THREATS IN CYBER SAFETY - OUTLINE OF THE PROBLEM

doi: 10.2478/czoto-2020-0043
Date of submission of the article to the Editor: 30/11/2019
Date of acceptance of the article by the Editor: 18/01/2020

Wojciech Gliń1 – orcid id: 0000-0002-8295-5702
Renata Stasiak-Betlejewska2 – orcid id: 0000-0001-8713-237X
Czestochowa University of Technology, Poland

Abstract: Currently, the industry is called as Industry 4.0, Internet of Things, Industrial Internet of Things, where devices, machines, information, organizations and people are connected to the network. Every day meet new solutions for Industry 4.o can be met, but in parallel with these solutions there are also threats in the field of security of industrial networks. Such threats have been called cyber-attacks or cyber threats. Cybersecurity is the global name of a field aimed at counteracting all types of threats on the web. Cybersecurity is to raise awareness, inform, control and introduce solutions to counteract cyber threats. Enterprises, organizations dealing with the promotion of Industry 4.0, IoT, IIoT, form the appropriate groups, departments, companies whose goal is to counteract all types of cyber-attacks. At present, the thesis can be formulated that cybersecurity of the broadly understood network is more important than the implementation of Industry 4.0. The publication will attempt to present the threats that cybersecurity enterprises must face and the ways and methods to counter them.

Keywords: cybersecurity, threats, enterprises

1. INTRODUCTION
Definitions of cyberspace should certainly be combined with cybernetics, which, according to the intentions of its creator N. Wiener, as shown by P. Sienkiewicz was the science of control and communication in objects of any nature (Sienkiewicz, 2009). Simultaneously, it has overtones of the writer, where American writer W. Gibson used this concept for the first time in his science fiction novels. Analysing the characteristics of cyber space this allows for consideration cyber network not as a technology but as a system, which is characterized by interactivity. Cyberspace has been shaped by the following processes (Sahrom, 2018; Manes and Valeriano, 2015, Sienkiewicz, 2009):

- The process of integration of basic forms of information transmission and presentation, which brought multimedia, "digitizing" the info sphere and the cono sphere.
- The process of ICT convergence: IT and telecommunications systems and electronic media.
  - The techno sphere integration process that has shaped the global integrated ICT platform.
Almost every phenomenon that is caused by technological progress, including cyberspace has its advantages and disadvantages (Dunn-Cavelty, 2008). Cyberspace has areas of positive and negative cooperation. In the positive part there is an undoubted increase in the possibilities of meeting social needs and self-development in various areas, for example (Taddeo, 2019; Sienkiewicz, 2009; Sulier, 2002):

- in education,
- in scientific research,
- in communication,
- in economics,
- in culture,
- in security.

Unfortunately, as there are advantages, there must be disadvantages, which means that cyberspace has become dangerous, which has become a source of threats to internal and external security. Most often we can deal with phenomena such as cybercrime, cyber war, cyber terrorism, cyber surveillance (Nikkel, 2018; Ciekanowski et al., 2016; Bendovschi, 2015).

The term cybersecurity comes from the term information security, however it is used to refer to a broader range of issues. There is no clear definition of cybersecurity. According to the European Commission, cyber security generally refers to safeguards and activities that can be used to protect a cybernetic domain, both civil and military, against those threats that affect its interdependent networks and IT infrastructure, and which may damage those networks and that infrastructure (Salminen and Hossain, 2018; Chmielewski 2016).

In contrast, the extended definition developed by NICCS describes cyber security as strategies, policies and standards for security and operations in cyberspace, covering the full range of risk reduction, vulnerability and deterrence, international involvement, incident response, and on the other hand a preventive policy that includes relevant operations in computer network, information provision, law enforcement, intelligence, diplomacy troops, related to the security and the stability of global information and communication infrastructure (Galinec et al., 2017; Chmielewski, 2016; Yar, 2013).

The area of cyber security is a horizontal area that penetrates all sectors of the country’s economy, has an impact on the functioning of the state and society in almost all its dimensions.

2. RESEARCH FIELD CHARACTERISTIC

Defining cyberspace areas threatened by attacks is very difficult, so when considering threats in IIoT, the management and departments dealing with enterprise network security management should know the answer to the questions: "Does the company know what cyber-attacks threaten it?", "Do the methods and procedures used in the company are sufficient? "," how to minimize the danger that the "human" side? ". However, the most important question of threats in cyberspace is "how to prevent, secure cyberspace against attacks?". Secondary data of entities dealing with cybersecurity in Poland were used in the publication. Over 100 Polish enterprises took part in the study.

Cyber threats in an enterprise are not only an IT problem but also a business risk. Most CEOs in the world rank them among the biggest risks for their own businesses. Cybersecurity is not a priority in several regions around the world. Among Polish companies,
cyber-roulette is often noticed, where companies count on luck and the false belief that the company is protected against attacks. The main assumptions that will be addressed in the article are the most dangerous cyber threats. Cyber-attacks are a widespread phenomenon, attacks on cyberspace are constantly increasing, with organized cyber-criminal groups emerging.

3. RESEARCH FINDINGS
The results of the conducted data relate to the period 2016-2018 concerns respondents group including 154 companies which were asked what and to what extent they are threatened by cyber threats. Information on cyber threats is a constant topic in the literature on the subject and in business conversations. The respondents show that from the point of view of enterprises it is an important topic and that they are taking actions to improve security. The basic activities of network security include audits, security tests, analyses and reports of companies dealing with cybersecurity analysis. The research conducted in enterprises shows that 1/4 of the surveyed enterprises stated that they have never conducted an IT infrastructure security audit. On the other hand, around a quarter of enterprises declare that they do not conduct any cybersecurity training in companies.

The positive conclusion of such research is the fact that about 3/4 of respondents take the subject of company security seriously. At the same time, among security experts, they have been repeating for years that industrial and IT networks are the most vulnerable to attacks. They lack: many built-in security mechanisms, qualified staff at every level of processes, which are the basic components in IT networks, such as automated updates and multi-level authentication mechanisms. Until recently, companies did not have enough data to allow an objective risk assessment. One may wonder whether this is really a lot or little and whether this information is sufficient in terms of security. Figure 1 presents the threats that, according to 154 enterprises, are the most significant in 2016.
In 2016, the most significant threats according to enterprises were general malware campaigns and accidental, unauthorized and / or destructive actions of employees, which translated into 62% and 60%. Less than half of those surveyed indicate a threat of data loss due to a hardware failure. The smallest threats pointed out by enterprises are natural disasters (1%), complex attacks on computers (3%) and intentional unauthorized and / or destructive actions of employees (9%). Figures 2 and 3 present the cyber threats that pose the greatest threat to enterprises in 2017 and 2018.
Advanced targeted attacks | 34% | 37% | 21% | 3%
Data leaks via malicious software | 23% | 46% | 27% | 4%
Data theft by employees | 22% | 41% | 33% | 4%
General ransomware campaigns | 23% | 44% | 23% | 10%
Phishing authentication | 11% | 49% | 37% | 3%
Attacks that exploit application errors | 9% | 43% | 42% | 6%
Data leakage due to theft or loss of media or mobile devices | 6% | 41% | 43% | 10%
Attacks on wireless networks | 7% | 35% | 38% | 20%
Eavesdropping and Man-in-the-Middle attacks | 6% | 27% | 51% | 16%
Hacking into mobile devices | 5% | 31% | 44% | 20%
Data theft as a result of a breach of physical security | 5% | 27% | 51% | 17%
Denial of service attacks | 2% | 32% | 50% | 16%

Fig. 2. Cyber threats that pose the greatest risk to organizations in 2017
Source: KPMG report, Cyber security barometer, Cyber-attack as a common phenomenon

Data leaks via malicious software | 16% | 26% | 34% | 10% | 10% | 4%
Data theft by employees | 20% | 23% | 26% | 17% | 11% | 7%
General ransomware campaigns | 17% | 22% | 29% | 18% | 12% | 2%
Advanced targeted attacks | 20% | 15% | 30% | 16% | 16% | 3%
Phishing credentials | 14% | 20% | 31% | 19% | 15% | 1%
Attacks on wireless networks | 5% | 19% | 22% | 23% | 22% | 9%
Attacks that exploit errors in applications | 4% | 16% | 28% | 27% | 21% | 4%
Traffic eavesdropping and Man-in-the-Middle attacks | 6% | 11% | 24% | 25% | 30% | 4%
Data theft as a result of a breach of physical security | 10% | 9% | 19% | 20% | 38% | 4%
Data leakage due to theft or loss of media or mobile devices | 4% | 13% | 18% | 23% | 33% | 9%
Denial of service attacks | 5% | 7% | 17% | 34% | 33% | 4%
Hacking into mobile devices | 6% | 8% | 18% | 14% | 35% | 19%

Fig. 3. Cyber threats that pose the greatest risk to organizations in 2018
Source: KPMG report, Cyber security barometer, In defence against attacks
Figure 2 shows the cyber threats that, according to companies, pose the greatest risk. Among the respondents surveyed in 2017, the biggest concerns about cybersecurity are advanced targeted attacks, data leakage via malware and the human factor of data theft. According to companies, the least fear of threats is denial of service attacks and data theft as a result of physical security breaches.

In contrast, Figure 3 according to the companies involved in the 2018 survey, the greatest risk is the risk of data leakage via malicious software and data theft by employees of their companies. Enterprises indicated that the smallest security risks in the audited year were hacking into mobile devices and denial of service attacks. In the years 2016-2018, threats related to cybersecurity in the enterprise change from year to year. Figure 4 presents the investments of enterprises focused on cyber threats.

![Security areas in which enterprises plan to invest](image)

Source: KPMG report, Cyber security barometer, In defence against attacks

Enterprises participating in the survey ensure that planned security investments will relate to continuous operation, protection against malware and security of contact with the Internet, are identified as priority investments to improve cybersecurity in the enterprise. The smallest expenditure on investments in the area of security concerns vulnerability management, security in software development processes, and security management of mobile devices.
4. CONCLUSION
In the examined period, we can observe an increased number of attacks that are becoming targeted at selected enterprises or sectors. Security threats remain virtually the same, only the level of threats is higher. Enterprises are realizing that IT security depends on the weakest link, where it is most often the human factor. Information today is the driving force of enterprises. They must realize that such activities require constant monitoring, because with the increase in transmitted data it is large, which also increases the occurrence of threats. The threats enterprises must face are too complex and dynamic, and processes and technologies must constantly evolve in response. There is no general cure for current cyber threats. Enterprises must acknowledge that a small battle against cyber threats that is permanent is better than no. Enterprises cannot forget that there are no ideal solutions that will always protect their companies from cyber threats.

REFERENCES
Bendovschi A., 2015. Cyber-Attacks – Trends, Patterns and Security Countermeasures, Procedia Economics and Finance, 28, 24-31.
Chmielewski Z., 2016. Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich, Studia z Polityki Publicznej, 2, 103-128.
Ciekanowski Z., Nowicka J., Wyrębek H., 2016. Bezpieczeństwo państwa w obliczu współczesnych zagrożeń, Pracownia Wydawnicza Wydziału Humanistycznego, Siedlce, Polska.
Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami.
Analiza sytuacji i rekomentacje działań, https://cyfrowapolska.org/wp-content/uploads/2019/01/Raport_cyberbezpieczne%C5%84stwo_2019.pdf
Cyber-ruletka po polsku, Dlatego firmy w walce z cyberprzestępcami liczą na szczęście, https://www.pwc.pl/pl/pdf/cyber-ruletka-po-polsku-raport-pwc-gsiss-2018.pdf.
Galinec D., Možnik D., Guberina B., 2017. Cybersecurity and cyber defence: national level strategic approach, Automatika, 58:3, 273-286, DOI: 10.1080/00051144.2017.1407022
Dębowski T., 2018. Cyberbezpieczeństwo wyzwaniem XXI wieku, Wydawnictwo Naukowe ArcheaGraph, Łódź-Wrocław, Polska.
Dunn-Cavelty M., 2008. Cyber-security and Threat Politics: US Efforts to Secure theInformation Age, New York, NY, Routledge.
Lakomy M., 2015. Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Wydawnictwo Uniwersytetu Śląskiego, Katowice, Polska.
Maness R.S., Valeriano, B. 2015. The Impact of Cyber Conflict on International Interactions, Armed Forces & Society 42(2), DOI: 10.1177/0095327X15572997
Nikkel B., 2018. Positive Changes and Collaboration in the Fight Against Cybercrime, Cybersecurity und IT-forensik.
Nowak A., 2013. Cyberprzestrzeń jako nowa jakość zagrożeń, Zeszyty Naukowe AON, Akademia Sztuki Wojennej, 3, 5-46.
Raport KPMG, Barometr cyberbezpieczeństwa, Cyberatak zjawiskiem powszechnym, https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/01/pl-Barometr-cyberbezpieczenstwa-cyberatak-zjawiskiem-powszechnym.PDF.
Raport KPMG, Barometr cyberbezpieczeństw, W obronie przed atakami, https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/04/pl-Raport-KPMG-Barometr-Cyberbezpieczeństwa-W-obronie-przed-cyberatakami.pdf.
Salminen M., Hossain K., 2018. Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North, Polar Record, 54(2), 108-118, DOI:10.1017/S0032247418000268
Sienkiewicz P., 2009. Analiza systemowa zagrożeń dla bezpieczeństwa Raport Specjalny: Jak chronić sieci przemysłowe przed cyberatakami?, Raport CyberX, Astor, 2017. Raport z badania, Cyberbezpieczeństwo Firm, https://docplayer.pl/49447584-Raport-z-badania-cyberbezpieczeństwo-firm.html.
Sahrom MD. A., Selamat R.S., Ariffin A., Yusof R., 2018. Cyber Threat Intelligence – Issue and Challenges, Indonesian Journal of Electrical Engineering and Computer Science, 10, 1, 371-379, DOI: 10.11591/ijeecs.v10.i1.pp371-379
Cyber threat intelligence – Issue and challenges. Available from: https://www.researchgate.net/publication/322939485_Cyber_threat_intelligence_-_-Issues_and_challenges [accessed Mar 23 2020].
Salminen cyber przestrzeni, Automatyka/Akademia Górniczo–Hutnicza im. Stanisława Staszica w Krakowie, 13, 2, 583—592.
System bezpieczeństwa cyber przestrzeni RP, https://www.cert.pl/wp-content/uploads/2015/12/nask_rekomendacja.pdf.
Suler, J.R., 2002. Identity Management in Cyberspace, Journal of Applied Psychoanalytic Studies, 4, 455-460.
Taddeo, M., 2019. Is Cybersecurity a Public Good?, Minds & Machines 29, 349–354, DOI: 10.1007/s11023-019-09507-5
Trubalska J., Wojciechowski Ł., 2017. Bezpieczeństwo państwa w cyber przestrzeni, Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji w Lublinie, Lublin, Polska.
Yar M., 2013. Cybercrime and society, Sage Publications, Second Edition.
Wasilewski J., 2013, Zarys deficyjny cyber przestrzeni, Przegląd Bezpieczeństwa Wewnętrznego, Wydawca Agencja Bezpieczeństwa Wewnętrznego, 5, 9, 225-234.
Wyzwania w cyber przestrzeni: przykłady rozwiązań, zagrożenia, regulacje, https://ik.org.pl/publikacje/wyzwania-w-cyberprzestrzeni-przykłady-rozwiązana-zagrożenia-regulacje/.