Ing. Miroslav Čermák
Police Academy of the Czech Republic in Prague
PhD student

Key Factors Affecting the Increase in Cybercrime

Introduction

This paper is based on an analysis of security reports issued by companies offering security solutions, seeking common characteristics such as the type and frequency of occurrence of threats and used attack vectors, in-depth interviews with information and cyber security managers operating in the private and public spheres along with, last but not least, personal experience with the investigation of serious cyberattacks executed against clients of the largest Czech banks over the last few years.

In the last two decades, there have been several, at first glance all-positive, transformations in the field of information technology, such as consolidation and virtualization of infrastructure, digitization of documents, data transfer to clouds, robotization of processes, advent of artificial intelligence, and the possibility of remote access to organizations' systems and data from any device, at any time, and from anywhere. Each of these changes in itself would not have to worry us at all, but together they can and do create favourable conditions for committing serious cybercrime and thus threaten most households and organizations in the Czech Republic, as these are increasingly dependent on information technologies, consuming or providing their services through them.

The development of information technology and architecture since the second half of the 1990s has essentially predetermined the current form of cyberattacks. Households and companies, their equipment, as well as the infrastructure itself, are victims of widespread or targeted cyberattacks,[1] which are becoming more and more sophisticated and intense. Unfortunately, there is no indication that this trend should change in the near future. On the contrary, given the developments in cyberspace so far, this trend can be expected to continue, as it strongly correlates with the growing number of users and their low security awareness, growing number of vulnerable devices connected to the Internet, and, last but not least, the easy availability of instructions and tools required for committing this serious crime.

If the term organization is used in the text, it means both the companies established for profit and individual enterprises, as well as organizations whose aim is not to generate profit, but to provide only selected services to households, such as education, health, police, courts, local government, and all organizational components of the state.

[1] GENES, Raimund. Targeted Attacks versus APTs: What's The Difference? - TrendLabs Security Intelligence Blog. *blog.trendmicro.com* [online]. 14 September 2015 [accessed on 12 March 2019]. Retrieved from: https://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-versus-apts-whats-the-difference/

Research question: Which of the factors that influence the increase in cybercrime could be described as key ones?

Methodology

Type of research: qualitative research

Scientific methods used: observation, in-depth interviews, Delphi method, analysis, comparison, synthesis

Brief description of the research: This paper has been prepared mainly **on the basis of observations, where the author of this paper acted as the so-called non-participating observer,**[1] monitoring the developments in the fields of information and cyber security in the last two decades in 11 organizations in the Czech Republic in order to **analyse** the approaches of top management to the issue of security.

Based on the comparison of these approaches with the approaches in other organizations, a common behaviour was identified and a **synthesis** of this information into research assumptions was performed, which were subsequently submitted to the security experts of the selected organizations for assessment.

Interviews were subsequently conducted with selected security experts with many years of experience in the field of information security and holders of CISM, CRISC, CISA, CISSP, CEH, OSCP, CHFI security certifications, in positions of information / cyber security managers / architects, in order to refine these key factors.

Sample size: 11 organizations

Composition of the sample: organizations in the private and public sectors, from various industries of the national economy, operating critical and non-critical information systems (4 banks, 1 software development company, 1 critical infrastructure company, 4 state-owned enterprises, 1 educational institution)

Method of selection of respondents: based on availability

Key factors

Since 1995, when I started monitoring the level of security in selected organizations, especially those with hundreds or thousands of employees, I have identified and analysed the following key factors that influence the increase in cybercrime. First of all, there is a growing number of users and vulnerable devices connected to the Internet, where private devices are used to access information systems of organizations, allowing access to these systems from home and over the Internet, transferring these systems and data to the cloud, outsourcing the management of these systems and, last but not least, the availability of instructions and tools necessary to commit this type of crime, where, unlike traditional crime, the perpetrator never physically appears at the crime scene before, during and after completion, which significantly hinders their detection and capture. Thus, we can encounter cyberattacks on households and companies, when the malicious code is

[1] DISMAN, Miroslav, Olga ŠMÍDOVÁ, and Jiří ORT. *Jak se vyrábí sociologická znalost* [online]. 2011 [accessed on 15 July 2020]. ISBN 978-80-246-2619-2. Retrieved from: http://site.ebrary.com/id/10887146

mainly disseminated via e-mail, intrusion, and misuse of poorly secured terminal equipment for another attack or data encryption and demanding ransom or misuse of access to Internet banking and transfer of funds, i.e., a criminal offence pursuant to Section 230 of Act No. 40/2009 Coll., the Criminal Code - unauthorized access to the computer system and information media. The following chapters briefly describe the individual factors. Certainly, other factors could be found, for which a similarly strong correlation with the increase in crime in cyberspace is evident, but **these factors are considered to be the key ones by the consulted security experts**.

Internet connection speed and computing power

The speed of both cable and mobile connections is increasing each year, which is due to the growing demand and competition in the advanced telecommunications market. Connection speed has increased from just a few kilobits per second up to several megabits per second. In two decades, the data transfer rate has increased thousandfold.[1] And while the amount of sensitive data is increasing, the size of individual sensitive data is still the same. In other words, the **credit card number, bank account number, social security number, or permanent address are still the same length and therefore the same size**, which can be expressed by the same number of bits. The total amount of information is changing, growing exponentially. The size of the information and the amount of information are two completely independent variables. As a result, while in the previous period it was not possible to download, for example, the entire database of clients in the size of several hundred MBs or even encrypt it, while staying unnoticed, because it would be computing power demanding and data-intensive operation, today, when it is a matter of only a few minutes, there is a greater risk that the organization may not notice it at all and most organizations do not actually notice it. **The analysis of security reports shows that the attacker operates unnoticed in the attacked organization for several months[2] and it also takes several months to solve the incident.[3]** Higher connection speeds enable a significantly faster implementation of the attack, which many organizations are not even able to respond to. It was the speed of connection that further accelerated the number of devices and users connected to the Internet, as well as the possibility of working from home using private devices.

Increasing computing power is another important factor that significantly affects the speed of the attack. This increase in computing power is mainly due to the technology used in the production of processors and increasing their density in accordance with the so-called Moore's Law,[4] size and speed of available cache, as well as the volatile and solid-state memories.

---

[1] *061004-17_S.pdf* [online]. [Accessed on 17 December 2019]. Retrieved from: https://www.czso.cz/documents/10180/46014808/061004-17_S.pdf

[2] FIREEYE. *M-Trends 2019* [online]. B.m.: FireEye. 2019 [Accessed on 8 March 2019]. Retrieved from: https://content.fireeye.com/m-trends

[3] 2019 Cost of a Data Breach Report| IBM Security. @*IBMSecurity* [online]. [Accessed on 25 May 2020]. Retrieved from: databreachcalculator.mybluemix.net

[4] PADUA, David A., ed. *Encyclopedia of parallel computing*. New York, NY: Springer, 2011. Springer reference. ISBN 978-0-387-09765-7.

Numbers of users and unsecured devices connected to the Internet

The number of Internet users continues to grow and despite the rate of growth slowing down it is likely to continue to do so, as it will essentially follow the population curve. The number of devices connected to the Internet is growing at a significantly higher rate and by far exceeds the current population. According to InternetLiveStats,[1] the number of Internet users has exceeded 4 billion, while in the Czech Republic, according to NetMonitor,[2] it has reached 7.8 million users.

The author's own investigation, where he acted as an independent observer,[3] conducted in several organizations with more than several thousand employees, but also in small family businesses, has shown that Internet access was initially possible only from dedicated computers connected to the Internet via a dial-up telephone line, which were outside the network and were also supervised. (Not so much for security, as due to the cost.) And when it comes to households, only a minimum of households had an Internet connection. This was due, inter alia, to relatively high connection charges, which were based on the duration of the connection. Later, computers in organizations connected to the Internet were located in a separate network and separated from the rest of the network. In the last stage, the Internet was accessed from all computers, but access was only possible to selected sites (white list). However, with the increase in the number of these websites, the situation became unmanageable and the opposite approach was chosen, when a list of pages or categories that are banned (black list) was created and the so-called content filtering applied. However, given that malware can also be found on completely trustworthy websites, this solution does not provide reliable protection either. (In small organizations with insufficient resources, this has never been much addressed and Internet access is managed based on the role/position of the employee in the organization's hierarchy or not at all.) Today, entire networks and even operating technologies are connected to the Internet, rather than individual computers, which was not possible until a few years ago.[4] According to iot-analytics,[5] more than 17 billion devices are connected to the Internet. This represents about 4 devices per user, usually including a desktop computer, laptop, tablet, and smartphone. As the numbers of users and connected devices increase, the surface of the attack increases, too, which is best reflected in the Metcalfe's Law.[6] Together with the factor identified in the previous chapter, the size of

[1] Number of Internet Users (2016) - Internet Live Stats. *Internet Users* [online]. [Accessed on 16 February 2019]. Retrieved from: http://www.internetlivestats.com/internet-users/

[2] NetMonitor [online]. [Accessed on 16 February 2019]. Retrieved from: http://www.netmonitor.cz/

[3] DISMAN, Miroslav, Olga ŠMÍDOVÁ, and Jiří ORT. *Jak se vyrábí sociologická znalost* [online]. 2011 [Accessed on 15 July 2020]. ISBN 978-80-246-2619-2. Retrieved from: http://site.ebrary.com/id/10887146

[4] SIEMENS. Bezpečnost průmyslových dat je otázka správné strategie. *Národní centrum průmyslu 4.0* [online]. 5 February 2020 [Accessed on 16 June 2020]. Retrieved from: https://www.ncp40.cz/aktuality/bezpecnost-prumyslovych-dat-je-otazka-spravne-strategie

[5] LASSE LUETH, Knud. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. *iot-analytics.com* [online]. 8 August 2018 [Accessed on 16 February 2019]. Retrieved from: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[6] *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT).* Place of publication not identified: IEEE., 2016. ISBN 978-1-5090-4130-5.

the program code has also increased. The consulted experts agree that it is the direct cause of this condition and that as a result, there has been a huge increase in the number of lines and the size of the operating system, from just a few hundred kBs (MS DOS) to GBs (Windows 10), which in itself means that such a code may contain, depending on its cyclomatic complexity, a larger number of errors that may not be detected in time. With the introduction of an agile approach, adopted by traditional organizations, such as banks, the development cycle is shortened and the release of new versions of SW running on these operating systems is accelerated, which only increases the attack surface.

In addition, computers appear in the form of various dedicated devices connectable to the Internet, refrigerators, dishwashers, microwaves, TVs, light bulbs, thermostats, in short, the so-called IoT (Internet of Things), but also smartphones and tablets, which have in fact become consumer goods with a short period of moral and physical obsolescence. Due to their price and rapid development, these devices are not even expected to have a long lifespan, let alone a lifetime of issuing security updates in order to eliminate the vulnerabilities that these devices already suffer from when they leave the production line and which are subsequently abused by attackers shortly after they connect to the Internet. This is because most of these devices contain vulnerabilities and will never get any updates to their operating system over their lifetime. Substantial pressure on the lowest possible price in order to reduce costs ultimately leads to the fact that there is an enormous number of devices connected to the Internet, which can be attacked, taken control of, and used to conduct an attack on other targets.

The growing number of attacks on organizations was also caused by the support of the BYOD (Bring Your Own Device) programme, which won over the COPE (Corporate Owned Personally Enabled) approach and led to an increase in the attack surface, thus, it became necessary to introduce additional security measures and rules.[1] Employees use their own private devices for work, which are not under the control of the organization at all, instead of using company devices for private purposes. And even though employees access the organization's systems from these devices via VPNs (virtual private networks), which provide end-to-end encryption, use two-factor authentication to log in, with VDE (virtual desktop environment) running on their devices, basically a virtual desktop, where some hardening has taken place and certain policies are enforced by security policies, these employee devices or their host systems may still be attacked. They can run malicious code that can take complete control of the device, integrate it into the botnet, and allow the attacker to remotely access the organization's data and system.[2] It should be noted that these devices often do not have an up-to-date operating system, not all applications used by their user are updated, there is no antivirus running, and their access to the Internet is completely unrestricted. Work from a private device is no longer a benefit in many organizations,

[1] KLESEL, Michael, Sebastian WEBER, Finja WALSDORFF, and Bjoern NIEHAVES. Are Employees Following the Rules? On the Effectiveness of IT Consumerization Policies. Wirtschaftsinformatik 2019 Proceedings [online]. 2019. Retrieved from: https://aisel.aisnet.org/wi2019/track07/papers/6

[2] Voice Phishers Targeting Corporate VPNs — Krebs on Security [online]. [Accessed on 31 August 2020]. Retrieved from: https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns/

but a way to reduce the cost of computer technology, including the contribution to the purchase of a given device.

Moreover, employees are increasingly taking advantage of the home office, i.e., working from home[1] and connecting to their employer's system from their private device via their ISPs. However, the problem is that an employee accessing the system and company data from home is not able to ensure and does not ensure the same level of physical security as an employee who is located in the organization's premises, usually accessible only through the reception, there is a control of persons, and there is also a significantly lower risk that the employee would be forced by physical or other form of violence to perform an unauthorized operation in the system without notice. This is possible in a home environment that is not under permanent surveillance and is not connected to a centralized protection panel. Work from home is also driven by efforts to further reduce costs per job and maintain business continuity when a crisis occurs, such as transport problems due to natural disasters or the spread of the infection that triggered emergency in March 2021, requiring to reduce physical presence at workplaces and start working from home. Immediately, the malicious code that was exploiting the situation appeared and was distributed, and the computers that were not secure were attacked.

The speed of creating new domains

With a decreasing price for the volume of transmitted data, faster connection speed, and a decreasing price for establishing and operating domains, companies are gradually moving their activities to cyberspace. **Each day, several hundred thousand domains are created, which, according to some sources, are used for criminal activities**,[2] such as spreading spam, phishing, malware or as a C&C server, shortly after their creation in up to 70% of cases. This was greatly aided by the emergence of Web 2.0, where basically anyone can become the author of the content, i.e., even the attacker, who can then hide their commands in the text on a trusted website that appears completely innocent at first glance.[3]

The analysis of the logs of the systems operated by the company, that was subject to this analysis, as well as the investigation of several hundreds of cases of attacks,[4] has shown that these domains are based on various top level domains. **Most of them are in the .com domain, and these are usually second-level (hundreds of thousands) or third-level (tens of thousands) domains, but sometimes even a fifteenth-level domain appears. Most frequently, the second-level domain is**

[1] S.R.O, VisionApps. Zaměstnanci chtějí home office. Splňte tyto 2 podmínky, aby práce z domu fungovala. *LMC* [online]. [Accessed on 17 December 2019]. Retrieved from: https://www.lmc.eu/cs/magazin/data-a-pruzkumy/zamestnanci-chteji-home-office-splnte-tyto-2-podminky-aby-prace-z-domu-fungovala/

[2] Should you block newly registered domains? Researchers say yes. *Help Net Security* [online]. 23 August 2019 [Accessed on 20 March 2020]. Retrieved from: https://www.helpnetsecurity.com/2019/08/23/block-new-domains/

[3] ČERMÁK, Miroslav. Na obzoru se objevují nové hrozby, třeste se! – 7. díl. *CleverAndSmart Management Consulting* [online]. 28 January 2020 [Accessed on 20 March 2020]. Retrieved from: https://www.cleverandsmart.cz/na-obzoru-se-objevuji-nove-hrozby-treste-se-7-dil/

[4] The author of this paper dealt with these cases from the position of a security analyst, when he assessed the attack vectors, techniques used, etc.

a number followed by a character. Often, several domains are generated, containing a number of consecutive numbers and characters. These domains have a short lifespan, often only a few hours or days, because they are marked as fraudulent by security solutions, and access to them is blocked or the domain is cancelled. However, at first, these domains are not identified as harmful at all by security solutions, and therefore it is suggested to preventively block all newly created domains at the DNS level and make them available only after a certain period of time.

Likewise, it is possible to assess domains when their ownership changes, because they can also be used for criminal purposes and benefit from their previous good reputation after the domain passes to a new owner. However, the question is whether this technique is really effective. At the moment, it is, but as soon as it becomes universally used, it can only lead to the attacker simply waiting a few days after registering the domain and then commencing their activity.

The effectiveness of this kind of protection will then decrease rapidly over time. Notwithstanding that the malicious content can only be made available to users accessing the website from a specific IP address range, which is already true, thus, the security solution does not know about it. There is another problem that quite often, sites running for a long time with a good reputation are abused, where the attacker in fact takes control of it, while this is not reflected in the domain record. The fact that users are lured to a fraudulent domain is also exacerbated by the fact that they are increasingly used to access the Internet with smartphones, as can be documented with logs from web servers. These devices use native clients, which are not always in an up-to-date version. It is also difficult to check the real address of the sender of the e-mail, where the link is directed, and the size of the letters also makes it difficult to correctly distinguish the domain name. This is used by attackers who create domains with similar appearance and start their own business with them. An ordinary user does not have many options to find out which service is the right one. The fact that experts, let alone ordinary users, can be mistaken is illustrated by the Zoom case, where there was an increase in the value of stock of another company only thanks to a similar name.[1] The situation is further aggravated by the growing number of top-level domains, with more than 1500 of them existing,[2] which allows the attacker to easily establish a domain of the same name, only using another top-level domain, and for the real owner, the possibility of response is significantly deteriorating. Defending against speculators and typosquatting and cybersquatting is becoming increasingly difficult due to the number of TLD domains, and attackers are still inventing new attack techniques, as was the case with the Privnotes.[3]

[1] FOOL, Contributor Evan Niu The Motley. The SEC Really Wants Investors to Stop Buying the Wrong Zoom Stock [online]. [Accessed on 22 June 2020]. Retrieved from: https://www.nasdaq.com/articles/the-sec-really-wants-investors-to-stop-buying-the-wrong-zoom-stock-2020-03-27

[2] List of Top-Level Domains - ICANN [online]. [Accessed on 22 June 2020]. Retrieved from: https://www.icann.org/resources/pages/tlds-2012-02-25-en

[3] KREBS, Brian. Privnotes.com Is Phishing Bitcoin from Users of Private Messaging Service Privnote.com. *KrebsonSecurity* [online]. 14 June 2020 [Accessed on 22 June 2020]. Retrieved from: https://krebsonsecurity.com/2020/06/privnotes-com-is-phishing-bitcoin-from-users-of-private-messaging-service-privnote-com/

The ease and speed of creating new dynamically generated domains using Domain Generation Algorithm, abbr. DGA, and changing IP addresses of servers, which these domains refer to, using the fast flux DNS technique in non-cooperating countries only worsens the situation and aids the attackers.

Security awareness

Low security awareness of employees and managers leads to mistakes and wrong decisions. The following essential facts emerged from conducting my own experiment[1] in organizations with several thousand employees and from the information of independent third parties which provide similar training and tests of resilience of employees on a commercial basis. Investments in security and training are basically the same, and although they have recently increased in some organizations in the context of the GDPR, there has been no significant and desirable change in the behaviour of employees. They still use weak and identical passwords in multiple systems, are not resistant to social engineering techniques, and thus fail to recognize the cases of phishing, vishing, baiting, and enable access to the workplace to unauthorized persons. Only in organizations which, together with training, provide also the testing of resilience of their employees to these attacks, it is possible to notice a significant improvement compared to the previous period. Year on year, there is also a continuous improvement, as the employees of these organizations are able to correctly identify phishing, which still represents the most common attack vector and thus the way in which the employees' terminal equipment is compromised and the attacker penetrates the organization's environment. In large organizations, it is a very good result when it is possible to reduce the number of employees susceptible to phishing to units of percentage.

We significantly lack better awareness of real vulnerabilities, threats and ongoing attacks in cyberspace. We learn about individual attacks from the media only rarely, there is no uniform classification of cyber threats, there is no clear statistics of attacks that would indicate the vector of the attack, the sector affected, the amount of damage, etc. Although there are various statistics, such as those from CSIRT[2] or the police,[3] these are often incomplete and unreliable. There are also security reports of foreign companies mapping the situation in the world, but these do not provide essential information and are often largely misleading. Certainly, it can be argued that there are professional publications, archives of security forces, etc., but majority of the professional as well as lay public do not have access to them and do not seek any information there. At least, it has emerged from interviews with security managers, who rely exclusively on publications from ISACA, consulting companies such as Gartner,

[1] ČERMÁK, Miroslav. Why Human Firewall Fails in the Battle with Sophisticated Spear Phishing Campaigns. In: Irena TUŠER and Šárka HOŠKOVÁ-MAYEROVÁ, eds. *Trends and Future Directions in Security and Emergency Management* [online]. Cham: Springer International Publishing, 2022 [Accessed on 28 January 2022], Lecture Notes in Networks and Systems, pp. 283-291. ISBN 978-3-030-88906-7. Retrieved from: doi:10.1007/978-3-030-88907-4_16

[2] Statistiky řešených incidentů - CSIRT [online]. [Accessed on 17 December 2019]. Retrieved from: https://csirt.cz/page/2635/statistiky-resenych-incidentu/

[3] Kyberkriminalita - Policie České republiky [online]. [Accessed on 17 December 2019]. Retrieved from: https://www.policie.cz/clanek/kyberkriminalita.aspx

Deloitte, KMPG, Accenture, and companies offering security solutions, which they consider to be up to date. This in itself worsens the perception of security by top management, which cannot be presented with specific cases that occurred in the territory of the Czech Republic and their actual consequences. The severity of security threats is thus underestimated.

In the long term, the level of security awareness is rather decreasing. Considering the growing number of users who are not at all interested in the security of their devices and who treat computers, tablets, mobile phones, and IoT purely as consumer goods, it is much easier for attackers to compromise these targets.

Globalization of cybercrime

For attacks in cyberspace, it is typical that the distance between the attacker and the victim does not play any role, and that the attacker is often also a victim, or the system which the attack is conducted from is fully under the control of the attacker, where the attacker can cover their tracks or even create false tracks to lead the investigation in a different direction. Malicious code, which is often used by various organized groups as part of these attacks, is located in a more or less modified form in various exploits and is placed on infected servers serving as watering holes, or is placed in trojanized applications or distributed as an attachment via various phishing campaigns, where it may be mistakenly attributed to someone else based on the names of individuals, variables, functions, libraries, and possibly even comments in parts of the code. In practice, it may happen, for example, that a Russian programmer places or sells his exploit on the dark web, which is then used as part of phishing conducted on clients of a Ukrainian bank. When the same exploit is used by another organized group to attack clients of banks in the Czech Republic at the same time, it is misinterpreted that the Russian APT group is behind the attack. Likewise, the fact that the server used as the controlling CaC server is located in China does not mean that there is a Chinese APT group behind the attack. Inter alia, deliberate counterfeiting of the code may be part of mutual attacking between powers.

The investigation of selected cases of attacks on Internet banking clients has shown that attackers like to use vulnerabilities in content management systems (in the vast majority of cases, it was Wordpress, which is not surprising because it has the largest share in the CMS market),[1] running on the web servers of companies with a good reputation for several years. In principle, attackers do not care which server they attack, they do not seem to prefer a server located in a particular country or running on a particular top level domain. Apart from the CMS used, no other common characteristic could be traced and it can be assumed that some kind of automated scanner is used to search the site and identify servers that suffer from a certain vulnerability. These are subsequently attacked and the attackers plant malicious code or phishing page on them.

For the above reason, it would be irresponsible to launch a counterattack on the system from which the attack is conducted under these conditions, because this attack could result in even more damage to the company that operates the server. It is

[1] Usage Statistics and Market Share of WordPress, June 2020 [online]. [Accessed on 25 June 2020]. Retrieved from: https://w3techs.com/technologies/details/cm-wordpress

necessary to contact the operator of the system in another country and ask for cooperation, which is often very problematic. Needless to say, the attacker, compromised server, and victim are typically located each in a different country with different jurisdiction. Thus, we are faced not only with a reluctance to cooperate, but also with cultural and language barriers, while the problem may also be the location of the server in a different time zone.

The transfer of crime to cyberspace raises the question of how to detect this crime already at the stage of preparation and whether the powers of the police should be strengthened, international cooperation deepened, and comprehensive monitoring enabled. Therefore, it is necessary to carefully consider how to proceed in the event of such an attack, pay sufficient attention to the amendment of the act on military intelligence, and also conduct a serious discussion on this issue.[1] Just as globalization increases profits in a legitimate market, it also increases the proceeds of crime in cyberspace.

With the speed of the Internet, the price of the connection, and the number of devices available over the Internet, the attack surface has increased enormously. With the development of Web 2.0 and the ability to share information and tools to commit cybercrime, the number of attackers has also increased.

If we view this sector as any other sector, we could, in the words of Michael F. Porter, characterize it as the sector where there are no barriers for entry, it is possible to leave it at any time, it is not necessary to have basically any capital (in principle, a computer and Internet connectivity are enough), it is not necessary to keep a scarce resource (a hacker who has the knowledge and abilities can be bought, and what was still considered a joke a few years ago, the 'Hacker as a Service', is now a common reality), and despite the ongoing competitive struggle, there is a minimal risk of loss of investment as well as getting caught and punished, which, together with low costs and high return on investment, makes the sector extremely attractive for entry of other players.

The motivation of the attackers has also changed; while two decades ago, hacking was motivated mainly by gaining reputation in the security community, and the maximum results of the attack consisted in making an entry in the logs, defacement of the website, or a message to the system administrator, currently, according to the consulted security experts, the vast majority of attacks are motivated by money. As a result, the system is compromised and abused for other attacks, e.g., on bank clients, when legitimate websites are hacked in order to place a copy of the bank website and attract login data from clients, theft of sensitive information, encryption of data, its deletion or, possibly, publication.

This also corresponds to the representation of the actors of these threats in cyberspace. Increasingly often, we encounter highly organized groups instead of isolated hackers. This can also be seen in how individual cyberattacks are being prepared, the incidence of which has been growing since approximately 2013, when the Czech Republic became a country on the map of the world, which systematic

[1] ŠPIDLA, Aleš. Novela zákona o vojenském zpravodajství – potřebujeme ji? *IT SECURITY NETWORK NEWS* [online]. 26 February 2019 [Accessed on 12 March 2019]. Retrieved from: https://www.itsec-nn.com/novela-zakona-o-vojenskem-zpravodajstvi-potrebujeme-ji/

cyberattacks are being conducted against and also whose citizens are more involved in, mainly as white horses, through which money are taken out of circulation. With the popularization of cryptocurrency, in recent years, money has been diverted in this way, which eliminates intermediaries, reduces the risk of disclosure, and further contributes to the attractiveness cybercrime.

IT transformation

The last factor, which has not yet manifested itself much, but which, according to the consulted security experts, cannot be ignored, because it will gain further importance and determine who will be the next victim of targeted cyberattacks, is the uncontrolled process of IT transformation, or related issues of security and risk management, especially the integration of solutions running in the cloud and on-premise, and the approaches to them.

In the last decade, it was possible to observe a relatively turbulent development in the monitored organizations (e.g., banks, transport companies), when the infrastructure in the data centres was **consolidated** and then **virtualized**. Together with this, documents were digitized and, in many cases, biometric signatures were introduced in order to reduce the costs of generating and archiving paper documentation. Afterwards, the processes were also **robotized** and the so-called RPA solutions[1] began to be promoted instead of direct integration, and it can be expected that their number will continue to increase.[2] The interviews with security experts show that it was preferred to immediately reduce costs by introducing a robotized process instead of direct integration consisting in adjusting the existing application, creating an API, etc. The danger of these RPA solutions, according to the consulted security experts, lies primarily in the speed at which these robots are able to control the application used within the robotized process and, in the event that they receive incorrect data or are intentionally presented with modified data by someone, to process the data.[3] Organizations often do not have set thresholds, i.e., the limits of how much or how large volumes of data mean suspicious activity, nor do they have a process set up to quickly undo any changes made by the robot. Another risk lies in the fact that these robots do not possess any artificial intelligence; this means, for example, that if a file in Excel, which is still used despite being inappropriate for the given purpose, is submitted to them, they process it. This is different from a person who immediately

[1] IVANČIĆ, Lucija, Dalia SUŠA VUGEC, and Vesna BOSILJ VUKŠIĆ. Robotic Process Automation: Systematic Literature Review. In: Claudio DI CICCIO, Renata GABRYELCZYK, Luciano GARCÍA-BAÑUELOS, Tomislav HERNAUS, Rick HULL, Mojca INDIHAR ŠTEMBERGER, Andrea KŐ, and Mark STAPLES, eds. *Business Process Management: Blockchain and Central and Eastern Europe Forum* [online]. Cham: Springer International Publishing, 2019 [Accessed on 26 June 2020], Lecture Notes in Business Information Processing, pp. 280-295. ISBN 978-3-030-30428-7. Retrieved from: doi:10.1007/978-3-030-30429-4_19

[2] DILMEGANI, Cem. Ultimate Guide to Robotic Process Automation (RPA) in 2020. *appliedAI* [online]. 22 November 2017 [Accessed on 25 June 2020]. Retrieved from: https://research.aimultiple.com/rpa/

[3] ČERMÁK, Miroslav. Stinná stránka robotizace. *CleverAndSmart Management Consulting* [online]. 11 February 2018 [Accessed on 15 June 2020]. Retrieved from: https://www.cleverandsmart.cz/stinna-stranka-robotizace/

notices abnormalities in the spreadsheet, as verified in a repeated experiment (I deliberately do not disclose the names of specific solutions). However, for the time being, the monitored organizations have not recorded attacks of this type, still, RPA does pose a certain risk, and this should be monitored further.

But robots and artificial intelligence are not only operated by companies, but also by cybercriminals. Their ability to solve CAPTCHA is a well-known fact. Little is known about situations, because of lack of publication, such as the repeated phishing attack on the clients of Czech banks in May last year, when the phishing site reacted very quickly compared to the previous waves, basically immediately (in the past, a delay of several minutes was also noticeable for the input data), so it can be assumed that **some form of robotics was used by the attacker**.

In the monitored organizations, it was also possible to observe the increase in the share of outsourced activities, including those related to data and system management. In practice, this means that data and systems are managed by employees of third parties, while these employees also manage data of other companies, possibly including systems and data of competitors. Thus, these workers may have a much greater opportunity to extract this data and abuse their access than the organization's own employees who do not have access to the data of other organizations. Given that outsourcing is often chosen for lower costs, it is entirely appropriate to ask how these lower costs can be achieved in practice, especially if the management is to be carried out by a qualified employee with appropriate certifications, while complying with all safety requirements. The interview with the respective managers has shown that the costs are only seemingly lower and they are achieved mainly because the scope of delivery is significantly reduced compared to the original assumptions, or exactly what is stated in the contract is delivered. And it is necessary to be careful,[1] as stated, e.g., by Rowan Legal, who specializes in the issue of IT contracts, because everything else must be paid for. The activity is also carried out in a country with significantly lower wage costs and higher staff turnover. Last but not least, managers state that they have also encountered the situation where even a company with certification hired another company, which was no longer certified, to process certain activities in order to further reduce costs, performing the activity on their behalf.

The outsourcing is also related to the **easy transfer of data and systems to the cloud**, which was made possible by the above-mentioned consolidation and virtualization of IT, preceding this step. Clouds are promoted by multinational companies such as Microsoft, Google, Amazon, but these only pursue their economic interests, namely, high return on investment and profit, thus, it is in their interest to convince the organizations' management to move their systems and data to the cloud. They use arguments such as the possibility of lower costs, achieved primarily as economies of scale, and then also a higher level of security. This also results from interviews with security experts in the position of ISO in organizations with several thousand employees. And since ownership has long been separated from management, and managerial bonuses are also tied to immediate economic results,

[1] ČERMÁK, Miroslav. Nejčastější úskalí IT smluv. *CleverAndSmart Management Consulting* [online]. 2020 [Accessed on 15 June 2020]. ISSN 2694-9830. Retrieved from: https://www.cleverandsmart.cz/nejcastejsi-uskali-it-smluv/

this massive exodus into the cloud is indeed taking place.[1] It is no wonder that, at the moment, when the average life cycle of a manager is several years, they choose currently the cheapest solution in the form of a cloud. However, it may be a moral hazard, too, because senior management may get the false impression that when its systems and data are managed by a reputable company, they no longer have to deal with security issues. It should be borne in mind that each state primarily pursues its national interests and supports its companies, and that whoever is our ally today may no longer be an ally tomorrow, so in the case of the state's critical information infrastructure, it is necessary to carry out cloud selection and risk analysis with particular care. Some caution is also recommended by the European Commission, which otherwise supports the cloud.[2] Moreover, the fact that the cloud is a two-way weapon is also stated in the National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025.[3] However, in the action plan for this strategy, there is an ambition to address only systems that are administered by the state[4] or those that can be described as part of the critical information infrastructure, important information systems or systems of basic services, which is insufficient, because most systems are not administered by the state and do not fall within the scope of the Act on Cyber Security. The performance of the national economy depends primarily on the level of security of private companies, which are led by professional managers who see the cloud rather as a solution that allows them to immediately reduce costs.

Moreover, the interviews with some managers have shown that they do not have any procedure in place in case the cloud is unavailable or they need to switch to another provider. And if organizations do not design and develop their systems as cloud-native, then the transition from one cloud provider (Cloud Service Provider, CSP) to another will not be possible; these organizations will be threatened with vendor lock-in with all the consequences resulting from this problematic condition, while CSP, of course, will not help them in any way. Such an organization can easily notice rising costs or security problems.

It should also be noted that the clouds were designed to be resistant to threats of natural origin, such as earthquakes, storms, floods, as well as conventional weapons, and could somehow work in the event of temporary unavailability of the data centre or its complete destruction. However, the weakness of clouds will always be a human error or a cyberattack exploiting SW vulnerabilities. When it comes to human error, let us not forget that when an admin in DC makes a mistake, it may remain unnoticed, but errors in the cloud are immediately recognized by everyone who uses it.[5] Attacking

---

[1] *ce31b358-2dca-4204-b507-c7e4656064e7.pdf* [online]. [Accessed on 17 December 2019]. Retrieved from: https://www.czso.cz/documents/10180/61601888/06200518.pdf/ce31b358-2dca-4204-b507-c7e4656064e7?version=1.1

[2] MICHLMAYR, Thomas. European Commission Cloud Strategy. Not dated, p. 28.

[3] *nskb-150216-final.pdf* [online]. [Accessed on 18 December 2019]. Retrieved from: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

[4] *akc48dnc3adplc3a1n-rkb-final-150408.pdf* [online]. [Accessed on 18 December 2019]. Retrieved from: https://www.govcert.cz/download/gov-cert/container-nodeid-967/akc48dnc3adplc3a1n-rkb-final-150408.pdf

[5] Don't be the fool in the cloud | Computerworld [online]. [Accessed on 18 December 2019]. Retrieved from: https://www.computerworld.com/article/3233289/don-t-be-the-fool-in-the-cloud.html

such a cloud and demanding ransom is very tempting, and if it happens, the weak will not survive, because the insurance company will not compensate them, as cyber warfare is excluded. It has been made clear by the Mondelez case.[1]

Despite some progress in recent years, there is still considerable dependence on the CSP regarding the possibility of logging events and their forensic analysis and investigation of security incidents, as well as the possibility of disaster recovery. The problem is that the CSP cannot, in principle, even provide any logs. Let us not forget that information about other clients is also stored in the logs. This is because shared infrastructure is used to reduce costs. Views of these logs are imperfect and incomplete, but you will only find out when you start investigating a security incident. According to some security experts, the error rate is up to 50%. The ongoing survey among security experts also shows that almost 80% of them believe that the state's critical information infrastructure should not be located in a foreign cloud.[2]

According to the consulted security experts, it can be expected in the future that still more attacks will use some form of robotization in cooperation with **artificial intelligence and machine learning**, and it will be necessary to secure defence in the same way.[3]

Conclusion

Key factors that influence and will influence the increase and form of crime committed in cyberspace in the future have been identified.

The studied organizations have certain common characteristics. The alpha and omega is the reduction of costs, which can be observed in all studied organizations. Employees connect from home via their ISPs and from their private devices, which suffer from multiple vulnerabilities, to their employers' systems and data, which are located somewhere in the cloud.

The physical locations from which employees connect are not under control, the devices from which employees connect are not under control, the data connections that employees use are not under control, and also the clouds where the data and systems of the organization are located are not under control, as everything is treated only contractually. With the number of vulnerable devices, the number of devices which can become a target of an attack and, at the same time, from which an attack can be conducted at the moment when they are compromised, increases. These devices can

[1] What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict. *Lawfare* [online]. 8 March 2019 [Accessed on 18 December 2019]. Retrieved from: https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict

[2] ČERMÁK, Miroslav. Ohrožuje přesun systémů do cloudu naše národní hospodářství a bezpečnost? *CleverAndSmart Management Consulting* [online]. 29 November 2019 [Accessed on 18 December 2019]. Retrieved from: https://www.cleverandsmart.cz/ohrozuje-presun-systemu-do-cloudu-nase-narodni-hospodarstvi-a-bezpecnost/

[3] PARATI, Namita, DEPARTMENT OF CSE, BRECW, HYDERABAD, INDIA, Pratyush ANAND, a FUNCTIONAL CONSULTANT, FUJITSU PVT. LTD., HYDERABAD, INDIA. Machine Learning in Cyber Defence. *International Journal of Computer Sciences and Engineering* [online]. 2017, vol. 5, no. 12, pp. 317-322. ISSN 23472693. Retrieved from: doi:10.26438/ijcse/v5i12.317322

be integrated into the botnet and further rented to those who pay, it is the so-called 'Crime as a Service', abbreviated as CaaS.

The possibilities of their misuse are considerable, they can be misused for breaking passwords, carrying out fraudulent banking transactions, conducting DDoS attacks on other organizations, hacking other systems, distributing spam, they can serve as proxy servers through which the attack is conducted, so the identity of the attacker will remain hidden and, in addition, it can then be attributed to a completely different entity on the basis of the source of the attack. The topical question is also no longer whether there will be an attack on a specific organization, but when and how long after the intrusion the organization will be able to find out and respond to the situation. According to M-Trends' statistics, this often takes a few weeks.

Nevertheless, most managers believe that the attack does not concern them, because their organization does not have any revolutionary technology or know-how that would be interesting for the attacker. Somehow, they do not want to admit that, in addition to targeted attacks, there are so-called untargeted attacks, which are much more frequent, and that their organization may be a victim of ransomware and its activity may be completely paralyzed.

A huge number of vulnerable devices and users connected to the Internet is a very attractive target for the attacker, especially when they can and usually also use another device located in another country to prevent the investigation or misguide it in a completely different direction and significantly reduce the risk of detection and getting caught.

The very low likelihood of being caught and the high return on investment provide offenders committing crimes in cyberspace with a very interesting alternative to traditional crime, where the risk of detection and getting caught is significantly higher. It is clear that these factors will continue to affect the form of cybercrime in the territory of the Czech Republic and its further increase can be expected.

Literature

2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). Place of publication not identified: IEEE. 2016. ISBN 978-1-5090-4130-5.

2019 Cost of a Data Breach Report| IBM Security. *@IBMSecurity* [online]. [Accessed on 25 May 2020]. Retrieved from: databreachcalculator.mybluemix.net

061004-17_S.pdf [online]. [Accessed on 17 December 2019]. Retrieved from: https://www.czso.cz/documents/10180/46014808/061004-17_S.pdf

akc48dnc3adplc3a1n-rkb-final-150408.pdf [online]. [Accessed on 18 December 2019]. Retrieved from: https://www.govcert.cz/download/gov-cert/container-nodeid-967/akc48dnc3adplc3a1n-rkb-final-150408.pdf

ce31b358-2dca-4204-b507-c7e4656064e7.pdf [online]. [Accessed on 17 December 2019]. Retrieved from: https://www.czso.cz/documents/10180/61601888/06200518.pdf/ce31b358-2dca-4204-b507-c7e4656064e7?version=1.1

ČERMÁK, Miroslav. Stinná stránka robotizace. *CleverAndSmart Management Consulting* [online]. 11 February 2018 [Accessed on 15 June 2020]. Retrieved from: https://www.cleverandsmart.cz/stinna-stranka-robotizace/

ČERMÁK, Miroslav. Ohrožuje přesun systémů do cloudu naše národní hospodářství a bezpečnost? *CleverAndSmart Management Consulting* [online]. 29 November 2019 [Accessed on 18 December 2019]. Retrieved from: https://www.cleverandsmart.cz/ohrozuje-presun-systemu-do-cloudu-nase-narodni-hospodarstvi-a-bezpecnost/

ČERMÁK, Miroslav. Na obzoru se objevují nové hrozby, třeste se! – 7. díl. *CleverAndSmart Management Consulting* [online]. 28 January 2020 [Accessed on 20 March 2020]. Retrieved from: https://www.cleverandsmart.cz/na-obzoru-se-objevuji-nove-hrozby-treste-se-7-dil/

ČERMÁK, Miroslav. Nejčastější úskalí IT smluv. *CleverAndSmart Management Consulting* [online]. 2020 [Accessed on 15 June 2020]. ISSN 2694-9830. Retrieved from: https://www.cleverandsmart.cz/nejcastejsi-uskali-it-smluv/

ČERMÁK, Miroslav. Why Human Firewall Fails in the Battle with Sophisticated Spear Phishing Campaigns. In: Irena TUŠER and Šárka HOŠKOVÁ-MAYEROVÁ, eds. *Trends and Future Directions in Security and Emergency Management* [online]. Cham: Springer International Publishing, 2022 [Accessed on 28 January 2022], Lecture Notes in Networks and Systems, pp. 283-291. ISBN 978-3-030-88906-7. Retrieved from: doi:10.1007/978-3-030-88907-4_16

DILMEGANI, Cem. Ultimate Guide to Robotic Process Automation (RPA) in 2020. *appliedAI* [online]. 22 November 2017 [Accessed on 25 June 2020]. Retrieved from: https://research.aimultiple.com/rpa/

DISMAN, Miroslav, Olga ŠMÍDOVÁ, and Jiří ORT. *Jak se vyrábí sociologická znalost* [online]. 2011 [Accessed on 15 July 2020]. ISBN 978-80-246-2619-2. Retrieved from: http://site.ebrary.com/id/10887146

Don’t be the fool in the cloud | Computerworld [online]. [Accessed on 18 December 2019]. Retrieved from: https://www.computerworld.com/article/3233289/don-t-be-the-fool-in-the-cloud.html

FIREEYE. *M-Trends 2019* [online]. B.m.: FireEye. 2019 [Accessed on 8 March 2019]. Retrieved from: https://content.fireeye.com/m-trends

FOOL, Contributor Evan Niu The Motley. The SEC Really Wants Investors to Stop Buying the Wrong Zoom Stock [online]. [Accessed on 22 June 2020]. Retrieved from: https://www.nasdaq.com/articles/the-sec-really-wants-investors-to-stop-buying-the-wrong-zoom-stock-2020-03-27

GENES, Raimund. Targeted Attacks versus APTs: What’s The Difference? - TrendLabs Security Intelligence Blog. *blog.trendmicro.com* [online]. 14 September 2015 [Accessed on 12 March 2019]. Retrieved from: https://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attacks-versus-apts-whats-the-difference/

IVANČIĆ, Lucija, Dalia SUŠA VUGEC, and Vesna BOSILJ VUKŠIĆ. Robotic Process Automation: Systematic Literature Review. In: Claudio DI CICCIO, Renata GABRYELCZYK, Luciano GARCÍA-BAÑUELOS, Tomislav HERNAUS, Rick HULL, Mojca INDIHAR ŠTEMBERGER, Andrea KŐ, and Mark STAPLES, eds. *Business Process Management: Blockchain and Central and Eastern Europe Forum* [online]. Cham: Springer International Publishing, 2019 [Accessed on 26 June 2020], Lecture Notes in Business Information Processing, pp. 280–295. ISBN 978-3-030-30428-7. Retrieved from: doi:10.1007/978-3-030-30429-4_19

KLESEL, Michael, Sebastian WEBER, Finja WALSDORFF, and Bjoern NIEHAVES. Are Employees Following the Rules? On the Effectiveness of IT Consumerization Policies. *Wirtschaftsinformatik 2019 Proceedings* [online]. 2019. Retrieved from: https://aisel.aisnet.org/wi2019/track07/papers/6

KREBS, Brian. Privnotes.com Is Phishing Bitcoin from Users of Private Messaging Service Privnote.com. *KrebsonSecurity* [online]. 14 June 2020 [Accessed on 22 June 2020]. Retrieved from: https://krebsonsecurity.com/2020/06/privnotes-com-is-phishing-bitcoin-from-users-of-private-messaging-service-privnote-com/

Kyberkriminalita - Policie České republiky [online]. [Accessed on 17 December 2019]. Retrieved from: https://www.policie.cz/clanek/kyberkriminalita.aspx

LASSE LUETH, Knud. State of the IoT 2018: Number of IoT devices now at 7B - Market accelerating. *iot-analytics.com* [online]. 8 August 2018 [Accessed on 16 February 2019]. Retrieved from: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

List of Top-Level Domains - ICANN [online]. [Accessed on 22 June 2020]. Retrieved from: https://www.icann.org/resources/pages/tlds-2012-02-25-en

MICHLMAYR, Thomas. European Commission Cloud Strategy. Not dated, p. 28.

NetMonitor [online]. [Accessed on 16 February 2019]. Retrieved from: http://www.netmonitor.cz/

nskb-150216-final.pdf [online]. [Accessed on 18 December 2019]. Retrieved from: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

Number of Internet Users (2016) - Internet Live Stats. *Internet Users* [online]. [Accessed on 16 February 2019]. Retrieved from: http://www.internetlivestats.com/internet-users/

PADUA, David A., ed. *Encyclopedia of parallel computing*. New York, NY: Springer, 2011. Springer reference. ISBN 978-0-387-09765-7.

PARATI, Namita, DEPARTMENT OF CSE, BRECW, HYDERABAD, INDIA, Pratyush ANAND, a FUNCTIONAL CONSULTANT, FUJITSU PVT. LTD., HYDERABAD, INDIA. Machine Learning in Cyber Defence. *International Journal of Computer Sciences and Engineering* [online]. 2017, vol. 5, no. 12, pp. 317-322. ISSN 23472693. Retrieved from: doi:10.26438/ijcse/v5i12.317322

Should you block newly registered domains? Researchers say yes. *Help Net Security* [online]. 23 August 2019 [Accessed on 20 March 2020]. Retrieved from: https://www.helpnetsecurity.com/2019/08/23/block-new-domains/

SIEMENS. Bezpečnost průmyslových dat je otázka správné strategie. *Národní centrum průmyslu 4.0* [online]. 5 February 2020 [Accessed on 16 June 2020]. Retrieved from: https://www.ncp40.cz/aktuality/bezpecnost-prumyslovych-dat-je-otazka-spravne-strategie

S.R.O, VisionApps. Zaměstnanci chtějí home office. Splňte tyto 2 podmínky, aby práce z domu fungovala. *LMC* [online]. [Accessed on 17 December 2019]. Retrieved from: https://www.lmc.eu/cs/magazin/data-a-pruzkumy/zamestnanci-chteji-home-office-splnte-tyto-2-podminky-aby-prace-z-domu-fungovala/

Statistiky řešených incidentů - CSIRT [online]. [Accessed on 17 December 2019]. Retrieved from: https://csirt.cz/page/2635/statistiky-resenych-incidentu/

ŠPIDLA, Aleš. Novela zákona o vojenském zpravodajství – potřebujeme ji? *IT SECURITY NETWORK NEWS* [online]. 26 February 2019 [Accessed on 12 March 2019]. Retrieved from: https://www.itsec-nn.com/novela-zakona-o-vojenskem-zpravodajstvi-potrebujeme-ji/

Usage Statistics and Market Share of WordPress, June 2020 [online]. [Accessed on 25 June 2020]. Retrieved from: https://w3techs.com/technologies/details/cm-wordpress

Voice Phishers Targeting Corporate VPNs — Krebs on Security [online]. [Accessed on 31 August 2020]. Retrieved from: https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns/

What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict. *Lawfare* [online]. 8 March 2019 [vid 18 December 2019]. Retrieved from: https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict

S U M M A R Y

This paper describes relevant key factors that affect the growth of cybercrime and will continue to determine the form of cybercrime. These factors were identified on the basis of selected indicators. This includes, in particular, an increasing number of vulnerable Internet-connected devices that can be both a target and also a tool of cybercrime, as well as the widely available guidance and means needed to commit this type of crime. Understanding these trends should enable better prediction of further cybercrime development.

Keywords: cybercrime, key factors, IoT, BYOD, cloud, home office, outsourcing, cyberattacks, security awareness, IT transformation.

R E S U M É

ČERMÁK, Miroslav: KLÍČOVÉ FAKTORY OVLIVŇUJÍCÍ NÁRŮST KYBERKRIMINALITY

Tato práce se zabývá klíčovými faktory, které ovlivňují nárůst kybernetické kriminality a budou i do budoucna určovat její podobu. Tyto faktory byly identifikovány na základě analýzy trendů vybraných ukazatelů. Jedná se zejména o rostoucí počet uživatelů a jejich nízké bezpečnostní povědomí a množství zranitelných zařízení připojených k internetu, z nichž může být páchána kybernetická trestná činnost a která zároveň mohou být i cílem této trestné činnosti. Dále pak široce dostupné návody a prostředky potřebné pro páchání tohoto typu trestné činnosti, snadnost a rychlost, s jakou lze vytvářet nové domény a na ně umísťovat škodlivý kód, a v neposlední řadě pak probíhající transformace IT a globalizace kybernality. Porozumění těmto trendům by mělo umožnit lépe odhadnout další možný vývoj této trestné činnosti.

Klíčová slova: kybernetická kriminalita, kybernalita, klíčové faktory, IoT, BYOD, cloud, práce z domova, bezpečnostní povědomí, transformace IT.