Cognitive Computing and Internet of Things, Vol. 43, 2022, 30–36
https://doi.org/10.54941/ahfe1001836

Internet of Things Security Policy in Enterprises

Michał Trziszka

Poznan University of Technology, J. Rychlewskiego 2, 60-965 Poznań, Poland

ABSTRACT

The aim of the article is to discuss the risks resulting from expanding access to the network of new devices, and at the same time to show to what extent the implementation of procedures in the field of data security and architecture of systems used for data processing may affect the security of the continuity of the company's technological processes, but also data protection. The author draws attention to the fact that the problem of data and process security in the Internet of Things should be considered not only in terms of the protection of the content of information, but also its authenticity and topicality. On the other hand, inadequate formulation of the rules of the Internet of Things security policy in a given enterprise may mean limiting the availability of solutions and access to data, often eliminating the possibility of obtaining and processing them altogether. Enterprises must therefore act in such a way as to help maintain both the functionality and security of their systems.

Keywords: Cybersecurity, Security policy, Internet of Things, IoT, Network risk, threats, Digitization, Data security

INTRODUCTION

Digitization, both in terms of the technological development of society and in terms of computerization of technological processes, brings many benefits, but at the same time requires the application of appropriate security measures, especially against the increasing threat of cyber attacks. For this reason, data protection should be considered company-wide, both in terms of operating systems, but also all devices connected to the network. Continuous communication between devices, which is the main feature of the Internet of Things, increases the likelihood of multiple data processing and transmission, and thus exposing information to additional threats. Much of the data collected in IoT systems may be sensitive, including personal information, about the activity and behavior of people, companies and devices. In this aspect, the key issue is to ensure appropriate procedures guaranteeing the security of collecting and transmitting data, not only technical, related to the technological sphere, but also the protection of personal data.

INTERNET OF THINGS AREAS IN THE CONTEXT OF CYBERSECURITY

The consumer sector, transport, production, utility media, retail, as well as business services are industries that have spent the most on Internet

© 2022. Published by AHFE Open Access. All rights reserved.

of Things technology (IoT) for years[1]. IoT systems are built from a huge number of connected devices as a point of unauthorized connections that cybercriminals can use to paralyze production systems and even terrorist attacks. Modern enterprises are creating more and more flexible and mobile workplaces. This process has particularly accelerated since March 2020, following the announcement of the global COVID-19 pandemic, when enterprises and public institutions rapidly moved their activity to the Internet and implemented remote work on a large scale[2]. All of them faced numerous challenges not only related to the implementation of changes, but also to maintaining the security of corporate information in an environment that extended far beyond the walls of a traditional office. Using solutions beyond the company's control can be fatal for the security of key data.

Communication in the Internet of Things process takes place not only between devices, but also remains in the configuration of a human device. For this reason, not only is the technological protection of access important, but also the behavior of the people who participate in this process. The security mechanism is useless if the user does not follow the rules of secure access and connection. Uncontrolled surveillance of people, threats resulting from hackers' activities and taking control of devices are the most important dangers[3] which, with the spread of IoT, will become real threats to user safety. Moreover, in the case of a company, a cyber attack may not only paralyze the entire enterprise and cause irreversible losses, but also expose customers and cooperators to theft of data. So regardless of the size and industry in which they operate, all enterprises are exposed to DDoS attacks[4], phishing or ransomware. Improper information management and failure to comply with security standards may expose the company to high financial and reputational losses.

[1]The value of the global IoT market, valued at USD 190 billion in 2018, will increase to USD 1.1 trillion in 2026, maintaining the growth rate at 24%. annually. By 2022, spending on IoT in all industries in the world will double on average, reaching a total of nearly $4 trillion. The forecasts show that in the years to come, apart from trade and services, the administration will invest the most: local governments (USD 140 billion in 2022) and central authorities (USD 118 billion in 2022). Healthcare and Education - up to $105 billion and $77 billion respectively in 2022. At the end of the list of industries that will grow along with the expenditure on the technology of the future will be: investment services (up to USD 12 billion) and banking (up to USD 8 billion). Source: 2020 IoT Market Report, https://cyfrowapolska.org/wp-content/uploads/2020/11/Raport_Rynek-IOT_2020_net.pdf [reading: 14.5.2021]

[2]Nearly 70 percent enterprises operating in Poland that had not yet offered remote work opportunities decided to take such a step after the outbreak of the coronavirus pandemic. Deloitte analysis: Remote work and teleworking during COVID-19 https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/newsletter-strefa-pracodawcy-podatki-i-prawo/praca-zdalna-a-telepraca-w-czasie-COVID-19.html [access: 14.5.2021]

[3]B. Józefiak, The Internet of Things will not be safe, CyberDefence24, http://www.cyberdefence24.pl/384609,internet-rzeczy-nie-bedzie-bezpieczny [access: 13.5.2021]

[4]DDoS attacks are currently the most likely threat to companies operating in the network, and their consequences extend beyond just the IT area, but also cause real, measurable financial and image losses. Attacks of this type are constantly evolving and becoming more and more precise. Their purpose is to use up all available resources of the network infrastructure or internet connection.

Figure 1: Relationships in security management. Source: Zielin'ski A., Personal data security, Office for Personal Data Protection

SECURITY POLICY - SECURITY PROCEDURES

As stated in the Encyclopedia of Management, the concept of security policy should be understood as all the principles, methods and tools for the protection and supervision of information: "It should include such elements as: information policy, protection of classified information, personal data protection rules, security policy of the ICT system, rules for the protection of business secrets or other professional secrets, prevention of crimes to the detriment of the company, especially forgery and fraud, rules of physical and technical protection, and other security related[5]". The security policy describes the assumptions regarding the protection of information in the company. It may concern its entire functioning or specific areas, such as:

1. Comprehensive security policy,
2. Personal data protection security policy (GDPR),
3. IT system security policy.

This division is often blurred, especially in small and medium-sized enterprises, where the overall security policy may constitute a decalogue of procedures and standards applicable in the enterprise, covering all or selected levels of its activity. In this case, they are in the form of general assumptions, without assumptions about specific areas. The issue is quite different in the case of enterprises operating in the Internet of Things technology, where the key is data security in the network, such as securing servers, instructions for responding to security incidents and configuring encrypted transmission of information between devices and employees supervising them (Figure 1).

The security policy is an internal document of the enterprise and should contain the following elements:

- information policy,
- IT system security,
- protection of classified information,

[5] More: https://mfiles.pl/pl/index.php/Polityka_bezpiecze%C5%84stwa [reading: 14.5.2021]

- GDPR rules,
- preventing crime to the detriment of the company,
- principles of physical and technical protection[6].

The main goal of the security policy is to create rules and principles for the proper protection of key data for the functioning of the enterprise as well as personal data of employees, customers and cooperating entities. It does not contain variable data that would cause frequent updating of the document. The data controller is responsible for approving the security policy. The document should be prepared in writing, and employees should confirm in writing their knowledge of the provisions of key rules for the enterprise from the point of view of data security[7].

The security policy should include:

- a list of rooms where the data processing will take place,
- a list of data sets and programs that are used in the data processing process,
- information on the flow of data between systems,
- description of organizational and technical measures to protect the data,
- a description of the data structure showing the links between information fields[8].

According to the above-mentioned Krzysztof Liderman, effective implementation of the security policy depends primarily on the awareness and degree of responsibility of the management staff, but also of each employee. Especially in the case of the Internet of Things, comprehensive data protection means being or not for modern companies. Inadequate information storage and sharing can have a disastrous effect on productivity, business continuity, organizational security and corporate reputation[9].

According to experts, humans are the weakest link in IT security systems. Simple mistakes, regardless of the quality of the applied security measures, expose organizations to financial losses and reputational risk the most. Employees' mistakes are usually made unconsciously and in good faith. The main cause of mishaps in this field is the improperly implemented employer's safety policy, the lack of sufficient control of employees' behavior during work and the lack of training. Although all companies currently process their strategic information in IT systems, many of them have trouble

[6]L. Kępa, *Ochrona Danych Osobowych w Praktyce*, Difin Publishing House, Warsaw 2014, pp. 272–274

[7]K. Liderman, *Bezpieczeństwo Informacyjne, nowe wyzwania*, Polish Scientific Publishers PWN, Warsaw 2017, pp. 229–230.

[8]The Polish Standard PN-ISO / IEC 27001 indicates that the purpose of the security policy is to support the management for information security and to provide directions for its activities. The security policy is to contain a set of rules and practices along with documentation on how the organization is to protect the processed personal data. Such a document is approved by the company's management and presented to all employees. Such a document is approved by the company's management and presented to all employees. If the security policy is to be compliant with the above ISO standard, additional information should be included, i.e. the definition of information security, emphasizing the intentions of the management, definitions of general obligations in the field of information security management, etc. Quotation. Kępa L., *Ochrona Danych Osobowych w Praktyce*, Difin Publishing House, Warsaw 2014, pp. 272–274

[9]J. Żywiołek, *Innowacyjność przepływów informacyjnych jako element udoskonalenia systemu informacji w przedsiębiorstwie logistycznym,* Scientific Journals of the Czçstochowa University of Technology Management No. 24 vol. 1 (2016).

implementing internal security policies - clear rules that define the rules for accessing IT infrastructure devices and the responsibility for violating these rules. Inappropriate records dilutes responsibility and promotes undesirable, harmful behavior of employees. Many other companies formally have a security policy but have not been properly implemented. Organizations cannot cope with its compliance, control and enforcement. Long-term neglect in this area increases IT risk and vulnerability to attacks in all areas of the security system[10].

SECURITY OF PERSONAL DATA ON THE INTERNET OF THINGS

The Internet of Things is characterized by the ubiquitous, often opaque collection and seamless connection of user data. Karolina Smolarek from Associate, Deloitte Legal emphasizes that „in order to use this functionality, Internet of Things devices and services must be connected and share data on user interactions with multiple nodes in the network. You also need to consistently identify users and devices across the entire network. The processing of personal data as part of the Internet of Things may cause difficulties in distinguishing between the data controller and the processor. This is because the use of IoT technology is usually based on finding correlations already during processing, predicting and creating forecasts, and supporting the decision-making process."[11].

IoT processes can pose numerous privacy threats. They are often designed in such a way that they are imperceptible to users in order to minimize the inconvenience to their use[12]. Low security standards and non-transparent operation of many devices and services included in the IoT contribute to increasing threats to privacy[13].

One of the European Union regulations serving to protect the data of natural persons are the provisions of the GDPR[14]. This regulation introduced restrictive provisions regarding the collection, storage and sharing of personal data collected online. The GDPR uses terms such as "the right to be forgotten" and the right to "data portability" which allow the user to easily transfer personal data between service providers. It does not cover the processing of personal data relating to deceased persons or legal persons. The provisions do not apply to the processing of personal data by a natural person in the

[10]The authors of the Deloitte report present the problem of security policy also in the national and military aspects: Defense Policy and the Internet of Things Disrupting Global Cyber Defenses, https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-IoT-defense-policy-and-the-internet-of-things.pdf [reading: 15.5.2021]

[11]K. Smolarek, Internet of Things, privacy protection and data security, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/Internet-Rzeczy-ochrona-prywatnosci-a-bezpieczenstwo-danych.html [reading:14.5.2021]

[12]S. Wachter, *The GDPR and the Internet of Things: A Three-Step Transparency Model*, Oxford Internet Institute University of Oxford.

[13]Currently, neither in Poland nor in the world there is a legal act regulating the Internet of Things in a comprehensive manner (horizontally), and there are no plans to pass such regulations. On the other hand, vertical regulations are adopted concerning only selected areas of IoT functioning. Quotation. X. Konraski, *Internet of Things - the most important legal regulations in Poland*, https://digitalandmore.pl/iot-regulacjeprawne/ [reading: 14.5.2021]

[14]Regulation (EU) 2016/679 of the European Parliament and of the Council

course of a purely personal or domestic activity, provided that it is not related to a professional or commercial activity[15]. Regardless of the protection specified in the GDPR, the privacy of IoT device users is also protected on the basis of writing. art. 173 of the Act of July 16, 2004 - Telecommunications Law[16], specifying the rules on the basis of which it is permissible to "store information or access information already stored in a telecommunications terminal device".

In the case of the Internet of Things, the provision of more detailed information on the nature and probability of the risk of violation of the rights or freedoms of natural persons is necessary in order to enable users to make informed choices regarding the further use and management of personal data. Threats and negative consequences resulting from the collection and processing of personal data, e.g. data loss as a result of hacking attacks or incorrect conclusions resulting from the processing of personal data, may pose a challenge in informing the user in clear and simple language about the processing of his personal data[17].

Due to the growing importance of the Internet of Things and the associated risk for privacy, a data protection impact assessment will be mandatory for most personal data processing processes under the Internet of Things covered by the security policy of a given company. Entities operating in the field of the Internet of Things will have to assess possible threats related to the devices or services they offer[18].

SUMMARY

Digitization and connection to the global Internet network can potentially bring huge benefits, but as long as all entities do not take on the tasks related to ensuring security, IoT can bring threats simultaneously with solutions. From the point of view of the operation of an IoT-based enterprise, the key issue is to implement such technical security measures and procedures that will allow it to run its business as safely as possible, while securing its own processes as well as the data of employees, customers and partners. This is the purpose of the security policy, for which not only the management of the company, but also the employees themselves are responsible. Usually, it is not devices that fail, but people. That is why it is so important to create rules and procedures applicable in the company, the observance of which will not only guarantee the smooth operation of the company, but also ensure a safe flow of information and protection of processed data, in accordance with applicable laws on the protection of personal data at the level of a given country and international regulations because more and more enterprises do

[15] When assessing the admissibility of personal data processing in connection with the Internet of Things, the guidelines of the Art. 29, now replaced by the European Data Protection Board (EDPB).

[16] Journal of Laws of 2004, No. 171, item 1800.

[17] J. Pisuliński, *Licencja na oprogramowanie a rozporządzanie rzeczą*, [w:] Scientific Journals of the Jagiellonian University. Works on Intellectual Property Law, 2018/2, pp. 74–84.

[18] *IoT in the Polish economy, report of the Working Group for the Internet of Things at the Ministry of Digital Affairs, April 2019*.

not limit their activities only to their own country[19]. A reliable study of the potential applications of the implemented Internet of Things system undoubtedly requires close cooperation of specialists in the field of IT and law[20]. Therefore, when starting to formulate a security policy document, the following elements should first of all be taken into account: the state of technical knowledge, scope, context and purposes of processing, as well as the risk of violating the rights or freedoms of natural persons. The necessity to perform an in-depth analysis results not only from the obligation specified directly in the GDPR, but also due to the economy of the organization's operation. As already mentioned, the security policy is to improve the company's operations and increase the security of its operation, and not constitute a procedural brake for it.

REFERENCES

Defense Policy and the Internet of Things Disrupting Global Cyber Defenses, https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-IoT-defense-policy-and-the-internet-of-things.pdf

Deloitte analysis: Remote work and teleworking during COVID-19 https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/newsletter-strefa-pracodawcy-podatki-i-prawo/praca-zdalna-a-telepraca-w-czasie-COVID-19.html

IoT in the Polish economy, report of the Working Group for the Internet of Things at the Ministry of Digital Affairs, April 2019.

2020 IoT Market Report, https://cyfrowapolska.org/wp-content/uploads/2020/11/Raport_Rynek-IOT_2020_net.pdf

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

Kępa L., Ochrona Danych Osobowych w Praktyce, Difin Publishing House, Warsaw 2014, pp. 272–274.

Konraski X., Internet of Things - the most important legal regulations in Poland, https://digitalandmore.pl/iot-regulacjeprawne/

Liderman K., Bezpieczeństwo Informacyjne, nowe wyzwania, Polish Scientific Publishers PWN, Warsaw 2017, pp. 229–230.

Pisuliński J., Licencja na oprogramowanie a rozporządzanie rzeczą, [w:] Scientific Journals of the Jagiellonian University. Works on Intellectual Property Law, 2018/2, pp. 74–84.

Radecki P., The Internet of Things and the protection of personal data, https://odo24.pl/blog-post.internet-rzeczy-a-ochrona-danych-osobowych

Smolarek K., Internet of Things, privacy protection and data security, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/Internet-Rzeczy-ochrona-prywatnosci-a-bezpieczenstwo-danych.html

Wachter S. The GDPR and the Internet of Things: A Three-Step Transparency Model, Oxford Internet Institute University of Oxford

Żywiołek J. Innowacyjność przepływów informacyjnych jako element udoskonalenia systemu informacji w przedsiębiorstwie logistycznym, Scientific Journals of the Częstochowa University of Technology Management No. 24 vol. 1 (2016).

[19] More on this topic: P. Radecki, The Internet of Things and the protection of personal data, https://odo24.pl/blog-post.internet-rzeczy-a-ochrona-danych-osobowych [reading: 15.5.2021]

[20] An example of such action is the California IoT Act, effective from January 1, 2020, under which the state civil code was amended. The essence of this regulation is to impose additional obligations on manufacturers of devices connected to the Internet in terms of ensuring the security of these devices, as well as the information stored in them.