulnerability of the Spanish public opinion. Here is a list of some of the key problems that people have to face everyday:

- **Ransomware.** The methods of infection using ransomware are:

- **Remote Desktop:** Protocol New way to infect computers with ransomware. It allows remote access to the system, which will be infected later on;
- **Mobile devices:** The volume of mobile ransomware multiplied more than three time during the last year;
- **Email:** It is the most popular means to distribute ransomware because there is no appropriate method to guarantee protection;
- **Exploits:** Used to infect systems. One example of this was seen in poorly protected databases, such as the Mongo DB attacks;
- **Tvs:** Cases of ransomware were seen concerning infection of conventional television sets, as a result of the new-found sophistication of these attacks;
- **Medjack:** Medical device hijacking, resulting from integrating traditional ICT and health technology.

– **Distributed denial of service (DDoS) attacks.** The type of attacks more frequent are:
  - **IOT devices:** The number of vulnerable IOT devices has contributed to the increase in the size of DDoS attacks;
  - **DDoS as a service:** In development, due to the reduction in the cost of the tools required to carry them out;
  - **Extortion:** Extortion actions under threat of DDoS attacks or interruption of online services.
– **Hacktivism**. These attacks can be even more damaging than traditional threats because hacktivists are often trying to make a statement, so their efforts are usually very publicly damaging for an organization's reputation;
– **Botnets.** Hacking into such systems will become more common over the coming years with ransomware and hacktivism thought to be key problem areas. There is also a significant privacy threat as smart devices typically contain a considerable amount of sensitive information that cyber criminals could access;
– **Manipulating or deceiving key individuals** into divulging important data or financial information, such as through phishing techniques;

- **Insider threats (access to confidential information).** There is a significant chance of cybersecurity issues arising internally. Most external threats are easy to recognize and identify. Of these, more than two-thirds were people with malicious intent, while the remaining incidents were due to 'inadvertent actors'. The latter refers to innocent individuals who accidentally allowed attackers access to information, or who failed to follow security measures;
- **Mobile malware;**
- **Fake ads and feedback**. Consumers are frequently bombarded with advertisements online and the proliferation of fake ads and phishing attacks have eroded trust in net-based marketing collateral;
- **Cloud-based services and computing**;
- **Information flow among various devices**. Most employees today will bring their own devices to work for example, smartphones, tablets, and laptops. But if these devices are doubling as both work and personal devices, this could compromise your company's confidential information or data;
- **Managing employee credentials.** Ensuring that only the proper employees and contractors have access to confidential or compartmentalized business information can be the difference between a strong security environment and falling prey to insider cyber threats.

4.5. What is being applied in your country in order to improve internet safety of the citizens in their private life?

4.5.1. Austria

In Austria there are some initiatives to improve internet safety of the citizens in their private life. Some of them can be seen above:

- **Brochures with basic security tips** for the correct use of the internet and computers for personal IT security. These tips deal with the following topics: protection of the PC; e-mails and chat; software; file-sharing networks; online shopping; payment; online banking on the web; private information, photos and

passwords; offers as commodity or financial agents; and, apps and subscription traps. These brochures are made by The Austrian Federal Criminal Police Office;

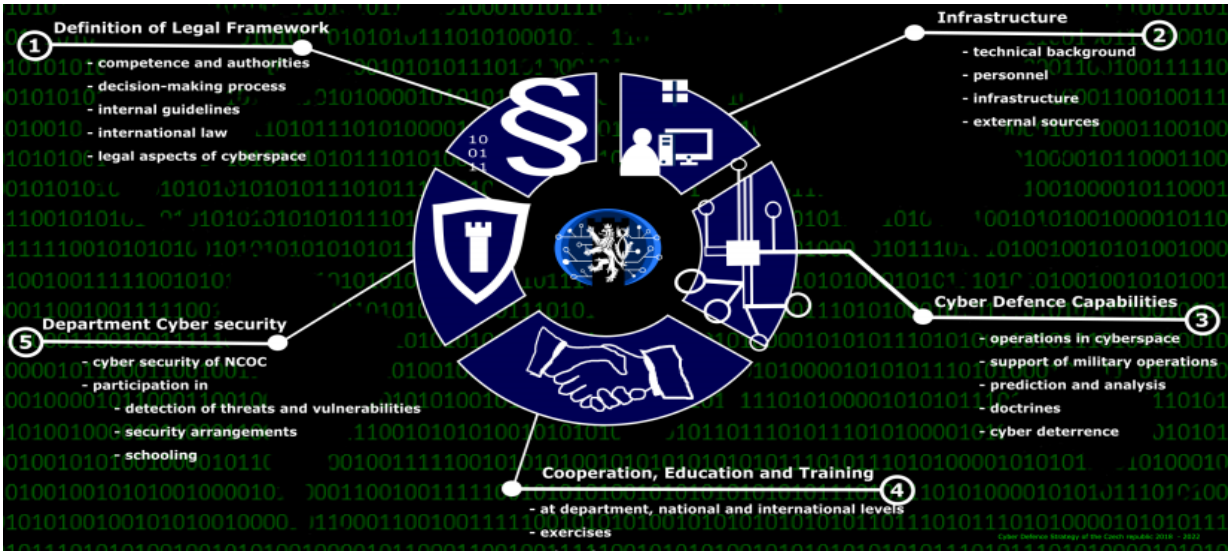
- **News**.

4.5.2. Czech Republic

In order to improve safety it is implemented The Cyber Security Strategy of the Czech Republic. The Cyber Security Strategy for the Czech Republic covers the years 2015 to 2020. The National Cyber Security Strategy of the Czech Republic is a **document** that declares the core values, interests, attitudes, ambitions and tools of the CR to safeguard the security and formulates the principles on which the security policy of the CR was founded. In this strategy are defined vital, strategic and other important interests of CR, the security environment of the CR as well as described the security system of the CR. Security Strategy is the basic document of the Security Policy of the CR. In the text is on the general level stressed also the cybersecurity. This strategy then builds sub-strategies and concepts.

The basic principles of the cybersecurity strategy: linking and strengthening the cooperation of all sectors of society; individual responsibility; departmental cooperation; international cooperation; adequacy of measures taken; use reliable and trusted information technology; and, raising cybersecurity awareness.

Figure 23 - Cyber Defence Strategy of the Czech Republic (2018-2022)



Source: National Cyber Operations Center (n.d.)

There are also other good initiatives to mentioned such as:

- **Project Safer Internet:** the aim is to raise awareness about internet safety, fight against illegal, unwanted and harmful content and raise awareness among end-users, parents and teachers. The fight against illegal content is focused on new types of communication as social networks. The main target groups of the project include children and young people, parents, educators, specialists, etc. More info in this website: https://www.saferinternet.cz;
- **Project E-Bezpečí:** the aim is raise awareness about prevention, education, research, intervention and risky internet behavior and related phenomena. The project is also focused on the positive use of IT in education and in everyday life in the Czech Republic. More info in this website: https://www.e-bezpeci.cz/.

4.5.3. Portugal

In Portugal there are some initiatives in order to improve internet safety of the citizens in their private life. Some of these examples include:

- **Consortium "CNCS"** organizes multiple initiatives: tips; recommendations; brochures; awareness sessions; seminars related to cybersecurity and the promotion of project; awareness and training program related to cybersecurity; national event regarding digital security area that happens once a year; general cybersecurity course and many more;
- **Two telephone lines** that help people if they have any doubts and problems related to online security, cybersecurity, bullying and unworthy exposure for young people, adults, teachers and children;
- **Online website "SegurançaNet - Navegar em segurança"** that is similar to a data base (with presentations, audio, pdfs and videos) oriented for children, schools, young people, fathers and teachers. With the initiative "Líderes digitais 2018-2019" that aims to motivate the students for the promotion of different subjects that leald to a more responsible utilization of technology and digital environment;
- **Digital security stamp (eSafety label)** that gives a certification and supports schools and aims to promote a secure environment related to digital technology as an

experience of teaching and learning;

- **Website "Ensina RTP":** this is an online website that has information (videos and short news) for multiple themes such as internet security;
- **Project "Net Segura e Viva":** this projects aims to offer a very useful repository (with information organized in Frequently Asked Questions) with advices from all areas related to cybersecurity. Besides being an online platform, Google and Deco Protest carried out multiple conferences "NETtalks" about cybersecurity in several Portugal cities. This national initiative also invites all the young people to produce some videos that shows the importance of participating in social media with safety and with respect for privacy. The videos produced by the students should promote secure internet utilization in a creative way especially in social media. The best videos became public in the online website;
- **Project "Internet Segura":** regarding the "European Safe Internet Day" that happens every year, usually in February, two companies (Microsoft and Guarda Nacional Republicana) organize an event related to this topic with a lot of activities all over the country during one week;
- **Centre "Centro de Segurança Google":** since 2018 Google gave access to "Centro de Segurança Google" in order to protect their users from threats such as spam, malicious software or virus. This center gives useful information to help Portuguese people have a better control, security and privacy about the online navigation and with this initiative Google aims to give information about many subjects especially for families;
- **APDPO Portugal - Associação dos Profissionais de Proteção e de Segurança de Dados":** this is a professional association that represents individuals and organizations that deals with protection and data security, privacy and electronic communication regulation or who hold the position of data protection officers in organizations operating in Portuguese territory;
- **Project "Miúdos seguros na NET":** this was a project that helped families, schools and communities to promote online security for children and young people. The main resources available are articles (between 2003 and 2008) and a blog.

Besides these initiatives, some companies promote the divulgation of information related to internet security in their own websites or blogs. In Portugal, there are also multiple books related to internet safety.

Nevertheless, although there are some activities related to internet safety the Portuguese government doesn't have an active role when it comes to promote dissemination activities. If anyone as a problem related to data protection or internet safety they have to search for a solution online, contact a lawyer or a person that has more knowledge related to these subjects.

4.5.4. Spain

In order to improve safety it is being implemented several responsibilities that are outlined below:

- **Safer Internet Centre Spain (SIC-SPAIN) project:** this project continues and extends the service provided by Internet Segura for Kids (IS4K). It promotes the safe and responsible use of the Internet and new technologies among children and teenagers. In line with the European BIK (Better Internet for Kids) strategy, is part of the pan-European network INSAFE of Internet Safety Centers. Based on its interoperability with the core service platform, funding, under this call, will allow the various European SICs to maintain and expand national platforms throughout the EU through the following services:
- **Awareness:** A center to raise awareness among children, parents, teachers and other professionals who work with children about the risks they may encounter through online activities about the protection of minors. Specific awareness-raising tools and services will be developed in cooperation with third parties.
- **Helpline:** Online help services that provide support for young people, parents, educators and other professionals in the field, in matters related to the protection of minors on the Internet.
- **Hotline:** Comprehensive citizen reporting service aimed at receiving and managing incidents related to illegal images and videos of child sexual abuse online.

Improvement of coordination among the consortium participants, as well as with other agents present and active in this area to create a public-private platform in which different entities coordinate to deploy awareness actions on the use of the internet in minors with an impact expanded at the national level.

5. Conclusions

Industry 4.0 is driven by disruptive technologies and the impacts of this new reindustrialization in many ways, mostly by providing operational effectiveness and challenging established business models. Although the numerous benefits in the areas connected to Industry 4.0 the fourth industrial revolution brings with it a new operational risk for connected, smart manufacturers and digital supply networks.

The interconnected nature of Industry 4.0 along with the digitalization transformation means that cyberattacks can have far more extensive effects than ever before. This means that it is imperative for organizations to fully understand the implications of these cybersecurity risks before adopting their cybersecurity strategies to be more secure, vigilant and resilient as well as fully integrated into the organizations.

Organizations need to focus and commit to a framework that: provides an integrated approach to cybersecurity, develops capabilities for threat detection to respond appropriately and proactively, capacity building in human resources for Industry 4.0 must involve a multi-pronged strategy internally in departments.

In order to achieve the actual benefits of the fourth industrial revolution, the government, and also people will need to take measures in order to adapt to the evolving risks.

The national governments and the public institutions should therefore develop programs for skill upgradation of the work force and ensure that the content of these programs are suitably modified to include all the core subjects in future. Additionally, public policies should give adequate incentives to companies to invest in this area.

When it comes to people, there is also a big need to upgrade measures for internal security for everyone. Therefore, the facilitation of education, training and skills development is equally fundamental. Also, being resilient and having a carefully posture also brings the necessity to people to become more informed because a secure world is a responsible shared by everyone.

Next, we have a list of the main barriers/difficulties faced by companies and citizens and some recommendations in order to improve cybersecurity.

5.1. Comparative analysis between all the countries

Industry 4.0 is promoting several changes all over the world in companies as well as the overall society and with this new industrial revolution the existence of attacks increased substantially. As a consequence, all the countries are facing everyday some challenges and cyber attacks that are becoming more complex and emerging more often.

Since the last few years, all of the countries are involved in organizing multiple initiatives that aims to improve the response to the main challenges of this new industrial revolution and the cybersecurity. The most common initiatives related to this theme that are present in each country are: strategical country plans; possible access to some financial support; access to information through some platforms; the existence of a public authority that help with data protection and cybersecurity in each country (such as CERTs); cybersecurity projects (public and private); and, the existence of national information (for example, guidelines, orientations,…). Despite all the initiatives that exist all of the countries still face a numerous challenges and they need to invest more and do continuously adaptations day-by-day.

Additionally, some of the most common challenges faced by the countries that were analyzed are: the lack of competences and requalification of human resources; lack of skills to detect and deal with security failures; lack of support through public authorities/organizations; cooperation between all the relevant bodies at the national level; the existence of obsolete legal foundation.

The most common cyber threats are: malware; phishing; malware; spam; ransomware attack; data breaches; and, Trojan and the most common risks/difficulties are: attacks are becoming more complex; the dependence of companies on hardware and software is growing; the increasing amount of data that needs to be protected and secure; lack of development/training is a key challenge.

Therefore, cybersecurity is now, and more than ever, a top priority for everyone and each country should include some measures and actions regarding this topic.

In the next two sections we can see the main difficulties/barriers and some suggestions/measures/recommendations/best practices in order to improve cybersecurity.

5.2. Work/Companies

The main difficulties/barriers in the countries involved in this report regarding workers and cybersecurity are:

- Attacks are becoming more complex and frequent and the main motivation behind attacks is monetization;
- Cloud security is becoming a critical issue and companies are expected to become increasingly dependent on cloud providers;
- The new rules concerning personal data protection will place considerable demands on companies;
- The importance of organizational measures (e.g. risk management) will increase in future compared to purely technical measures;
- The dependence of companies on hardware and software products represents an increasing threat;
- There are not enough incentives for security investments in companies;
- Lack of security awareness and standards;
- There are still missing or obsolete legal foundation in countries that difficult the understanding ant the application of security measures;
- Lack of safety awareness by most of the people;
- Lack of skilled/qualified cybersecurity personnel and digital competences;
- Lack of training activities to improve the knowledge and a much secure behavior by people;
- Lack of employee awareness of the cybernetic threats and IT security rules;
- Lack of a clear and concise technical guides related to cybersecurity and internet safety;
- Escalating salary requirements of skilled cybersecurity personnel can complicate the situation;
- Many separate security tools ultimately increase operational complexity and reducing visibility into overall security posture;

- Organisations often do not have a formal cybersecurity incident response team or even a named individual who is responsible for dealing with such an incident;
- There are a lack of collaboration between privacy and cybersecurity teams;
- Many companies don't have a consistent cybersecurity response plan;
- Lack of time and skilled resources necessary to implement cybersecurity plan;
- Lack of a proper budget in place to boost security capabilities;
- Obsolete IT security hardware and software;
- Lack of commitment by management along with an insufficient budget;
- Lack of involvement between all the workers in the cybersecurity strategy (if there is one);
- The inventory of assets with cybersecurity impact is not well known by all the workers in the company;
- Cybersecurity culture needs to be interiorized, security programs and measures such as processes, environment or labor risk prevention management;
- Few initiatives focused on industrial cybersecurity;
- There is no cybersecurity solutions tested enough;
- Lack of cooperation among company and government initiatives;
- Inefficient communication between the different teams because of their differences regarding their knowledge and capabilities about the use of software and hardware;
- There are activities that may endanger the systems and, as a consequence, the security of the industrial processes and facilities;
- Lack of awareness of the effects and the need of new technologies used to assure the interoperability of control systems;
- General perception that the threat is uncertain and quite unlikely;
- Espionage by modern digital means threatens national competitiveness and productivity;
- Different cybersecurity needs among different activity sectors;
- Lack of financial support for cybersecurity development;
- Shortage or absolute lack of specific standards for cybersecurity;

- Misunderstanding of the topic due to a shortage of focused training programs and public communication material;
- Wrong implementation of security solutions and technologies such as firewalls, solutions IDS/IPS, antivirus, etc;
- No relationship or agreement among authorities, business and providers in relation to cybersecurity;
- Little coordination among the different state members of the EU.

In order to **improve cybersecurity in companies we proposed some suggestions/measures/recommendations/good practices**:

- Provide training and awareness-raising to all the employees in day-to-day business;
- Passwords should always be kept secret as well as conform to a pre-defined policy. Furthermore, the password should be changed regularly;
- Use multiple authentication methods (e.g. username/password, answer to security question, Digital Certificate, smart card, fingerprint, facial recognition);
- In the settings of a Wireless LAN router it is necessary to set the encryption standard WPA or WPA-2. If the unit does not have one of these settings at least the insecure standard WEP must be used;
- Implement more security solutions and technologies such as firewalls, solutions IDS/IPS, antivirus, etc;
- Anti-virus programs and firewalls must be maintained by regular updates. This also applies to all other programs that have been installed on a computer so that known security gaps can be closed;
- External data carriers (USB sticks, external hard disks, DVDs, etc.) must not be used;
- Implement an appropriate training undergraduate and graduate programs must include topics related to cybersecurity in order to also improve the resilience of the existing industrial facilities;
- Development of procedures and policies to manage cybersecurity in complex interrelated environments;
- Creation of technical guides to improve workers knowledge;

- Develop methods and systems to detect miss functions in international networks;
- Develop solutions for the safe information exchange to coordinate the response to cybersecurity incidents in the industrial facilities environment;
- Develop techniques for detecting, following and studying incidents and to cooperate with defense organizations;
- Develop strategies that improve the information systems related to cybersecurity;
- Development of standards for several areas in the industrial cybersecurity environment such as: equipment, interoperability and management, data collection and analysis, testing and training;
- Organize events and workshop related to cybersecurity for all the stakeholders and individuals;
- Access your intranet resources via Virtual Private Network;
- Create an incident response strategy;
- Implement measures for detecting compromises and develop a cybersecurity incident response plan;
- Form an incident cybersecurity response team;
- Implement a cybersecurity risk plan in your company/organization and review it every year;
- Raise awareness about cyber threats in companies and how they affect the bottom line;
- Cybersecurity should be everyone's responsibility. Organizations must make cybersecurity a core part of business strategy and culture. Embedded in strategic decision-making and benefits from and adopts ongoing innovation. Regarding to this topic see for example: talent management; risk and security culture; and, training and awareness;
- Putting cybersecurity at the heart of an organization strategy will help maintain and even enhance the trust of consumers, regulators, media and other stakeholders related to the companies/organizations;
- Develop national strategies to help companies deal/response to their principal cybersecurity accidents if possible for each activity sector;

- Encourage new forms of partnerships and engagement by different types of stakeholders;
- The programs used in computers and technological equipment should always be updated with recent versions;
- Block access to bad websites and limited the internet control;
- Protect the Wi-fi network with a strong password and connection with data encryption and also change the default setting on the router used, changing the password to the router settings panel;
- Provide training to all the workers because the majority of the workers don't have the enough knowledge and competences to have a safer behavior all the time;
- Have backups with all the relevant data for the business;
- Involve people in all the initiatives in such a way that it may contribute with its experience and knowledge;
- Develop enablement programs, tools and techniques and reference documents that may support the performance of the cybersecurity professionals;
- Organize training initiatives, free manuals and workshops that take into account the different needs;
- Organizations should perform risk assessments periodically.

5.3. Private life

The main difficulties/barriers in your country regarding people and cybersecurity are as follows:

- Lack of security awareness and standards;
- Negligent behaviors when using internet;
- Current undergraduate school programs do not include, most of the times, cybersecurity topics;
- Although there are good initiatives, tips and hints but it does not reach the general population;
- High number of malicious software on the market;

- Inadequate understanding of the cyber-attack status;
- There are many rural areas in which not very many further training offers are possible due to the location;
- Help with difficulties is usually only available over the phone or online (with the exception of going directly to the police). A direct contact point is needed, to which people can also contact directly in case of problems;
- Regulations, policies and laws are not formulated in a user-friendly way;
- Information on the supporting materials is sometimes very difficult to find (on the internet) and it needs a faster and an easier access;
- Using a weak password, a one password to log in to multiple accounts and not changing password;
- Lack of study materials about cybersecurity;
- People easily trust email attachments;
- People share a lot of personal information on social networks;
- General lack of interest of young people about internet safety;
- Lack of awareness of the cybernetic threats and IT security rules;
- There are not many cybersecurity platforms to exchange and share information;
- Lack of financial support for promotion of internet security to people and cybersecurity development;
- Few initiatives focused on internet safety in every day life;
- Shortage educational and training programs and public materials about internet safety;
- Low digital literacy of end users;
- Basic awareness of potential threats is missing from public users;
- There is not created a cybersecurity culture;
- Lack of a clear and concise technical guides regarding internet safety and cybersecurity;
- The inventory of assets with cybersecurity impact is not well known;
- Lack of awareness of the effects and of the need of new technologies used to assure the interoperability of security/control systems;

- Misunderstanding of the cybersecurity and internet safety due to a shortage of focused training programs and public communication material;
- Policies and procedures are not suitable from the cybersecurity point of view;
- Cybersecurity risks are not integrated in tools and systems;
- There are no cybersecurity solutions tested enough;
- Wrong implementation of security solutions and technologies such as firewalls, solutions IDS/IPS, antivirus, etc;
- Little coordination among the different state members of the EU.

In order to improve the cybersecurity of citizens in their private life please find suggestions/measures/recommendations/good practices to improve:

- Use a diversity of computer protection such as virus protection, firewall and updates;
- Do not open suspicious files, be careful with bank e-mails and do not click on any link;
- People should be more careful regarding the software that will be installed (due to malware, virus,…);
- Paying more attention to the information that is given during online shopping, e.g. certificates and seals, ratings, consumer protection, "healthy distrust";
- Use encrypted connections;
- Passwords should have, at least, 8 characters and a combination of upper and lower case letters, special characters, numbers and don't re-use them;
- Be more careful with subscription systems;
- Set a good example and talk more about the use of the system and agree on rules;
- Keep a back-up of all your data;
- Implement training programs and workshops about cybersecurity for schools (undergraduate and graduate);
- The need to revise existing curricula in education regarding these subjects;
- Develop educational platform to improve people knowledge about internet security;
- Raise awareness of security measures and technologies such as firewalls and antivirus;

- Create general guides to improve people knowledge and that can be easily understood by everyone regarding their education and knowledge;
- Implement more security solutions and technologies such as firewalls, solutions IDS/IPS, antivirus, etc;
- Organize events and workshop related to cybersecurity for all the stakeholders and individuals;
- Install original software versions and update them every time you can.

6. References

Ardielli, E., Ardiellli, J. (2017). Cyber security in public administration of the Czech Republic. Sociálně-ekonomická revue: VŠB-TUO. Retrieved from: https://fsev.tnuni.sk/revue/papers/147.pdf.

Bulletin Průmyslu 4.0. (2019). Národní centrum Průmyslu 4.0. Retrieved from: https://www.ncp40.cz/files/bulletin-prumyslu-2019-04.pdf.

Bundeskanzleramt, Digitales Österreich (2012). IKT-Sicherheit. Nationale IKT Sicherheitsstrategie Österreich. Wien: BM.I Digitalprintcenter.

Bundeskriminalamt (2015): Schutz vor IT-Kriminalität. Retrieved from: https://www.finkenstein.gv.at/_Resources/Persistent/94fb6a97ff9fafa801abe506dd7eb3cc5f6f6c31/IT-Sicherheit.pdf.

Bundeskriminalamt[1] (2019): IT-Sicherheit. Retrieved from: https://bundeskriminalamt.at/news.aspx?id=43534F5A38367453614D493D.

Bundeskriminalamt[2] (2019): IT-Sicherheit: 7 Tipps für Unternehmen und öffentliche Einrichtungen. Retrieved from: https://bundeskriminalamt.at/202/Internet_kennen/files/IT_Sicherheit_7_Tipps_fr_Unternehmen_Juni2015.pdf.

Bundesministerium für Inneres (2019): Schutz vor IT-Kriminalität. Retrieved from: https://www.bundeskriminalamt.at/202/Internet_kennen/files/TippsSchutzCybercrime_Juni2015.pdf.

Bundesministerium für Digitalisierung und Wirtschaftsstandort[1] (2019). Meldestellen. Retrieved from: https://www.onlinesicherheit.gv.at/erste_hilfe/meldestellen/249337.html.

Bundesministerium für Digitalisierung und Wirtschaftsstandort2 (2019). Informationssicherheit – Industrial Security. Retrieved from: https://www.usp.gv.at/Portal.Node/usp/public?gentics.rs=PDF&gentics.pb=notvisibleposition&contentId=10007.44661.

Busch, J./Soukup, A./Dutzler, H./Loinig, M./Gorholt, A. (2015). Industrie 4.0. Österreichs Industrie im Wandel. PwC Österreich GmbH Wirschaftsprüfungsgesellschaft.

CCI (2018). Spanish Industrial Cybersecurity Roadmap 2013 – 2018. Retrieved from https://www.cci-es.org/ documents/10694/0/Roadmap+CCI+English/998bbf3c-da70-4781-b40f-83d391f0cf85.

Centro Nacional de Cibersegurança Portugal (n.d.). Retrieved from: https://www.cncs.gov.pt/.

Cyber Sicherheit Steuerungsgruppe (2018). Bericht Cyber Sicherheit 2018. Wien: Cyber Sicherheit Steuerungsgruppe.

Cyber Sicherheit Steuerungsgruppe (2019). Bericht Cyber Sicherheit 2019. Wien: Cyber Sicherheit Steuerungsgruppe.

Delloite (2017). Industry 4.0 and cybersecurity - Managing risk in an age of connected production. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiFubazxb7jAhUVolwKHUbTA7oQFjAAegQIAxAB&url=https%3A%2F%2Fwww2.deloitte.com%2Finsights%2Fus%2Fen%2Ffocus%2Findustry-4-0%2Fcybersecurity-managing-risk-in-age-of-connected-production.html&usg=AOvVaw0mfdMLmiERC-Aec8s71G2s.

Delloite (n.d.) Indústria 4.0. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwi15be5x77jAhXXAmMBHanIAvsQFjACegQIARAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fpt%2FDocuments%2Ftransportation-infrastructures-services%2Findustria4_0medidas-pt.pdf&usg=AOvVaw1WbNQpRq0JufT1IYQvw5x0.

EY (2018). Is cybersecurity about more than protection? EY Global Information Security 2018-19. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiEhdODx77jAhUZ8uAKHUcxCGIQFjAAegQIBRAB&url=https%3A%2F%2Fwww.ey.com%2Fen_gl%2Fadvisory%2Fglobal-information-security-survey-2018-2019&usg=AOvVaw2H0YlwJ2GWhy7IEPTTLYMS.

EY (n.d.) Cybersecurity for Industry 4.0 - Cybersecurity implications for government, industry and homeland security. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjWlevexb7jAhWLQUEAHTANCa4QFjAAegQIBBAC&url=https%3A%2F%2Fwww.ey.com%2FPublication%2FvwLUAssets%2Fey-cybersecurity-for-industry-4-0%2F%24File%2Fey-cybersecurity-for-industry-4-0.pdf&usg=AOvVaw3Na4d6orEYCSgwo3f3q3Ku.

EY (2018). Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017-18. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwid7Mv66ZPjAhX1QEEAHZQ-AQkQFjAAegQIABAC&url=https%3A%2F%2Fwww.ey.com%2FPublication%2FvwLUAssets%2Fey-cybersecurity-regained-preparing-to-face-cyber-attacks%2F%24FILE%2Fey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf&usg=AOvVaw0wrAdSeBMKqIg9uxX4YEC9.

Gabinete de Estratégia e Estudos (2018). A Cibersegurança em Portugal. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjNnMPwx77jAhUK-hQKHSLWDY0QFjABegQIBRAC&url=https%3A%2F%2Fwww.gee.gov.pt%2F%3Foption%3Dcom_fileman%26view%3Dfile%26routed%3D1%26name%3DTE56%2520-%2520A%2520Ciberseguran%25C3%25A7a%2520em%2520Portugal.pdf%26folder%3Destudos-e-seminarios%2Ftemas-economicos%26container%3Dfileman-files&usg=AOvVaw1CGUQIIQs7DHKQDX0E5Y-s.

Gabinete de Estratégia e Estudos (2019). Ponto de Situação da Cibersegurança em Portugal. Retrieved from: https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=imgres&cd=&ved=2ahUKEwjt3-ayzr7jAhULnhQKHaMGDGYQ5TV6BAgBEAg&url=https%3A%2F%2Fwww.gee.gov.pt%2F%3Foption%3Dcom_fileman%26view%3Dfile%26routed%3D1%26name%3DPowerPoint%2520GEE%2520-%2520Coimbra%2520(ENIAP)%25202019-01-26%2520GOB.pdf%26folder%3Destudos-e-seminarios%252Fparticipacao-em-conferencias%252F2019-3%26container%3Dfileman-files&psig=AOvVaw25PWkebk5Fiznu9PuAPFzu&ust=1563544257946449.

Federal Chancellery of the Republic of Austria (2013). Austrian Cyber Security Strategy. Wien.

Fernández, L. España y la ciberseguridad: hora de remangarse. Revista SIC,410, 27-37. Retrieved from https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomia Industrial/410/LUIS%20FERN%C3%81NDEZ%20DELGADO.pdf.

Gmv Innovation Solutions (n.d.) Cibersegurança. Retrieved from: https://www.gmv.com/pt/Sectores/SegurancaInformacao/.

Iniciativa Průmysl 4.0 (2015). Ministerstvo průmyslu a obchodu. Retrieved from: https://www.mpo.cz/assets/dokumenty/53723/64358/658713/priloha001.pdf

Kaspersky Lab. (2019). Span and phishing in 2012. Retrieved from: https://securelist.com/spam-and-phishing-in-2018/89701/.

Microsoft (n.d.). Trends in Global Cybersecurity. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwiy1tfUyb7jAhVlA2MBHagjB6QQFjAFegQIABAC&url=https%3A%2F%2Finfo.microsoft.com%2Frs%2F157-GQE-382%2Fimages%2FEN-US-CNTNT-eBook-Security-Trends-In-Global-Cybersecurity.pdf&usg=AOvVaw04gc_UHooXgmmdPcO-c-Vx.

Microsoft (2018). Microsoft Security Intelligence Report Volume 23. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwiy1tfUyb7jAhVlA2MBHagjB6QQFjACegQIBRAC&url=https%3A%2F%2Finfo.microsoft.com%2Frs%2F157-gqe-382%2Fimages%2Fen-us_cntnt-ebook-sir-volume-23_march2018.pdf&usg=AOvVaw0OJ4NbRtj5pdkCoWxfQjVP.

Ministerio del Interior España (2017). Estudio sobre la Cibercriminalidad en España. Secretaría de Estado de Seguridad. Retrieved from http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70.

Modern massive Data Analysis for Industry 4.0 Industry 4.0 at VŠB-TUO (2016). Faculty of Electrical Engineering and Computer Science VŠB-TUO Czech Republic. Retrieved from: https://www.czelo.cz/files/prezentace-pozvanky/1-Snasel-2016-e-mail.pdf.

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 (2015). Národní bezpečnostní úřad. Retrieved from:

https://www.cybersecurity.cz/data/navratil2014.pdf.

Nic.at GmbH (2018). Bericht Internet-Sicherheit Österreich 2017. Wien: nic.at GmbH.

OECD (2017). Digital Economy Outlook 2017. Retrieved from: https://www.oecd.org/internet/oecd-digital-economy-outlook-2017-9789264276284-en.htm.

PwC (n.d.). Industry 4.0: Global Digital Operations Study 2018. Retrieved from: https://www.strategyand.pwc.com/industry4-0.

Pwc (2018). Global Digital Operations 2018 Survey. https://www.strategyand.pwc.com/industry4-0#Download.

Safer Internet (2019). Ministerstvo vnitra České republiky. Retrieved from: https://www.mvcr.cz/clanek/safer-internet.aspx.

Security Strategy of the Czech Republic (2015). Ministry of Foreign Affairs of the Czech Republic. Retrieved from: http://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf.

Simio (n.d.). Industry 4.0. Retrieved from: www.simio.com/applications/industry-40.

Spanish Government (2017). National Security Strategy. Government Presidency. Retrieved from https://www.dsn.gob.es/sites/dsn/files/2017_Spanish_National_Security_Strategy_0.pdf

Spanish Government - CCN-CERT (2018). Cyber threats and trends 2018. National Cryptologic Centre. Retrieved from https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2997-ccn-cert-ia-09-18-cyberthreats- and-tendencies-executive-summary-2018-1/file.html.

Spanish Government - CCN-CERT (2019). Aproximación española a la Ciberseguridad. Centro Criptológico Nacional. Retrieved from https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/16-decalogo-ciberseguridad-2018/file.

Spanish Government - CCN-CERT (2019). Ciberamenazas y tendencias 2019. Centro Criptológico Nacional. Retrieved from https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html.

Spanish Government - INCIBE (2015). Gestión de riesgos, una guía de aproximación para el empresario. Retrieved from https://www.incibe.es/protege-tu-empresa/blog/gestion-riesgos-seguridad-informacion.

Spanish Government - INCIBE (2016). Market Trends in Cybersecurity. Spanish National Cybersecurity Institute. Retrieved from https://www.incibe.es/sites/default/files/estudios/cybersecurity_market_trends.pdf.

Spanish Government - INCIBE (2017). Decálogo de ciberseguridad empresas. Una guía de aproximación para el empresario. Retrieved from https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf.

Spanish Government - INCIBE (2018). La ciberseguridad es cosa de todos, establece buenas prácticas. Retrieved from https://www.incibe.es/protege-tu-empresa/blog/ciberseguridad-cosa-todos-establece-buenas-practicas.

Strategie kybernetické obrany ČR (2018). Národní centrum kybernetických operací. Retrieved from: http://www.acr.army.cz/assets/informacni-servis/zpravodajstvi/strategie-

kyberneticke-obrany.pdf.

Sevillano, F. (2019). Principales incidentes de ciberseguridad en España durante 2018. Retrieved from https://willistowerswatsonupdate.es/ciberseguridad/ciberataques-en-espana-2018/.

The Czech Republic opened national cyber security center (2019). National Cyber Security Center. Retrieved from: https://www.govcert.cz/en/info/events/2456-the-czech-republic-opened-national-cyber-security-center/.

Verein Industrie 4.0 (2016). Österreichischer Normungs-Kompass Industrie 4.0. Retrieved from: https://plattformindustrie40.at/wp-content/uploads/2016/12/WEB_INDUSTRIE_4.0_ES-2.pdf.

WebsiteBuilderExpert (2018). Which EU Country is Most Vulnerable to Cybercrime. Retrieved from: https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/.

Wirtschaftskammer Steiermark (2019). Cyber-security-hotline. Retrieved from: https://www.wko.at/Content.Node/kampagnen/cyber-security-hotline/index.html#unternehmen.

WKO Bundessparte Information und Consulting (2019). IT-Sicherheitshandbuch für KMU. Retrieved from: https://www.wko.at/site/it-safe/sicherheitshandbuch.html.

World Economic Forum (2019). The Global Risks Report 2019. Retrieved from: https://www.weforum.org/reports/the-global-risks-report-2019.