UDC 338.3

Trziszka M.
Ph. D., Faculty of Engineering Management
Poznan University of Technology
Poznan, Poland
ORCID ID: 0000-0003-0170-5849

SECURITY POLICY FOR REMOTE WORKERS IN ENTERPRISES

The aim of the article is to discuss the threats resulting from extending access to Internet tools to remote employees, and at the same time to demonstrate to what extent the introduction of procedures in the field of data and infrastructure security can 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 should be considered not only in terms of protecting the content of information, but also its authenticity and timeliness. On the other hand, inappropriate formulation of security policy rules in a given enterprise may limit the availability of solutions and access to data. Enterprises therefore need to take steps to help maintain both the functionality and security of their systems.

Digitization, both in terms of the technological development of society and in terms of computerization of technological processes, gives many benefits, but at the same time requires the use of appropriate security measures, especially against the increasing threat of cyberattacks. For this reason, data protection should be considered on a company-wide scale, both taking into account operating systems, but also all devices connected to the network. Many data collected in IT systems can be sensitive, containing personal information, activities and behavior of people, enterprises and devices. In this aspect, the key issue is to ensure appropriate procedures and policies guaranteeing the security of the collected data.

The study analyzed two companies in the IT industry that used remote work from time to time before the COVID-19 pandemic, and three from the financial industry that did not use telework before the COVID-19 pandemic. In 2020, as a result of lock-down and forced remote work, all five companies switched to full remote work. The author's research focused on issues related to the security of employees' access to company resources via the Internet. Among other things, awareness of the dangers in the network, training employees in the field of security, securing the company infrastructure and employees' computers.

As a result of the work, the need for a security policy for remote employees was verified, and the research results allowed to show the key elements of the document and the procedures for its implementation in the enterprise. A complicated and multi-level security policy paralyzes the smooth functioning of the enterprise, extending and complicating data processing processes, causing strong restrictions on the transfer of necessary information to paralyze the entire process and reduce its effectiveness, which is crucial in the case of remote work. Therefore, for the smooth functioning of the organization, easy and reliable access to documents, data, colleagues and customers is crucial. This requires the use of security measures that will ensure that the shared documents are properly protected at every stage.

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 at the same time as solutions. From the point of view of the functioning of a company based on the Internet of Things, the key issue is the implementation of such technical safeguards and procedures that will allow it to run its business in the safest possible way, while securing its own processes as well as the data of employees, customers and cooperators. This is the purpose of the security policy, which is the responsibility of not only the company's managers, but also the employees themselves. Usually it is not devices that fail, but people. That is why it is so important to create rules and procedures in force in the company, the observance of which will not only guarantee the smooth operation of the company, but will also ensure the 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, as more and more companies do not limit their activities to the territory of their own country. A reliable study of the potential applications of the implemented Internet of Things system undoubtedly requires close cooperation between IT and law specialists. Therefore, when starting to formulate a security policy document, the following elements should be taken into account: the state of the art, the scope, context and purposes of processing, as well as the risk of violating the rights or freedoms of natural persons. The need to conduct an in-depth analysis results not only from the obligation set out directly in the GDPR, but also from the economics of the organization's operation. As mentioned before, the security policy is to improve the operation of the enterprise and increase the security of its operation, and not to constitute a procedural brake for it.