Joanna GRUBICKA

Pomeranian University in Słupsk

Department of National Security

Department of Safety and Civil Protection Engineering

joanna.grubicka@apsl.edu.pl

https://orcid.org/0000-0001-7934-6044

https://doi.org/10.34739/dsd.2022.02.06

SELECTED DETERMINANTS OF THREATS RESULTING FROM THE IMPLEMENTATION OF THE IOT/IOE CONCEPT

ABSTRACT: Access to the global Internet network has now become so common that it begins to control typical devices and very complex technological processes. This phenomenon is now referred to as the Internet of Things/Internet of Everything. Undoubtedly, the possibility of using this modern tool gives unlimited development opportunities, but it also poses many threats that can lead to catastrophic phenomena. The article discusses the risk assessment of threats and presents a practical methodology for risk analysis and estimation. The main purpose of the study is to identify the selected aspects and changes that affect the threats to transmitted information and the significant role of the user in the IoT/IoE information security system. According to the principle of information security management, the answers to the following questions should be included: 1) What is digital (information) security?; 2) What is digital (information) security management?; 3) What are the key challenges faced by information security management in the IoT/IoE ecosystem?; 4) Are these solutions secure enough to be implemented in information delivery systems? Verification of the given reason and providing answers to additional questions required a critical analysis of selected items of the subject category. The results of many years of the author's research on this issue were also made conditional.

KEYWORDS: information, information security, threats, security, Internet, risk, risk analysis

WYBRANE DETERMINANTY ZAGROŻEŃ WYNIKAJĄCE Z IMPLEMENTACJI KONCEPCJI IOT/IOE

ABSTRAKT: Dostęp do globalnej sieci internetowej stał się obecnie na tyle powszechny, że zaczyna sterować urządzeniami powszechnego użytku oraz bardzo złożonymi procesami technologicznymi. Obecnie nadano temu zjawisku termin Internet Przedmiotów/Internet Wszechrzeczy. Niewątpliwie możliwość wykorzystania tego nowoczesnego narzędzi daje nieograniczone szanse rozwoju, niemniej jednak stwarza wiele zagrożeń, które mogą doprowadzić do zjawisk katastrofalnych. Artykuł poświęcony jest ocenie ryzyka wystąpienia zagrożeń oraz prezentuje praktyczną do wykorzystania metodologię analizy i szacowania ryzyka. Głównym celem opracowania jest wskazanie wybranych aspektów i zmian, które mają wpływ na zagrożenia dla przesyłanej informacji oraz znaczącą rolę użytkownika w systemie bezpieczeństwa informacji IoT/IoE. Ponadto koncepcja zarządzania bezpieczeństwem informacji powinna w szczególności precyzować odpowiedzi na następujące pytania: 1) Czym jest bezpieczeństwo cyfrowe (informacyjne)?; 2) Na czym polega zarządzanie bezpieczeństwem cyfrowym (informacyjnym)?; 3) Jakie są kluczowe wyzwania stojące przed zarządzaniem bezpieczeństwem informacyjnym w ekosystemie IoT/IoE?; 4) Czy istniejące rozwiązania w ekosystemie są wystarczająco bezpieczne, aby można je było wdrażać do systemów przetwarzających informacje? Weryfikacja powyższej hipotezy oraz podanie odpowiedzi na powyższe pytania wymagało dokonania krytycznej analizy wybranych pozycji literatury przedmiotu. Uwzględniono także wyniki badań autorki w zakresie tej problematyki.

SŁOWA KLUCZOWE: informacja, bezpieczeństwo informacji, zagrożenia, bezpieczeństwo, Internet, ryzyko, analiza ryzyka

INTRODUCTION

Digitization as a continuous process of convergence of the real and virtual world is becoming the main driver of innovation and change in most sectors of the economy. The key factors driving the development of the digital economy are currently: the Internet of Things (IoT) and the Internet of Everything (IoE), hyperconnectivity, cloud-based applications and cloud computing, Big Data Analytics (BDA) and Big-Data-as-a-Service (BDaaS), automation and robotization, -multi-channel and omni-channel models of product and service distribution[1]. However, the context of constant business changes and the evolution of modern technologies have had a significant impact on what was previously called *cybersecurity*[2] and has slowly replaced it with the broader term *digital security*.

Digital security (cybersecurity, security in the digital environment) is usually understood as information security, (...) "as an element of an IT system (...), as a synonym for computer, telecommunications or network security"[3]. Digital security is aimed at ensuring safe activity of various types of entities in the digital environment and counteracting threats related to the security of networks, servers, data on devices, etc.

Due to the very rapid development of IoT/IoE devices, consumers and entrepreneurs have the opportunity to use many innovations in various areas, thus increasing the number of potential attack points. The research used methods of social sciences with a qualitative orientation as well as methods of problem analysis and solution analysis methods. A significant contribution to the research was made by the method of critical analysis of the literature on the subject. The research objective of searching both Polish and foreign literature on the subject is to analyze the impact of threats on the security of cyberspace functioning resulting from the implementation of the IoT / IoE concept. To achieve the above goal, a research problem was defined, which is as follows: Does the use of modern information technologies and IoT/IoE devices pose a threat to cyberspace users, and to what extent? Detailed problems: Therefore, one should ask whether these solutions are already secure enough to be implemented in information processing systems? Furthermore, it should be checked whether appropriate mechanisms are already in place to secure these closely connected systems so that the introduction of such solutions can be safely used.

INTERNET OF THINGS/OBJECTS/ INTERNET OF EVERYTHING AS KEY COMPONENTS OF THE ECOSYSTEM

IoT has the potential to add a new dimension to this process by enabling communication not only between people and smart objects but also communication between such smart objects

[1] J. Pieriegud, *Cyfryzacja gospodarki i społeczeństwa – wymiar globalny, europejski i krajowy* [in:] J. Gajewski, W. Paprocki, J. Pieriegud (ed.), *Cyfryzacja gospodarki i społeczeństwa – szanse i wyzwania dla sektorów infrastrukturalnych*, Gdańsk 2016, p.11.

[2] See: C. Banasiński (ed.), *Cyberbezpieczeństwo. Zarys wykład*, Warsaw 2018, pp. 27-33.

[3] L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego*, "Zeszyty Naukowe" 2014, 2(10), p. 212.

alone. M2M technology allows for communication and data collection, e.g. between computers, sensors, embedded processors, and mobile devices[4]. Eventually, it enables decision-making, most often automatically, without human intervention[5]. For such a combination of objects, two conditions must be met: power and connectivity. Therefore, today the Internet of Things is mainly in enterprises and homes. Applications using this technology are developing in mobile phones that are widely used, have power and connectivity[6]. IoT can be determined as "a set of all devices that are capable of network communication and that are able to process data sent over the network to some extent and are also uniquely identified in this network"[7]. In a forward-looking and general way, Min-Woo Ryu, Jaeho Kim, Sang-Shin Lee and Min-Hwan Song[8] define IoT as "the connection between anyone, anytime and anywhere". Therefore, the concept of IoT can be reduced to specifying that it is an ecosystem in which objects equipped with sensors communicate with computers[9]. It includes devices of various types of everyday life that start to go online, and human intervention is not necessary or essential. Its elements are connected via the Internet, but data exchange between them takes place via the ICT/IP protocol.

Regardless of the adopted definition, each IoT ecosystem is built of similar types of components. At the basic level, it is formed by the so-called end points of the system, which are sensors and actuators performing one type of function, monitoring changes, i.e. movement, temperature, humidity, location, etc. Due to their connection capabilities, they have the ability to perform two tasks, i.e. collecting and analyzing data from the environment and connecting via the Internet to control systems. The second level of the IoT ecosystem consists of the so-called simple hubs, i.e., joining points of a relatively small number of sensors and actuators. Due to the IT components (hardware and software) contained in them, embedded in specific products, they enable optimization of their operation and adaptation of their functioning to the user's habits. They are transformed into so-called intelligent, connected products. They can be an integral part of a specific product or be attached to it. In the social aspect, they can be so-called technologies worn in the form of sensors placed on the human body, e.g. a watch, a heart rate band, etc. To receive information, you must have a device that receives the transmitted signal and processes it into a specific reaction. The device can be a computer, tablet, smartphone, or other mobile device. Thanks to them, you can read the information sent from

[4] J. Grubicka , E. Matuska, *Employer branding and Internet security*, [in:] Christiansen B., Chandan H.C. (eds), *Handbook of Research on Industrial and Organizational Psychology in the Modern Workforce*, Hersey 2017, pp. 357-378.

[5] The Global Wireless M2M Market, Berg Insight, 04.2012, p. 2, http://www.berginsight.com/ReportPDF/ProductSheet/bi-globalm2m4-ps. pdf (19.12.2022).

[6] C. Associati, *The Evolution of Internet of Things, Focus*, 02.2011, p. 14, http://www.casaleggio.it/pubblicazioni/Focus_internet_of_things_ v1.81%20-%20eng.pdf (17.12.2022).

[7] J. Heppelmann, M. Porter, *How Smart, Connected Products Are Transforming Competition*, "Harvard Business Review" 2014, November, p. 64-88; A. Działdowski, *Internet rzeczy – wyzwania dla bezpieczeństwa,* „Networld" 2014, no. 7-8, p. 34.

[8] M.-W. Ryu, J. Kim, S. Lee, M.-H. Song, *Survey on Internet of Things: Toward Case Study*,"Smart Computing Review" 2012, 2(3), pp. 125-137.

[9] S. Vongsingthong i S. Smanchat, *Internet of Things: a Review of Applications and Technologies, Suranaree "*Journal Science and Technology" 2014, 21(4), p. 359.

the sensor. Another element of the ecosystem is the means of communication through which we can send data from the sensor to the device. So far, the most commonly used technologies have been Wi-Fi, Bluetooth, or NFC[10].

The third level of the IoT ecosystem is the so-called integrating hubs. They connect simple nodes, offering a wide range of similar types of service bundled together. At the same time, an appropriate infrastructure layer is necessary for the overall functioning of the IoT ecosystem. Its creation is not possible without the use of a number of leading technologies, which themselves have a huge transformational potential. This applies to cloud computing[11], Big Data, and mobile solutions[12]. The IoT network consists of six hierarchical layers: code, perception, network, middleware, application, and business.

The coding layer ensures the identification of items. In this layer, each object is assigned a unique identifier that allows the device to be recognized. The next layer gives physical meaning to each object. It consists of various types of sensors that receive programmed states or incidents[13]. An example of this type of sensors can be infrared sensors, temperature, air humidity, speed, position of objects, RFID tags. This layer collects information from sensors-equipped devices and converts it into digital signals, which are then transferred to the network layer for further operation. The next layer of the network is responsible for transmitting digital signals from the perception layer to the middle layer thanks to various data transmission standards on the Internet, i.e.: WiFi, Bluetooth, WiMaX. The following protocols should also be distinguished: IPv4, IPv6, MQTT, DDS[14]. The middle layer processes information received from sensory devices, i.e. sensors. It includes cloud computing technologies that provide direct access to the database and stored information. The data is automatically processed to obtain the desired information, also referred to in the literature as intelligent data processing. The application layer implements all possible aspects of IoT. It expresses the need to use the Internet of Things in a given field. It is application software for devices that are used for a specific purpose, e.g. they support the operation of a smart home, transport, production. The application layer is developed to support and specify IoT activities. The last layer is the business layer. It manages IoT applications and services. It is also responsible for all activities on the network.

[10] A. Mateos, J. Rosenberg, *Chmura obliczeniowa. Rozwiązania dla biznesu*, Gliwice 2011, p. 62

[11] J. Wielki, *Analiza szans, możliwości i wyzwań związanych z wykorzystaniem Internetu rzeczy przez współczesne organizacje gospodarcze*, „Przedsiębiorczość i Zarządzanie" 2016, 17(11), part 1: Agile Commerce – zarządzanie informacją i technologią w biznesie, pp. 127-140.

[12] J. Heppelmann, M. Porter, *How smart, connected products are transforming companies*, "Harvard Business Review" 2015, October, pp. 96-114; L. Zeng, *A Security Framework for Internet of Things Based on 4G Communication*, "International Conference on Computer Science and Network Technology (ICCSNT)" 2012, pp. 1715-1718; R. Dobbs et al., *No Ordinary Disruption, PublicAffairs*, New York 2015, p. 38.

[13] D. Bandyopadhyay, J. Sen, *Internet of Things – Applications and Challenges in Technology and Standardization*, "Wireless Personal Communications" 2011, 1(58), p. 2.

[14] Y. Zhang, *Technology Framework of the Internet of Things and Its Application*, "Electrical and Control Engineering (ICECE)" 2011, p. 4111.

Threats Resulting From the Implementation of the Concept of the Internet of Things/Objects/ Internet of Everything in Selected Areas of Application

It is a common misconception that protective measures eliminate risks, which is not true because the existence of a risk cannot be influenced. An example of this is the destruction of the infrastructure supplying the ICT system as a result of atmospheric discharges. The ICT system administrator, being aware of the risk, should take measures to ensure continuity of the system operation and availability of information by providing an emergency power supply. In this way, the vulnerability is eliminated, minimizing the possibility that the threat affects the protected ICT system. The implementation of safeguards is therefore aimed at minimizing or eliminating vulnerabilities that could be exploited by a threat. Threats to information processed in the ICT system have been divided into the following groups[15]:

- *Force majeure* (e.g. accidents, catastrophes, natural disasters) resulting in destruction of data, physical resources, and unavailability of information.
- *Unauthorized and criminal actions of people*: - threats related to physical theft or loss of equipment, - threats related to eavesdropping of hardware or software, - unauthorized actions of personnel, - unauthorized actions of third parties.
- *Unconscious mistakes* of the personnel operating the computer system – possible consequences include the violation of the protection of each of the attributes of secure information.
- *Consequences of poor organization of work* – also risks related to errors in physical and technical protection.
- *Hardware failures and damage, and software defects*.

The above hazard classification identifies five basic classes. Among the possible incidents in the force majeure category, there may be a fire. In the category of unauthorized and criminal activities of people, an attempt of a deliberate hacker attack. An unconscious mistake of the staff may be accidental disclosure of access data to the information processing system. Poor organization of work may result in improper security of physical access to the system[16]. Hardware failures and damage, as well as software defects, are a very large group of incidents. These include hardware imperfections that result in failures, physical damage, and software defects resulting in vulnerabilities that can be exploited by a hacker. It is very difficult to protect against the last of the above-mentioned groups of incidents, because a software error or hardware defect does not have to be known, and if it is identified, it is only during the investigation of the causes of a failure or attack, i.e. after the occurrence of an information security breach incident.

The number of applications in the IoT area is growing exponentially from very sophisticated military applications to an innumerable number of general applications. A significant

[15] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warsaw 2008, pp. 39-45.

[16] See: J. Grubicka, *Bezpieczeństwo konsumenta jako uczestnika e-rynku*, [in:] H. Lisiaka, W. Stach (eds.), *Bezpieczeństwo współczesnego świata. Historia i bezpieczeństwo publiczne*, Poznań 2012.

threat resulting from the implementation of the Internet of Things concept may be the multiplicity of data for the user and the problem with their absorption and interpretation. The right direction will be to provide information already processed automatically by the subject in a simple, understandable form. A separate problem is adjusting the speed of information processing to the appropriate form of the message and sending it to the recipient[17] at the right time.

The basis for the security of an ICT system is a well-developed security system design. Using already developed standards and regulations makes it much easier to create from scratch or modify the existing security architecture. A very comprehensive and up-to-date standard is STIG[18]. It is an acronym for the English words Security Technical Implementation Guide. It is a set of standards that define the methodology for the installation, operation, and management of computer devices and software. The guidelines developed for the purposes of the US Department of Defense by the government agency DISA (Defence Information Systems Agency) are still being developed and updated by it[19]. STIG's recommendations show how to significantly increase the system's chances of resisting attacks and how to minimize losses in the event of successful penetration of the security system. The standards also define the processes related to the administration of operating systems, such as software updates and the installation of security patches. The guidelines are also a starting point for non-standard configurations, those that must meet strict requirements imposed by legal or industry standards. In the US, all devices operating under the control of the Department of Defense[20] are required to meet the STIG standards. The necessary factor that determines the usefulness of the implemented security system in the course of operation is supervision and management by continuing its development. The efficiency of the security system is achieved by the ongoing elimination of vulnerabilities, improving the qualifications of users, and testing the implemented protection. The system is consistent if there are one or more safeguards for each vulnerability.

In the area of IoT, no standards are developed that would ensure compatibility between devices from different manufacturers. The lack of standardization and agreement between manufacturers makes the transition from one manufacturer's device to another device a serious challenge, even for an experienced user.

Along with the general challenges related to IoT/IoE, challenges related to data, their sources, quantity, multidimensionality, quality, information that can be obtained from them and business value that can be translated into a specific goal of the organization are identified. This data comes from different sources, contains different types of data and comes in different formats. To some extent, it is irrelevant from the point of view of the purpose of any organization and contains incorrect or untrue information. Therefore, it is a serious challenge to assess its

[17] I. Maj*, Internet rzeczy i zagrożenia z nim związane, Bezpieczeństwo. Teoria i praktyka,* „Bezpieczeństwo. Teoria i Praktyka" 2015(3), pp. 51-57.

[18] J. Muniz, A. Lakhani, *Web Penetration Testing with Kali Linux*, Birmingham 2013, p. 254.

[19] Standardy STIG – aspektów bezpieczeństwa teleinformatycznego, https://public.cyber.mil/stigs/downloads/ (2.01.2022).

[20] J. Muniz M., *Web Penetration Testing* …, op. cit., 254.

quality. An example is content from social networks, where it is not known whether users tell the truth in them and whether they do not create the so-called second life, creating a new, different image of themselves on portals. The banking sphere and other entrepreneurs, relying on false data, are therefore exposed to making wrong decisions. An undesirable result will be exposing oneself to additional costs or losses related to, for example, a poorly prepared marketing campaign or granting a loan to a person unable to repay it.

How to understand a large amount of data? How to translate data into information? Which are important? How do we draw conclusions? The answer to these questions becomes a serious problem. To understand data and draw appropriate conclusions from it, both new tools for data analysis and high analytical skills of people dealing with information processing are needed. Understanding data has become a focus of research and investment among organizations. In addition, responses to the influx of information are expected in real time. Entire industries have sprung up dedicated to data collection and understanding.

Another challenge, perhaps the most important, is security. The concept of data security is understood as the security of information collected by devices connected to the network. What, on the one hand, can be considered as a benefit resulting from the use of modern technology, on the other, one can be treated as a threat. Under these circumstances, a potential IoT issue could be device ownership. After purchase, we physically own it, but it is not fully our property. Problems remain to be resolved: who is the owner of the collected data? Are there any restrictions on the transfer of data to third parties? Up to what point are software updates free of charge, paid for when purchasing the device? To what extent do we have access to the collected data? Does the collected data constitute a danger?[21] The disadvantage of this type of ecosystems may be that the manufacturer will remotely decide on the functions provided by the device. Enterprises that decide to implement IoT/IoE technology must have an infrastructure that will guarantee uninterrupted circulation and access to information, and thus the security of the entire digital ecosystem. Unfortunately, practice shows that the policy in this area is full of loopholes.

The Internet of Things is a completely new threat to the IT security of companies. It means the need to apply tighter protection not only to the so-called critical infrastructure, but to all the networks in the company. Security departments and IT companies specializing in cyber protection face new challenges related to the increased risk of attacks referred to as Denial of Service, i.e., overloading the infrastructure with an avalanche of requests, or the risk of hacking into business applications through systems supervising communication between devices[22].

The effective takeover of control over a network of strategic sensors or machines has unimaginable consequences. This could be prevented through better control of virtual private

[21] R. Weber, *Internet of Things – New security and privacy challenges*, “Computer Law & Security, Review" 2010, January, Vol. 26, pp. 23-30.

[22] Ł. Kryśkiewicz, *Wyzwania IoT w biznesie – potencjalne zagrożenia i niedogodności*, http://di.com.pl/wyzwania-iot-w-biznesie-potencjalne-zagrozenia-i-niedogodnosci-56027 (23.06.2021).

networks, at least partly. However, adequate physical protection of devices and sensors that provide data to applications will remain a huge challenge.

Consideration should also be given to the implementation or strengthening of encryption systems to protect data in networks, cloud services, and end devices.

It should be emphasized that the IoT is based on various information related to a person, including their interests, 'parameters' of the body, and habits. This information, as personal data, may be protected under the Personal Data Protection Act and pose a serious threat to privacy. While objects, not people, are at the heart of IoT, objects serve people, which is why personal data about individuals is ultimately crucial. In the IoT, the user leaves a full history of all banking and card operations, as well as location data, including by providing a locator in mobile telephony and many tags indicating the use of household appliances, TV, car, GPS, home and personal computers[23]. The development of new applications of the Internet of Things must go hand in hand with trust in it and with providing guarantees to citizens regarding the non-use by unauthorized persons of information generated on the network. Without trust in this system, it is not possible to use its full potential.

One should consider whether it will be risk-free. Will there not be a situation where someone or something causes interference in the functioning of objects connected to the network? Will the forces of nature, otherwise unpredictable, cause damage to the power grids that power devices that allow unlimited access to the Internet? What then?

When talking about IoT/IoE security, one should take into account how much data is shared or used by the devices within it. In a hypothetical situation, the Internet of Things may collect so much information that it becomes a threat to our privacy, and errors in the functioning of the infrastructure leading to incorrect decisions, for example, the traffic management system, may affect our security. Other threats to freedom and privacy may be related to complete surveillance related to facial recognition systems. Cameras in shops, hotels, the city, at railway and airport stations, on roads give the opportunity, through the face recognition system, to trace the history of our travels, as well as follow us online. We should also mention a simple, generally available, photo search software on the Internet based on a face photo. Many devices that enable reading the data contained in them using contactless technology are susceptible to eavesdropping and skimming, i.e. illegal copying of content without the knowledge of its owner to create copies and perform unauthorized transactions[24]. The advantage of data processing by autonomously operating IoT/IoE is the fact that they can do it much more effectively than a human, whose attention is usually not focused on one problem. This is an advantage, but also a problem, because until we are ready to fully trust artificial intelligence systems, IoT / IoE intelligence

[23] J. Grubicka, *Internet Rzeczy - wyzwanie czy zagrożenie?*, [in:] J. Grubicka (ed.), *Zagrożenia i bezpieczeństwo współczesnego człowieka w cyberprzestrzeni*, Słupsk 2018, pp. 129-131.

[24] A. Kobyliński, *Internet przedmiotów: szanse i zagrożenia*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2014, 112(1), pp. 101-109; B. Józefiak, *Internet rzeczy nie będzie bezpieczny*, CyberDefence24, http://www.cyberdefence24.pl/384609,internet-rzeczy-nie-bedzie-bezpieczny (8.11.2022).

depends on how we program it ourselves. IoT/IoT hardware is by definition not dangerous. Dangers are associated with their users. The user will be exposed to the following list of threats:

- violation of privacy by stealing data provided by devices that take pictures of people and the environment or collect audio recordings;
- access to the settings of the equipment, for example, a car, through the Wi-Fi network it creates;
- disclosure of information about our whereabouts, information about the apartment;
- taking control of automated logistics systems in shops and companies;
- an incorrect decision of the system analyzing data from Internet of Things devices may be a threat not only to the equipment, but also to our personal safety;
- stealing identification data collected in mobile electronics.

Threats are not part of the IoT/IoE concept. However, it was not created from scratch but uses existing Internet infrastructure and mobile technologies. Therefore, the problems of cybercrime and insufficient security known in the old world of computers also apply to the world of IoT/IoE.

Lack of electricity supply and, consequently, lack of supplies of basic needs for people, including lack of water, food, serious disruptions in road, rail, and air transport. Lack of fuel supplies necessary for the normal operation of transport and many other structures, including those responsible for security. All of this was caused by the terrorist activity of a group of people who interfered with the electricity supply system by using IoT access. Terrorists caused the entire electrical supply system to malfunction by entering incorrect codes into the electricity meters in the private homes of recipients, which were wirelessly connected to the global Internet network[25].

The consequences of such an action have been and may cause many failures and technological disasters in industrial plants processing chemical substances. The effect can be serious, contamination of the natural environment, water intake sources, as well as soil intended for cultivation. This may be compounded by failures in nuclear power plants and the release of radioactive elements into the natural environment, which for many decades destroyed the soil and surface waters and, in many cases, caused the population to be exposed to their effects, leading to radiation sickness.

What if, in fact, a terrorist group, especially in the current era of operation of many terrorist groups with extremely religious background or the current Russian invasion of Ukraine (February 24, 2022) will lead to the events described above? And what if, as a result of extreme weather phenomena, storms, heavy rains, strong winds, and hurricanes, they cause disruptions in the functioning of networks supplying IT systems, and the consequence will be improper operation of other infrastructures? The consequence may be serious disruptions in the operation of critical infrastructure elements at the local, regional, and even national level.

[25] B. Fura, M. Fura, *Green jobs in the European Union – an empirical study,* “Acta Universitatis Lodziensis. Folia Oeconomica” 2016, 2(319), pp. 39–53.

THREAT RISK ANALYSIS

However, the development of IoT/IoE also involves risks. Implementing this concept in practice is a technical and social challenge. The key aspect here is data management. Given a world of connected things constantly exchanging different types of information, the volume of data generated and the number of processes involved in processing this data is critical.

An inseparable element of management is awareness of the existence of risk, its assessment (estimation), risk management, i.e., acceptance of its level, and ways of mitigating or eliminating it. Research by the SANS[26] Institute has identified the greatest risks associated with the Internet of Things, which include: problems with updating the software of objects, the use of objects as the least secure entry points into the network for subsequent infections or attacks, DoS (Denial of Service) attacks, which, in the case of, for example, power grid infrastructure or medical devices, may lead to serious consequences, unauthorized modifications of device operating parameters, users' errors, and accidental modifications, which from networks of very strongly interconnected systems may lead to unpredictable consequences on the scale of all devices of the interconnected system devices. The concept of risk, as the possibility of a specific undesirable effect occurring at a certain time and under certain circumstances, is represented by a simple mathematical formula, a combination of two components: the probability of the occurrence of a threat causing undesirable effects and the magnitude of the effects caused by the threat[27]:

$$\mathbf{R = P \text{ x } S}$$

where:
R – risk, P – probability of occurrence, S – effect (size of losses or damages).

In classical mathematical decision theory, risk refers to a situation in which the choice of a given decision variant entails the possibility of various negative and positive consequences with a known probability of the occurrence of each possibility. Formally, decisions taken under risk conditions are a class of decision problems in which the probability distribution of all its consequences[28] is known for each possible decision. The contemporary technical culture and the tradition of engineering awareness allow for a broader view of the continuity of technical systems. The impact of the natural environment,, the technical environment and the social environment on the continuity of operation of various systems[29], including safety management systems, is taken into account. Currently, risk is defined as a four-element set calculated using finite element method[30]:

[26] J. Pescatore, *Securing the Internet of Things Survey*, SANS Institute InfoSec Reading Room, http://www.sans.org/reading-room/whitepapers/covert/securing-internet-thingssurvey-34785 (5.12.2022).

[27] K.R. Zieliński, *Ochrona ludności. Zarządzanie kryzysowe*, Warszawa 2017, p. 70.

[28] T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warsaw 2005.

[29] J.R. Rak, M. Kwietniewski, *Bezpieczeństwo i zagrożenia systemów zbiorowego zaopatrzenia w wodę*, Rzeszów 2011, p. 23-28.

[30] J. Rak, B. Tchórzewska-Cieślak, *Metoda analizy i oceny ryzyka w systemie zaopatrzenia w wodę,* Rzeszów 2005, p. 45-52.

$$\mathbf{r = (S_i, P_{Si}, C_{Si}, O_{Si})}$$

where:
Si – finite accident scenario, PSi – probability of occurrence of the finite emergency scenario, CSi – the amount of losses caused by the implementation of the finite emergency scenario, OSi – protection against the finite emergency scenario.

Great civilization and environmental catastrophes caused interest in risk in the field of engineering and environmental protection. Currently, risk assessment is recognized as the basis for taking effective preventive measures to increase the level of security. The need to minimize the probability of a threat to life or health is particularly accepted[31]. The results of the risk assessment are the basis for taking corrective and preventive actions in the nature of risk management. Certainly, the issue of security, especially related to the local community and the functioning of various systems designed and intended for use by people, is far from solved if, despite the experts' high assessment of real security, there is a low sense of security. Referring to expert assessments is often missing the point. It often happens that an expert assessment is prepared for a specific need and is made based on a preconceived thesis of low or negligible risk related to the project. However, hiding the fact of the investment is unacceptable, as it violates the right to information. Therefore, it became necessary to consult with the local community on matters related to all projects, even those with a ‘zero’ risk. Nevertheless, what is safe for one person or group of society, according to one's own assessment, may be a threat[32] to other evaluators. Therefore, it is necessary to indicate which solutions, structures, and forms of action are accepted, tolerated, and which should be solved by immediate action. The justification should be completed in detail, taking into account the internal criteria and parameters used in a given institution.

CONCLUSIONS

IoT/IoE, based on cloud computing and devices connected by millions of supporting applications, does not create a uniform environment and is therefore exposed to numerous threats. Uncontrolled surveillance of people, threats resulting from hackers’ activities, and taking control of devices are the most important dangers that, along with the spread of IoT, will become real threats to the security of users. Vulnerabilities are found in a number of devices, and hackers can easily obtain passwords to access them with administrator privileges and then modify their system software to suit criminal purposes.

Threats arising from the Internet of Things/Internet of Everything should therefore be considered in two categories related to the computerization of the consumer world and optimization of the industrial sector. Using the Internet safely is the most important thing a consumer can do for the security of the IoT/IoE Internet. We just need to extend the understanding of the

[31] See: R. Wolniak, B. Skotnicka, *Metody i narzędzia zarządzania jakością. Teoria i praktyka*, Gliwice 2007.
[32] J. Wolanin, *Zarys teorii bezpieczeństwa obywateli*, Warsaw 2005, p. 64.

concept of digital security to this sphere of informatization of our lives. We need to understand that by keeping our computers safe, we eliminate numerous loopholes that cybercriminals can use to enter our world. We need to be aware that our computer may be infected with a virus, which can lead to data loss. We need to accept the fact that a cyber spy can steal our data and, based on it, expose us to financial losses and even put us in conflict with the law by using our identity for criminal activities. We need to know that smartphones can be dangerous, especially when they fall into the hands of a thief with a large database of information about us and our lives. Any prudent user of computers, mobile devices, and digital services seems to know all these things. It seems that, as practice shows, many people do not use modern technologies wisely.

REFERENCES

Ashton K. 2009. "That 'Internet of Things' Thing. In the real world, things matter more than ideas." RFID Journal, http://www.rfid journal.com/articles/pdf?4986.

Associati C. 2011. The Evolution of Internet of Things, Focus, http://www.casaleggio.it/pubblicazioni/Focus_internet_of_things_ v1.81%20-%20eng.pdf.

Banasiński Cezary (ed.). 2018. Cyberbezpieczeństwo. Zarys wykładu [Cybersecurity. Lecture outline]. Warsaw: Wolwers Kluwer.

Bandyopadhyay Debasis, Sen Jaydip 2011. "Internet of Things – Applications and Challenges in Technology and Standardization." Wireless Personal Communications 1(58): 49-69.

Biedugnis Stanisław, Smolarkiewicz Mariusz, Podwójci Paweł, Czapczyk Andrzej. 2009. „Ciągłość działania rozległych układów technicznych [Continuity of operation of extensive technical systems]" Rocznik Ochrona Środowiska, Vol. 11: 1077-1082.

CERT Polska. 2019. Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2019 z działalności CERT Polska [The security landscape of the Polish Internet. Annual report 2019 on the activities of CERT Polska], https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.

Dobbs Richard et al. 2015. No Ordinary Disruption, PublicAffairs. New York: PublicAffairs.

Działdowski A. 2014. „Internet rzeczy – wyzwania dla bezpieczeństwa", Networld No. 7-8.

Fura B., Fura M. 2016. "Green jobs in the European Union – an empirical study". Acta Universitatis Lodziensis. Folia Oeconomica 2(319): 39–53.

Grubicka Joanna, Matuska Ewa, 2017. Employer branding and Internet security In Christiansen B., Chandan H. C. (eds) Handbook of Research on Industrial and Organizational Psychology in the Modern Workforce, IGI Global Publ.

Grubicka Joanna. 2012. Bezpieczeństwo konsumenta jako uczestnika e-rynku [Consumer security as a participant in the e-market] In Lisiaka H., Stach W. (eds.) Bezpieczeństwo współczesnego świata. Historia i bezpieczeństwo publiczne [Security of the modern world. History and public safety], Instytut Naukowo Wydawniczy Maiuscula.

Grubicka Joanna. 2018. Internet Rzeczy - wyzwanie czy zagrożenie? [Internet of Things – A challenge or a threat?] In Grubicka Joanna (ed.), Zagrożenia i bezpieczeństwo współczesnego człowieka w cyberprzestrzeni [Threats and security of modern man in cyberspace], Wydawnictwo Społeczno – Prawne.

Józefiak Bartosz. 2016. Internet rzeczy nie będzie bezpieczny [The Internet of Things will not be safe]. CyberDefence24, http://www.cyberdefence24.pl/384609,internet-rzeczy-nie-bedzie-bezpieczny.

Kaczmarek Tadeusz. 2005. Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne [Risk and risk management. Interdisciplinary approach]. Warszawa: Wydawnictwo Difin.

Kobyliński A. 2014. „Internet przedmiotów: szanse i zagrożenia [Internet of Things: Opportunities and Threats]". Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług 808(112).

Kryśkiewicz Łukasz. 2016. Wyzwania IoT w biznesie - potencjalne zagrożenia i niedogodności [IoT Challenges in Business – Potential Threats and Inconveniences]. In http://di.com.pl/wyzwania-iot-w-biznesie-potencjalne-zagrozenia-i-niedogodnosci-56027

Liderman Krzysztof. 2008. Analiza ryzyka i ochrona informacji w systemach komputerowych [isk analysis and protection of information in computer systems]. Warsaw: PWN.

Mateos Arthur, Rosenberg Jothy. 2011. Chmura obliczeniowa. Rozwiązania dla biznesu [Cloud computing. Solutions for business]. Gliwice: Helion.

Mitnick Kevin. 2003. Sztuka podstępu – łamałem ludzi, nie hasła [The art of deception – I broke people, not passwords]. Gliwice: Helion.

Pescatore John. 2014. Securing the Internet of Things Survey, SANS Institute InfoSec Reading Room, http://www.sans.org/reading-room/whitepapers/covert/securing-internet-thingssurvey-34785.

Pieriegud Jana. 2016. Cyfryzacja gospodarki i społeczeństwa – wymiar globalny, europejski i krajowy [Digitization of economy and society – Global, European and national dimensions] In: Gajewski Jerzy, Paprocki Wojciech, Pieriegud Jana (ed.), Gdańska Akademia, Cyfryzacja gospodarki i społeczeństwa – szanse i wyzwania dla sektorów infrastrukturalnych [Digitization of economy and society - opportunities and challenges for infrastructure sectors], Gdańska Akademia Bankowa.

Polski Komitet Normalizacyjny [Polish Committee for Standardization]. 2002. Technika informatyczna, Zabezpieczenia w systemach informatycznych – terminologia [Information technology, Security in information systems - terminology]. Warsaw: PKN.

Porter Michael, Heppelmann James. 2014. "How Smart, Connected Products Are Transforming Competition". Harvard Business Review, November. https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition.

Porter Michael, Heppelmann James. 2015. "How smart, connected products are transforming companies". Harvard Business Review, October. https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies.

Rak Janusz, Kwietniewski M. 2011. Bezpieczeństwo i zagrożenia systemów zbiorowego zaopatrzenia w wodę [Safety and threats to collective water supply systems]. Oficyna Wydawnicza Politechniki Rzeszowskiej.

Rak Janusz, Tchórzewska-Cieślak Barbara. 2005. Metoda analizy i oceny ryzyka w systemie zaopatrzenia w wodę [Method of risk analysis and assessment in the water supply system]. Oficyna Wydawnicza Politechniki Rzeszowskiej.

Ryu M.-W., Kim J., Lee S.– S., Song M. – H. 2012. „Survey on Internet of Things: Toward Case Study". Smart Computing Review 2(3): 125-137.

Sarnowski Janusz, Prokopowicz Dariusz. 2015. Zastosowanie innowacji marketingowych w przedsiębiorstwach w Polsce [The use of marketing innovations in enterprises in Poland] In M. Sitek, T. Graca (ed), "Nowe wyzwania dla Europy XXI wieku w dziedzinie zarządzania i edukacji [New challenges for Europe of the 21st century in the field of management and education]", post-conference edition, Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie, 135-156.

Sulich Adam, Zema Tomasz. 2020. Role of the Management in the World Driven by the Industry 4.0 In "Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development during Global Challenges". Conference Paper, 2565-2576. DOI: 10.5281/zenodo.4083795.

The Global Wireless M2M Market, Berg Insight. 2012, http://www.berginsight.com/ReportPDF/ProductSheet/bi-globalm2m4-ps. pdf.

Vongsingthong Suwimon, Smanchat Sucha. 2014. "Internet of Things: a Review of Applications and Technologies". Suranaree Journal Science and Technology 21(4): 359-374.

Warren James, Marz Nathan. 2016. Big Data. Najlepsze praktyki budowy skalowalnych systemów obsługi danych w czasie rzeczywistym [Big Data. Best practices for building scalable real-time data handling systems]. Warszawa.

Wasilewski Janusz. 2013. "Zarys definicyjny cyberprzestrzeni [Definitional outline of cyberspace]". Czasopismo Przegląd Bezpieczeństwa Wewnętrznego 9(5): 225-234.

Weber Rolf H. 2010. "Internet of Things – New security and privacy challenges". Computer Law & Security, Review 26(1): 23-30. DOI: 10.1016/j.clsr.2009.11.008.

Whitmore Andrew, Agarwal Anurag, Xu Li. 2015. "The Internet of Things – A Survey of Topics and Trens". Information Systems Frontiers 17: 261–274. https://doi.org/10.1007/s10796-014-9489-2.

Więcaszek-Kuczyńska Lidia. 2014. "Zagrożenia bezpieczeństwa informacyjnego [Information security threats]". Zeszyty Naukowe 2(10): 201-233.

Wielki Janusz. 2016. "Analiza szans, możliwości i wyzwań związanych z wykorzystaniem Internetu rzeczy przez współczesne organizacje gospodarcze [Analysis of opportunities and challenges related to the use of the Internet of Things by modern business organizations]". Przedsiębiorczość i Zarządzanie 17(11), Part 1: Agile Commerce – zarządzanie informacją i technologią w biznesie.

Wolanin J. 2005. Zarys teorii bezpieczeństwa obywateli [An outline of the theory of citizen security]. Warsaw: DANMAR.

Wolniak Radosław, Skotnicka Bożena. 2007. Metody i narzędzia zarządzania jakością. Teoria i praktyka [Quality management methods and tools. Theory and practice]. Gliwice: Wyd. Politechniki Śląskiej.

Zeng Lyuan. 2012. A Security Framework for Internet of Things Based on 4G Communication, "International Conference on Computer Science and Network Technology (ICCSNT)".

Zhang Ying. 2011. Technology Framework of the Internet of Things and Its Application, Electrical and Control Engineering (ICECE).

Zhou Keliang, Liu Taigang, Zhou Lifeng. 2016. Industry 4.0: Towards future industrial opportunities and challenges In 12th International Conference Fuzzy Systems Knowledge Discoveries, FSKD 2015. Retrieved January 26, 2022 from https://doi.org/10.1109/FSKD.2015.7382284.

Zieliński Krzysztof R. 2017. Ochrona ludności. Zarządzanie kryzysowe. Warsaw: Difin.