ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 7, No. 4, 105-113 (2022)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

A Comparison of Cyber Security Reports for 2020 of Central European Countries

Kamil Halouzka*, Ladislav Burita, Aneta Coufalikova, Pavel Kozak, Petr Františ

Department of Informatics and Cyber Operations, University of Defence, Brno, 66210, Czech Republic

ARTICLE INFO

Article history:
Received: 11 May, 2022
Accepted: 23 July, 2022
Online: 16 August, 2022

Keywords:
Cyber security
Cyber threat
Cyber-attack
Annual reports
Strategic documents
Phishing email defense

ABSTRACT

The aim of the article is to analyze the annual reports on cyber security of Central European countries, i.e. the Czech Republic, Slovakia, Poland, Germany, and Austria. The article focuses on the development of the state of cyber security, actors of threats in cyberspace, cyber threats, and the most common types of attacks. The article evaluates the objectives of cyber-attacks from the point of view of state institutions, organizations, and state and private companies, and they have listed the follow-up measures here. The method used is a critical verbal evaluation with comments and comparative analysis to find the strengths and weaknesses of the evaluated cyber security strategies and learn from them. The experiment of the cyber defense against phishing attacks is mentioned as an example of the cyber defense of individuals. The rules in Microsoft Outlook were used by filtering incoming email messages. The result is promising by stopping 88 % of phishing emails. The discussion and conclusion state that COVID-19 played a big role in the cyber security situation in countries to the analyzed documents.

1. Introduction

This review paper is an extension of the work originally presented in the 2021 Communication and Information Technologies Conference Proceedings [1].

The goal of the article is to analyze the situation in the field of cyber security, using the latest strategic documents of Central European countries, reports of Computer Emergency Response Teams (CERT), and The National Security Agencies (NSA).

The result of the analysis is somewhat pessimistic because in cyberspace we are the object of an ever-increasing number of cyber-attacks and technologically we lag behind the attackers. On the other hand, the paper mentioned a positive example of an effective defense against phishing email attacks.

Cyberspace is not limited by geographical boundaries, and its actual state can be characterized by continuing enlargement of cyber threats and cyber-attacks, whereas any of them are very serious and the form of cyber warfare is approaching.

Private companies and public organizations have to face permanently against cyber-attacks and deal with their consequences. International cooperation in cyber security is very important, countries participate by exchanging information about cyber threats and attacks and organizing joint exercises.

Cyberspace was recognized by NATO as a new domain of warfare in 2016; comparable to other domains: land, air, sea, and outer space. Appropriate policies, action plans, committees, and agencies have been adopted to ensure Member States' cyber security. Cyber headquarters and operational centers with relevant troops have been established and intensive preparations are underway against cyber threats and cyber-attacks.

The article is interesting in existing threats in cyberspace with regard to their danger and with a focus on cyber-attacks, associated with real military activities (aggression), especially from Russia.

The core of the article is the analysis of new strategic documents in cyber security in selected countries in order to look for their identical and different areas and obtain the necessary lessons learned for the development of better endurance in cyber security and preparation of suitable sources for education.

The analyzed documents often deal with phishing attacks and defense against them, because these attacks are usually at the beginning of larger cyber-attacks.

Phishing is a form of attack with the help of social engineering techniques, in which an attacker pretends to be a trusted authority in order to obtain sensitive data from the victim. The attacker thus often tries to gain the trust of the victim, who then actually communicates the necessary information or data voluntarily.

*Corresponding Author: Kamil Halouzka, kamil.halouzka@unob.cz

https://dx.doi.org/10.25046/aj070414

An example of a possible effective defense of individuals against phishing attacks is mentioned in an experiment about the application of Microsoft Outlook email client functions.

2. The Literature Review

The section presents selected comparative studies of national and international documents in cyber security and analyzes the ability of cyber defense. The analyzed studies are prepared in the form of a verbal and tabular description of the comparison, but suitable analytical procedures and models with the form of graphical outputs are also used. The aim is to identify the strengths and weaknesses of the analyzed documents and learn to improve their own approaches.

An extensive study [2] prepared for the Italian Parliament compares NATO member countries' approaches to cyber defense and finds that some countries have more proactive approaches (US, UK, France), while others have a more defensive approach (Germany, Spain). Although there are differences in the approaches to cyber defense, it must be seen that all nations are affected by NATO's unified regulatory and doctrinal framework, so that despite existing differences, national elements of cyber security can be integrated with the Alliance's command structure. The 2019 NATO Summit declared that due to the geopolitical activities of China and Russia, preparation for cyber defense had become a top priority. From the technical point of view, the NATO Communications and Information Agency (NCIA) provide capabilities necessary to the Alliance’s structures in terms of cyber defense. The NCIA administrates some of the allied networks with the NATO Cyber Security Centre (NCSC) and the NATO Computer Incident Response Capability (NCIRC). Finally, outside the NATO military command structure, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia, created in 2008, prepares reports and other documents in the field of cyber defense and, since 2010, hosts regularly cyber security exercises.

A paper [2] further analyzes the procedures and results in the cyber defense of individual NATO nations. The US approach to cyber defense is qualitatively and quantitatively different from that of most European countries. The National Security Strategy from 2017 underlines the cyber domain as one of the main future battlegrounds, and the 2018 Strategy warns against adversarial capabilities damaging American armed forces, economy, and society in cyberspace. The US Department of Defense established a Cyber Command (USCYBERCOM) in 2009, within the Strategic Command, whose commander is at the same time the Director of the National Security Agency (NSA), to ensure seamless cooperation between cyber and intelligence operations. The USCYBERCOM strategy is focused to:

1. Achieve and sustain capabilities, by anticipating technological changes and exploiting them faster and more effectively than the adversaries.
2. Create cyberspace capabilities to support operations in other warfare domains.
3. Ensure information superiority to achieve strategic impact.
4. Operationalize the cyber battlespace for agile maneuvers.
5. Expand and deepen partnerships with agencies, the private sector, and academia.

The conclusion stated that cyber defense at the NATO level is not limited to the creation of command structures and the employment of dedicated personnel, but also involves broader partnerships. The necessity of equipping NATO with cutting-edge technology led in 2014 to the formation of specific cooperation with industries operating in the cyber sector. NATO-EU cooperation was already listing the cyber dimension among priority areas of collaboration in 2016.

Analysis of the Polish National Cyber Security Strategy (NCSS) in comparison to EU strategy and regulations and to other NCSS of the countries (US, UK, France, Lithuania, and Estonia) is the content of the paper [3]. The definition of cyberspace is not enough clear and often is in the documents missing. An example is a definition by the US Department of Defense “A global domain and the information environment including networks, information technology infrastructure, data sources, telecommunications, the Internet, computers, and embedded systems”, cited in [4]. The EU security strategy in cyberspace, issued in 2013, clarified goals, responsibility roles, and tasks as achieving cyber resilience, preparing an EU Cyber Defence Policy and sources, reducing cybercrime, and developing needed technologies. In 2017, the EU published a cyber security document including initiatives in resilience to cyber-attacks and cyber security capacity, effective criminal law, and complex stability in international cooperation. The 2019 Cyber Security Act has provided a consolidated cyber security certification framework. The sanctions system Cyber Diplomacy Toolbox, allows the EU to impose targeted restrictive measures to prevent and respond to cyber-attacks. The European Parliament adopted 2021 a decision on the EU’s Cyber Security Strategy for the next digital Decade to make developed tools and services secure from the start of development, resilient to cyber threats, and able to quickly react if vulnerabilities are discovered. Poland has agreed in 2017 to its NCSS for 2017-2022 which defines cyber security as “The resilience of information and communication systems, at a given level of confidence, to any activity that compromises the availability, integrity, authenticity, or confidentiality of data, or the related services oriented by or accessible via these information networks and systems”. In 2018, Poland adopted the National Cyber Security System Act establishing coordination measures of state policy in the area of cyber security, and in 2019, in accordance to the European Union Agency for Network and Information Security (ENISA) lifecycle approach, Poland adopted its improved NCSS for 2019-2024. The final evaluation of the Polish NCSS contains recommendations for its further development, based on comparisons with the approaches of other countries.

Complex comparative analyses [5] of national cyber security strategies (NCSS) combine areas of industry, economy, technology, and defense. The study characterizes the NCSSs of countries US, UK, Japan, and EU, and describes cyber security agendas for the revision of NCSS in South Korea, by applying topic modeling. Topic modeling involves statistical techniques to identify hidden structures from a set of documents. The result is 15 agendas in the areas of Infra Stability, Protection and Response Capability, Industry and Technology, and International Cooperation. The NCSS of the US emphasized improving incident response capabilities, especially cybercrime law enforcement and investigation capabilities, and establishing cyber security governance. Similar to the US, the UK prioritized protection and response capability. On the other hand, the NCSS of Japan establishes a relatively high proportion to the cyber security industry and technology sector. Finally, the NCSS of the EU picks up international cooperation.

The article [6] is interesting in terms of currently ongoing Russian aggression in Ukraine, it includes a comparative analysis of cyber security systems in Russia and Armenia. In the introduction, the close cooperation between both countries in the economic, political, and military fields is appreciated. Two levels (legal and practical) are used to analyze cyber strategies, policies, and institutions. Key theoretical concepts in information security, information warfare, etc. are described. The cyber security definition is mentioned as "A set of technical and non-technical (policies, security arrangements, actions, guidelines, risk management) measures allowing to provide social, ethnic and cultural evolutionary modernization of the critical cyber infrastructure, as well as protection of vital interests of human, society, and state." The experiences from the military operation of Russia in August 2008 in South Ossetia and Georgia changed the Russian Defense Ministry's intention to create informational troops, whose functions include all aspects of information warfare, from psychological operations and propaganda to security of computer networks and cyber-attacks on the enemy's information systems. Cyberspace in Armenia is rather liberal. The principle is "allowing everything that is not prohibited" when prohibited are direct and clear criminal acts. Similar to the Russian approach, the Armenian side uses a wider concept of information security without specifying the concept of cyber security.

3. Analysis of selected cyber threats

The aim of the section is not to list every possible cyber threat. A brief introduction into cyber threats was presented in [1]. The initial point of an intrusion into a system by attackers is a very often successful phishing campaign. Therefore, the aim of the section is to analyze phishing from several points of view, especially phishing associated with real military actions.

Phishing campaigns usually have the following aims:

1. They try to lure sensitive data from end-users and misuse obtained data. It can be personal data, corporate data, or governmental data.
2. The goal is to infect a computer for later abuse by adding malicious attachments to e-mails or creating links leading to fake malicious websites, thus computers may become part of a botnet, be infected with ransomware, contain a key logger, etc.

In addition to classical phishing attacks that target as many victims as possible, there are also other types of phishing [7]:

- Spear phishing attempts are targeted toward specific individuals or groups of individuals. They may include the recipient's name, position, or company. IT administrators can be great targets because of the level of access they usually have within the organization.
- Whaling targets high-level employees, like executives or directors. They typically have access to the most valuable information in a company, making them appealing targets for attackers.
- Clone phishing is typically targeted at a small group of people. Attackers copy a legitimate email that has previously been sent by a trusted organization but replace links to redirect the victim to a malicious site.

Phishing attacks usually take place over email but attacks using other mediums have also been observed. Smishing is the text message (SMS) version of phishing attacks. Vishing is phishing that is executed via telephone (Voice).

Phishers usually exploit three types of events. Firstly, phishing campaigns misuse long-term affairs such as humanitarian aid to countries affected by perpetual fighting, or an education for African children. Secondly, regularly occurring events are commonly exploited by phishers, e.g., holidays, summits (EU, NATO), or elections. Thirdly, phishers take advantage of current events, e.g., outbreaks of fighting, rapid changes in the financial market. A common characteristic of phishing is the feeling which is intended to evoke in people. This effect encourages users to react, and as a consequence, it increases the effectiveness of phishing. The feelings they usually evoke can be: sympathy, fear, joy from prize, urgency, stress, and patriotism.

Patriotic or nationalist hackers see themselves as irregular soldiers, or conscripts fighting a war for their country, a form of cyber militia. Their attacks are motivated by strong feelings of patriotism and nationalism, reflected in the language and rhetoric used. The actions of the patriotic hacker may result in serious damage to targeted systems [8].

In the case of intensified Russian military activities there are 2 possible vectors of cyber-attacks:

1. From Russia - attacking information systems (IS) of the enemy and enemy sympathizers.
2. Against Russia - attacking IS of Russia and Russian sympathizers.
3. From all around the world - attacking IS of adversaries and their sympathizers, depending on which side the attackers are inclined towards.

Phishing campaigns related to current events in the context of Russian activities may use the terms humanitarian aid, solidarity, support for the fight, signing petitions, and providing accommodation to refugees. The impact of such phishing campaigns tends to be personal or sensitive data leakage, payment card details leakage, subsequent misuse of the leaked data, and payments to the attackers' accounts instead of accounts for humanitarian purposes, computers infected with malicious codes, and their subsequent abuse for adversary activities.

Phishing can also contain fake actual news. It aims to manipulate people across the board and significantly influence their behavior. This method is often used in state information operations to weaken an adversary or, on the contrary, to strengthen the confidence of its own population in the government aggressive activities. Such phishing messages include fake news of invasion, troop movements, shortages of goods in shops, fuel shortages, shutdown of gas supplies by Russia, power cuts due to gas shortages, etc. On the other hand, fakes news about military successes, humane treatment of the enemy, liberation of the population from oppression and other justifications for fighting are then used to influence the confidence of the population in the governmental aggressive decisions.

In a widespread phishing campaign against an adversary, the consequences can be immeasurable - population panic, buying frenzies, and stockpiling of resources. With an unexpectedly height public reactions, we can expect repercussions in all sectors. Particularly for the communication and information area, we can expect disruptions or even unavailability of services or entire information systems, e.g., disruption of electronic banking, unavailability of telephone lines, unavailability of web information portals, and unavailability of bank card payments. Additionally, if the critical infrastructure is affected, the functioning of the state and human lives may be endangered.

Another frequent impact of successful phishing can be a ransomware infection or a data leakage. Both encrypted data as well as data leakage are common subject of a ransom. It is not recommended to pay the ransom due to uncertainty as to whether the attackers keep their promises. In case of encrypted data there is a risk the attackers will not send decrypting keys after payment or the keys will not work properly. In case of the data leakage there is a risk the attackers will sell stolen data to a third party after payment anyway. A new approach to ransomware has emerged. Anybody can buy ransomware as a service for a fee or a shared ransom. Effects of ransomware on information systems range from denial of service, and data loss, to loss of reputation, and bankruptcy. The consequences of an infection in the critical infrastructure are immense, as it was mentioned above.

A new and additional set of phishing related to Russian military activities and the current situation in Russia and Ukraine is emerging. This new set has specific keywords in conjunction with the words Russia or Ukraine, e.g., solidarity, refugees, war victims, aid, fundraising, petition, cohesion, but also shortages in connection with the words gas, wheat, energy, building materials, etc. Such keywords can be effectively used in individual defense against phishing attacks which is described in section 5.

There are two main approaches to reduce a rate of success phishing. From a technical point of view we can increase detection capabilities. From a non-technical point of view we can reduce a phishing risk by spreading security awareness.

Firstly, technical measures work reliably but they need to be updated and adapted regularly. It is very difficult to respond adequately to rapidly changing links in phishing emails. Links in emails are changed by attackers faster than it would be possible to manually respond to them in real time. Manually adding malicious links into blacklists is an inefficient human-consuming and time-consuming method. A more appropriate method is to automatically and regularly download updated blacklists from selected trusted sources that deal with this issue.

Blocking selected file types (.dll, .exe, .js, .msi, .reg...) is a very effective method. However, if we block files types inappropriately, users will not receive their attachments needed for their work. For example, .pdf files may contain links to malicious sites, but it is not possible to block all .pdf attachments in bulk. The solution is a technology that runs selected suspicious attachments in a sandbox. The technology automatically evaluates the behavior of the system after the attachment is launched and if everything works normally, the email is sent to the user's mailbox. If malicious behavior is found, the user is informed about the situation and the email is sent with a modified attachment, for example an attachment is converted from a .pdf file to an image (.png, .jpeg...). This prevents the user from clicking on the malicious link or executing the malicious code, but the information from the attachment is still delivered to the user.

Another technical measure is blocking emails based on sets of keywords. The sets must be chosen with caution, taking into consideration the possibility of a high number of false positives. In long-term tuning, this method achieves a very good level of reliability. The practical application of this technical measure is discussed in section 5.

Secondly, there are many methods of security awareness spreading. For example, users can attend specialized seminars and courses to learn how to recognize phishing. However, these trainings are usually only once a year due to financial and time constraints. In addition, this approach is not proving to be as effective as expected. In practice, short training sessions followed by testing employees with mock phishing is more effective method. Metrics such as the number of tricked users, the most clicked links, types of attachments launched, and, of course, leaked passwords are analyzed and final reports are published within the organization. Modified mock phishing emails are then repeated at random time intervals and repeat clickers are then invited to additional trainings. According to [9], it is advisable to increase the difficulty of mock phishing up to 3 levels:

- Tier 01 – generic type of mass phishing attacks. Emails include misspellings, poor graphic design, and well-known scams.
- Tier 02 – more professional or more personalized phishing attacks. Emails contain victim's name and are work related.
- Tier 03 – targeted attack and customized for selected high-risk groups.

The best results for reducing the success rate of phishing attacks are achieved through a combination of technical measures and educated users. It depends on the availability of resources, how many security technical tools are used and to what extent users are trained and tested.

4. Cyber Security Status Report

The aim of the next section is to analyze the cyber security status reports of the Czech Republic, Slovakia, Austria, Germany, and Poland for the year 2020. Cyber security status reports are issued by these countries in the second half of the year. For this reason, the reports for 2020 were prepared. The reports for 2021 were not available at the time of writing. The aim is to assess the problems that each country has in the area of cyber security, to evaluate the frequency of cyber-attacks or incidents, and to evaluate the most common types of attacks.

4.1. Czech Republic

A report on the state of cyber security in the Czech Republic has been published by the National Cyber and Information Security Agency (NÚKIB) [10]. The year 2020 in the Czech Republic was characterized by an increase in the number of cyber-attacks against Czech institutions, organizations, and companies in all sectors. In 2020, the NÚKIB recorded a more than double increase in incidents compared to 2019. The most common types of attacks in the Czech Republic in 2020 were spam (59%), phishing (16%), and scanning (12%). Respondents ranked ransomware (19%), DoS / DDoS attacks (19%), spear-phishing emails (14%) and attempts to exploit vulnerabilities (13%) as the most serious attacks. Cybercrime has long been among the most serious threats to the country's cyber security. In 2020, cybercrime emerged in the form of ransomware attacks, which hit the Czech healthcare sector to a large extent.

The most serious threats to the Czech Republic's cyber security include state-sponsored actors in cyberspace and cybercrime. A new development is Ransomware as a Service (RaaS), which is a service provided by ransomware developers to other hackers, usually for a share of the ransom, and they do not care about the actual penetration of organizations' systems.

In terms of personnel and financial security, a large number of organizations in the country have been facing a lack of experts and insufficient budgets in the field of cyber security. This situation was more evident in the government sector than in private companies. Almost none of the interviewed organizations had all cyber security positions filled. More than half of the organizations cited inadequate salary conditions as the main factor.

In terms of training, the NÚKIB placed a strong emphasis on the training of state administration employees and trained more than 22,000 state administration employees, employees of the Army of the Czech Republic, and medical and prevention personnel from the education sector in e-learning courses during 2020.

In the report on the state of cyber security in the Czech Republic, much attention is paid to the security of 5G networks. In 2020, the Prague 5G Security Conference was organized jointly with the Office of the Government and the Ministry of Foreign Affairs, the main topic was the risks associated with building 5G infrastructure. The main outcome was the presentation and the launch of the Prague 5G Security Repository, a virtual library designed to share legislative, strategic and other tools that states adopted in the past year in the area of 5G network security.

4.2. Slovak Republic

A report on the state of cyber security in Slovakia has been published by the National Security Authority of Slovakia [11]. The report is divided into seven main parts. The focus is on the description of actors in cyberspace, namely inexperienced attackers (script-kiddies), cybercriminals motivated by financial gain, state-sponsored groups, hacktivist groups interested in obtaining sensitive and classified state information, and cyberterrorists, whose role is mainly to hit civilian and military targets with cyber-attacks.

Furthermore, the report focuses on the categories of cyber security incidents (monitored by SK-CERT) and threats. The most detected and reported incidents were in the "Unwanted Content" category and the most solved incidents were in the "Attempted Intrusion" category. The most frequent threats in Slovakia were phishing campaigns (Microsoft tech support scam, abuse of Slovak Post), malicious code distribution (mainly ransomware – the attack on Slovak TV Senzi, which refused to negotiate with the attackers and filed a criminal complaint), data leaks (leak of 130,000 personal data of patients tested on COVID-19) and vulnerability exploitation.

The Slovak cyber security status report also goes into detail on cyber threats targeting specific organizations, such as healthcare, public administration, banking, electronic communications, and digital infrastructure, and energy. The report pays great attention to, among other things, issues related to national and European legislation, the preparation of the National Cyber Security Strategy, national and international activities and cooperation, cyber security audits, and cyber defense exercises (Table-Top exercise BlueOLEx 2020 and Cyber Coalition 2020). Among other important security actions that were implemented in Slovakia was the establishment of the Competence and Certification Centre for Cyber Security. The aim of this center is to assist the National Security Authority in fulfilling its professional tasks in the field of cyber security, protection of classified information and cryptographic protection, and trust services in the public interest.

4.3. Austria

The Cyber Security Status Report was prepared by the Cyber Security Steering Group (CSS) in accordance with the Austrian Cyber Security Strategy (ÖSCS) [12]. As in the above-mentioned countries, the number of malware attacks on computer systems and networks in Austria increased over the past year. A large part of Austria's annual report was devoted to the impact of the SARS-CoV-2 pandemic on cyber security. At the beginning of the pandemic, many companies were forced to change to a home office for which they were unfortunately not prepared. Companies were often forced to reduce their own cyber security to allow their employees to work away from their offices.

There has been a sharp increase in the number of fraudulent sites, seemingly related to Covid-19, designed to phish or spread malware. The authors of these scams demanded from victims to pay them USD 4 000 in bitcoins. If they didn't pay, they were told their families would be infected with the coronavirus. Other frauds involved changing delivery times for shipments due to the pandemic. Opening the link and/or file contained in the message caused the installation of malware (including AZORuIt, Emotet, Nanocore RAT and Trick-Bot) on the target computer. There were major problems in Austria with data leaks from corporate computer networks, where attackers demanded a ransom for its return. Several waves of DDoS attacks occurred during the reporting period, mainly against banks, the financial sector and Internet Service Providers (ISPs). The aim of these attacks was not only to deny services but also to blackmail their victims.

A large part of the report is devoted to cyber security cooperation between Austria and European Union, United Nations, NATO, and other important committees and forums. Equal attention is paid to clarifying national cyber security actors such as Cyber Security Centre, Cybercrime Competence Centre, CIS and Cyber Security Centre, Austrian Armed Forces Security Agency, and many others.

The Austrian Cyber Security Status Report is the only one that does not provide any specific numbers of cyber security breaches, as all values were given only as percentages.

4.4. Poland

A report on the state of cyber security in Poland has been published by CERT (Computer Emergency Response Team) Poland [13]. In the period under review, 60.7% more cyber security attacks were registered than in the previous year. The most common type of incident was phishing, which represented 73% of all cyber-attacks. In March 2020, Poland released a list of dangerous websites (List of warnings), which had a significant impact on the number of phishing attacks recorded. These phishing attacks were targeted at obtaining e-banking authentication details, payment card details, email account access details, and social media accounts.

Cybercriminals used, for example, Facebook messages with sensationalist headlines, fake SMS messages, and WhatsApp messages for this purpose. There also was an increase in unwanted messages (spam) on mobile platforms (especially Android). CERT Polska focused on analyzing IP addresses localized in Poland that were used for Distributed Reflective Denial of Service (DRDoS) attacks. For that purpose, a list of poorly configured services that were the most frequently used for DRDoS attacks was published.

As in previous years, disinformation campaigns related to attacks on information portals and accounts of Polish politicians were recorded in Poland. Criminals used the accounts to publish fake information aimed at, for example, reducing the trust of public officials or spreading negative information about the US military in Poland.

The report on the state of cyber security in Poland also contains a large number of practical examples (in text and graphic form) of the most common form of malicious software distribution, fake job offers on Facebook, fake parcel post services, fake bills for the advertisement and others. The extensive chapter is completed with recommendations on how to avoid infection.

4.5. Germany

In Germany, the Federal Office for Information Security (BSI) monitors IT security threats [14]. According to the report on the state of cyber security in Germany, the trend of attackers using malware to launch mass cyber-attacks continued during the period. The malware was the most commonly used attack and was responsible for cyber-attacks on individuals, private companies, government offices, and other institutions. The malware was also used to launch targeted attacks against pre-selected victims.

A large amount of personal data was also leaked, which unfortunately also included data on patients and their clinical records (this data was unfortunately freely accessible online). The reporting period also showed the emergence of a number of vulnerabilities in software products that attackers were able to exploit to spread malware, attack or steal data. Some of these vulnerabilities were assessed as critical.

There were targeted attacks on financially powerful victims such as car manufacturers and their suppliers, attacks on airports and airlines, and on less known high-income companies. Attackers also used increasingly the "human factor" as a starting point for attacks that use social engineering to gain an entry point for further attacks. Also in Germany, the COVID-19 pandemic was often used for cyber-attacks.

One example was the large-scale waves of spam offering fake advice about the coronavirus. These emails urged company employees to post personal or company information on copies of official websites. Cybercriminals designed these sites similar to (government) websites.

One of the biggest threats mentioned in the annual report was Emotet. Emotet was used to create a cascade of other malware attacks that can culminate in targeted ransomware attacks on selected, usually wealthy victims. Critical BlueKeep and DejaBlue vulnerabilities in Windows Remote Desktop Protocol were also published. This vulnerability allowed attackers to execute malicious code, including malware, on unpatched systems.

4.6. Brief comparison of cyber security reports

As noted, each of these states issues an annual report on the state of cyber security. Each state publishes information in this report at its own discretion, and there is generally no rule specifying what the report must contain. The following table (Tab. 1) shows a basic comparison of the cyber security status reports of these states, with information from the United States and the United Kingdom reports added for comparison.

While for the UK the Annual Review 2020 report [15] issued by The National Cyber Security Centre was used for comparison, in the US two reports were used, namely the NSA cybersecurity year in review for 2020 [16] and the FISMA FY 2020 Annual Report containing The State of Federal Cybersecurity [17]. In the case of the United States, both reports are very general and contain little specific information compared to other reports.

Tab. 1 shows who is responsible for the policy/strategy in the countries listed, when the first National Cyber Security Strategy (NCSS) was issued, and when the last update was made or the period of validity. The table also shows important aspects of each cyber security status report, when the focus was on new IT security measures in organizations and the status of security-focused budgets, which were heavily affected by the COVID-19 pandemic and the resulting increase in security and budgetary measures. Cyber security Status Report lists the most frequent incidents during the reporting period, where the most popular type of incident was phishing. The second most reported incident type was ransomware. There was also mentioned a large increase in malware on mobile platforms in 2020. An important part of cyber preparedness is also participation in international cyber exercises, which have also been affected by the COVID-19 pandemic. Even though the Locked Shields 2020 and Cyber Europe 2020 international exercises were canceled in 2020 due to the pandemic, individual countries have organized several cyber security exercises that are important for training defense against cyber-attacks. The table also shows that national security authorities support cyber security education in the form of cooperation with schools (e.g. cyber security information cards for schools), business (e.g. various levels of consulting for business customers), and voluntary sector (e.g. guidance on cyber security).

Table 1: Basic comparison of the cyber security status reports

	USA	GBR	Germany	Polland	Austria	Slovakia	Czech Republic
Policy/strategy responsibility	CISA	NCSC	BMI	MDA	BMEIA	NBÚ	NÚKIB
First NCSS	2003	2011	2011	2009	2009	2008	2012
Actual NCSS	2018	2022 - 2030	2021	2019 - 2024	2021	2021 - 2025	2021 - 2025
New IT security measures in companies	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security budget in companies	Not mentioned	Increase	Not mentioned	Increase	Increase	Increase	Increase
The most frequent incident reported during the reporting period	Spear-phishing	Phishing	It's not specified. The report generally mentions malware and phishing.	Phishing	Phishing	Phishing	Spam
The second most frequent incident reported during the reporting period	Not mentioned	Ransomware		Ransomware	Not mentioned	Ransomware	Phishing
Participation in cyber exercises	Not mentioned	Not mentioned	Yes / Crossed Swords 2020, Common Roof	Yes / KSC-EXE 2020, Capture The Flag, Hack-A-Sat	Yes / Crossed Swords 2020, Common Roof	Yes / BlueOLEx, Cyber Coalition	Yes / Cyber Coalition
Cyber security education in companies	Yes / improving	Yes / improving	Yes / improving	Yes / improving	Yes / improving	Yes / improving	Yes / improving
Cyber security incidents in 2020	30819	723	419 (mentioned only critical infrastructure)	10420	Not mentioned	3793	1267

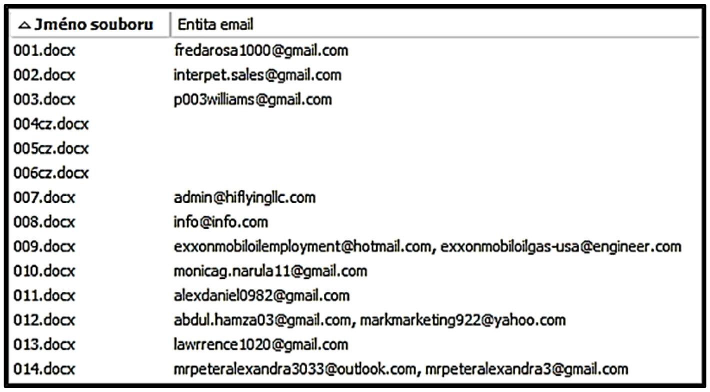
The latest comparison is on the number of cyber incidents in 2020. It is difficult to compare the number of reported cyber incidents from the cyber security status reports of these states because each state reported these cyber incidents in the form of the most frequent, most serious, reported or resolved cyber incidents. For this reason, a clear comparison of the number of cyber incidents is not possible. Austria, for example, did not mention the number of cyber incidents at all in its cyber security report.

5. Cyber Defense of the Individual

This part of the article focuses on the cyber defense of individuals against phishing attacks. The result of research on the phishing attacks in the previous two years has collected the set of almost 400 phishing emails that were sent to the email inbox of one of the authors. The emails were the subject of analysis, the necessary knowledge was obtained, and that was used for the cyber defense of individuals. The functions of the mail client MS Outlook were used for individual defense.

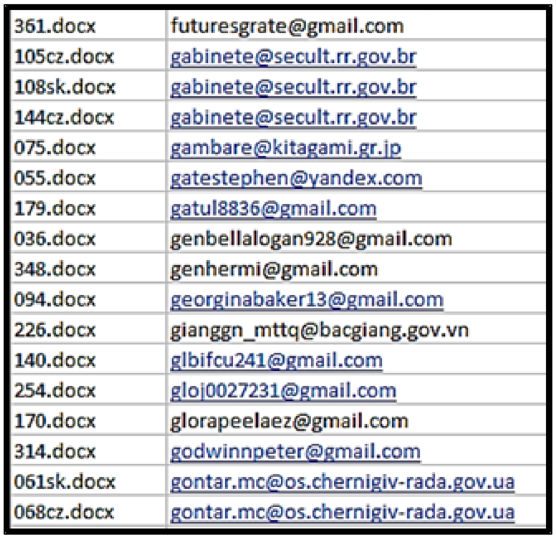
One of the options for individual cyber defense against phishing emails is the possibility to block all email addresses detected from the content of phishing email messages. Email addresses were obtained from phishing emails using the intelligent function entities extraction of the Tovek [18] software, using the Tovek Agent module, see Fig. 1. The first column in Fig. 1 is the file name (phishing email) and the second column includes email addresses.

A total of 365 emails were analyzed, from which 511 email addresses were extracted, of which only 17 were reused; i.e., 3%. It is obvious that blocking that volume of addresses with such low efficiency would not be effective in terms of protection against phishing attacks, see Fig. 2; normalized email addresses in the Excel table, and ordered.



△ Jméno souboru	Entita email
001.docx	fredarosa1000@gmail.com
002.docx	interpet.sales@gmail.com
003.docx	p003williams@gmail.com
004cz.docx	
005cz.docx	
006cz.docx	
007.docx	admin@hiflyingllc.com
008.docx	info@info.com
009.docx	exxonmobiloilemployment@hotmail.com, exxonmobiloilgas-usa@engineer.com
010.docx	monicag.narula11@gmail.com
011.docx	alexdaniel0982@gmail.com
012.docx	abdul.hamza03@gmail.com, markmarketing922@yahoo.com
013.docx	lawrrence1020@gmail.com
014.docx	mrpeteralexandra3033@outlook.com, mrpeteralexandra3@gmail.com

Figure 1: Entity extraction



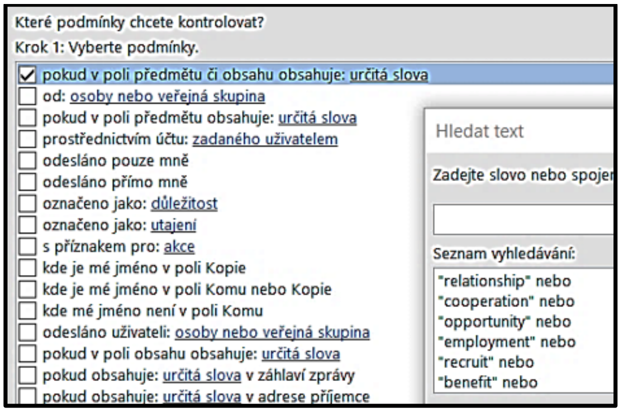
361.docx	futuresgrate@gmail.com
105cz.docx	gabinete@secult.rr.gov.br
108sk.docx	gabinete@secult.rr.gov.br
144cz.docx	gabinete@secult.rr.gov.br
075.docx	gambare@kitagami.gr.jp
055.docx	gatestephen@yandex.com
179.docx	gatul8836@gmail.com
036.docx	genbellalogan928@gmail.com
348.docx	genhermi@gmail.com
094.docx	georginabaker13@gmail.com
226.docx	gianggn_mttq@bacgiang.gov.vn
140.docx	glbifcu241@gmail.com
254.docx	gloj0027231@gmail.com
170.docx	glorapeelaez@gmail.com
314.docx	godwinnpeter@gmail.com
061sk.docx	gontar.mc@os.chernigiv-rada.gov.ua
068cz.docx	gontar.mc@os.chernigiv-rada.gov.ua

Figure 2: Extracted email addresses

Another possibility of individual cyber defense against phishing emails is the use of rules in the MS Outlook client to filter incoming emails. We have chosen rules for email detection based on the occurrence of keywords in the subject and content of the email message. The keywords were taken from the results of research on phishing emails, published in the article [19]. Keywords that characterize the particular email segment:

- BUSINESS (investment, project, contract, business, intention, export, service, product, partner, relationship, cooperation, employment, recruit, benefit, inquiry);
- FUND (deposit, fraud, scam, credit, compensation, inheritance, award, sum, price, prize, claim, winning);
- TRANSFER (transfer, property, gold, diamonds, box, packet, shipment, airport, bank, payment);
- CHARITY (charity, donate, Christ, God, sister, brother, promise, illness, disease, hospital, cancer, widow);
- OTHERS (offer, loan, communicate, message, response, contact, friendship, package, undelivered).

The rule is easily set up using the wizard in MS Outlook see Fig. 3. An overview of the rules is shown in Fig. 4.



Které podmínky chcete kontrolovat?

Krok 1: Vyberte podmínky.

☑ pokud v poli předmětu či obsahu obsahuje: určitá slova
☐ od: osoby nebo veřejná skupina
☐ pokud v poli předmětu obsahuje: určitá slova
☐ prostřednictvím účtu: zadaného uživatelem
☐ odesláno pouze mně
☐ odesláno přímo mně
☐ označeno jako: důležitost
☐ označeno jako: utajení
☐ s příznakem pro: akce
☐ kde je mé jméno v poli Kopie
☐ kde je mé jméno v poli Komu nebo Kopie
☐ kde mé jméno není v poli Komu
☐ odesláno uživateli: osoby nebo veřejná skupina
☐ pokud v poli obsahu obsahuje: určitá slova
☐ pokud obsahuje: určitá slova v záhlaví zprávy
☐ pokud obsahuje: určitá slova v adrese příjemce

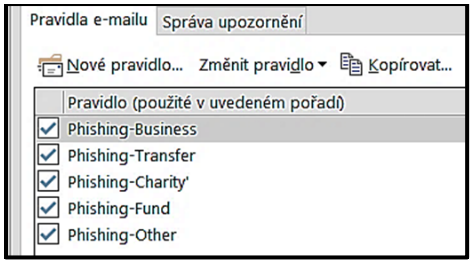
Hledat text

Zadejte slovo nebo spojen

Seznam vyhledávání:

"relationship" nebo
"cooperation" nebo
"opportunity" nebo
"employment" nebo
"recruit" nebo
"benefit" nebo

Figure 3: Setting email message filtering rules



Pravidlo (použité v uvedeném pořadí)

☑ Phishing-Business
☑ Phishing-Transfer
☑ Phishing-Charity'
☑ Phishing-Fund
☑ Phishing-Other

Figure 4: Overview of email message filtering rules

During the debugging of how the rules work successfully, conditions in the rules were continuously updated, on the basis of which emails were not excluded from phishing (manuscript, conference, journal, editor, publication, System NEWS, Smart Cities, Computerworld, Reuters, webcast, Deloitte, identity, Sophos). These are keywords associated with activities associated with publishing scientific articles and offering professional events. The phishing messages are stored in a dedicated folder; based on the set rules. The testing phase was realized for two weeks and after that followed the four weeks experiment.

The results of the experiment were evaluated, see Tab. 2. There were recognized two types of mistakes:

1. Uncaptured (undetected) phishing email (false negative).
2. Phishing erroneously detected, means the correct email that was included in the Phishing folder (false positive).

All seven false-negative messages were phishing, of which 2 in Czech. Content included in groups OTHERS-3, FOND-2, BUSINESS-1, TRANSFER-1, and CHARITY-0.

Table 2: Statistics of the experiment

Phish-email / Week	1	2	3	4	Σ
Total number	27	36	31	26	120
-of which undetected	1	2	2	2	7
Erroneously detected	1	3	1	2	7
Total detection errors	2	5	3	4	14

On the contrary, none of the false-positive messages was phish; they contained corporate information about the event or information about some facts. They contained some of the keywords for inclusion in the phishing folder and then included necessary changes in phish detection rules.

It is also worth mentioning that the number of phishing emails in the experiment increased, compared to the previous ones, by almost 50%. The result of the experiment is promising, correctly captured phishing emails account for 88%.

The described method of defense against phishing attacks can be recommended because it can be individually customized and is easily adjustable. It should be noted that phishing emails are an individual matter. Several years of experimentation have confirmed that the content and extent of phishing attacks against the same person vary a little.

6. Discussion and Conclusion

Cyber security is unfortunately a much-used term these days, and because of the current political situation (Russia-Ukraine conflict), it is not expected that there will be any return to the good old days. The information published in this article is not yet influenced by this conflict, but the main role in it is affected by the Covid-19 pandemic. This pandemic has greatly affected the behavior not only of attackers in the Internet world but also of ordinary users who have started to take the problem of cyber security at least a little bit seriously.

It is interesting to see how the countries mentioned in this article declare their cyber security challenges, and it is important to mention that a detailed comparison of the annual reports was almost impossible in terms of frequency of cyber incidents, structure, and content, as each national report had a different way of assessment. Comparable information was aggregated into Table 1, which shows information regarding the number of cyber incidents, where the United States clearly dominated, as well as the most frequent incidents encountered by those states, and information regarding support for training and cyber exercises.

Individual reports described each type of attack, with one of the most common being ransomware attacks, which caused hundreds of millions of euros in damage to various state and non-state institutions during the pandemic. Cyber-attacks have most often targeted critical infrastructure, the public sector, the financial sector, industry, healthcare, and, unfortunately, education.

As already mentioned, COVID-19 played a big role in cyber security in 2020, clearly showing how adaptable cybercriminals are. The most common methods of cyber-attacks that were recorded during COVID-19, according to the annual reports of the mentioned countries, were the following attacks:

- Fake news or links to fraudulent sites with disinformation such as there is a miracle cure for COVID-19.
- Fake messages or phone calls pretending to be from companies like Microsoft or Google Drive. Their goal was to extort a password from the user under the premise of offering help or threatening to cancel the account.
- Messages about non-existent packages being delivered.
- Fake appeals to donate money.
- Emails that appear to be from a medical organization.

Subsequently, the biggest threats according to the annual reports include:

- Ransomware - demanding a ransom to recover encrypted data.
- Threats associated with personal data - data breaches/leaks;
- Malware - malicious programs.
- Disinformation - spreading misleading or false information.
- Harmless threats - human error and system misconfiguration.
- Availability and integrity threats - attacks that prevent system users from accessing their information.
- Threats related to electronic mail - e-mail attacks.
- Supply chain threats - attacks (e.g. on service providers) to gain access to customer data.

The main contribution is analysis of cyber security documents, their comparison and evaluation in individual areas. There is a benefit for learning and developing a perspective on security requirements that follow from the findings of the analysis. An experiment was carried out on the subject of phishing, which, based on the use of MS Outlook rules, was able to significantly reduce phishing emails. This approach is original.

Acknowledgment

The article represents the results of the research in cyber security of the project [20] at the University of Defence in Brno, Faculty of Military Technology, Department of Informatics and Cyber Operations.

References

[1] K. Halouzka, L. Burita, P. Kozak, "Overview of Cyber Threats in Central European Countries," in 2021 Communication and Information Technologies Conference Proceedings, Liptovsky Mikulas, Armed Forces Academy of General Milan Rastislav Stefanik in Liptovsky Mikulas, 81–86, 2021.

[2] A. Marrone, E. Sabatino, "La difesa cibernetica nei Paesi NATO: modelli a confront, Cyber Defence in NATO Countries: Comparing Models," Rome, Senate, 2020, [Online]. Available: http://www.parlamento.it/documenti/repository/affariinternazionali/osservatorio/approfondimenti/PI0164.pdf.

[3] A. Jacuch, "Comparative analysis of cyber security strategies, European union strategy and policies. Polish and selected countries strategies", Online Journal Modelling the New Europe, **37**, 102–120, 2021.

[4] US Congressional Research Service, Defence Primer: Cyberspace Operations, https://sgp.fas.org/crs/natsec/IF10537.pdf.

[5] M. Song, D.H. Kim, S. Bae, S.-J. Kim, "Comparative Analysis of National Cyber Security Strategies using Topic Modelling," in International Journal of Advanced Computer Science and Applications, **12**, 62–69, 2021, doi:10.14569/IJACSA.2021.0121209.

[6] R. Elamiryan, R. Bolgov, "Comparative analysis of cyber security systems in Russia and Armenia: Legal and political frameworks," in Digital Transformation and Global Society, **858**, 195–209, 2018, doi:10.1007/978-3-030-02843-5_16.

[7] J. Fulmer, "Complete Guide to Phishing Attacks: What Are the Different Types and Defenses?," 2022, [Online]. Available: https://www.esecurityplanet.com/threats/phishing-attacks/.

[8] M. Dahan, "Hacking for the homeland: patriotic hackers versus hacktivists," in ICIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security, 51–57, 2013.

[9] SANS, "Phishing Strategic Planning Document," 2022.

[10] NÚKIB, "Zpráva o stavu kybernetické bezpečnosti za rok 2020," 2021.

[11] NBÚ, SK CERT, "Správa o kybernetické bezpečnosti v Slovenskej Republice za rok 2020", 2021.

[12] Cybersecurity Report 2020, Austria, Vienna, 2021.

[13] NASK PIB/CERT Polska, "Security landscape of the Polish Internet, Annual report from the actions of CERT Polska 2020," 2021.

[14] Federal Office for Information Security, "The State of IT Security in Germany in 2020," 2021.

[15] National Cyber Security Centre, Annual Review 2020, UK, 2021.

[16] NSA United States of America, NSA cybersecurity year in review for 2020, 2021.

[17] FISMA FY 2020 Annual Report to Congres, The State of Federal Cybersecurity, Federal Information Security Modernization Act of 2014, 2021.

[18] Tovek, "The text analytical software TOVEK," 2022, [Online]. Available: https://www.tovek.cz.

[19] L. Burita, P. Matoulek, K. Halouzka, P. Kozak, "Analysis of phishing emails," in AIMS Electronics and Electrical Engineering, **5**(1), 93–116, 2021.

[20] DZRO FVT 2_KYBERSILY, Research project Cyber forces and resources, University of Defence, Faculty of Military Technology, Brno, Czech Republic, 2021.