Dmytro Zatonatskiy
Ph.D. Student,
National Institute for Strategic Studies,
Kyiv, Ukraine
dzatonat@gmail.com

PERSONNEL SECURITY FOR REMOTE WORKING DURING COVID-19 PANDEMIC

With the constant development of computer technology, many companies have begun to use a system of remote work, which allows them to attract a wider range of professionals, create better working conditions and save on the need to maintain larger office space. In the context of the COVID-19 pandemic and the implementation of the initial severe lockdown, many companies were forced to switch to the remote format for their employees. It turned out that for some companies, remote work of employees is more profitable because it saves significant resources. As a result, even with the easing of restrictions, they are in no hurry to return their employees to office work. On the other hand, such companies face a serious problem of personnel security for employees working from home.

This means that now the provision of personnel security involves the emergence of a new dimension, namely cyberspace. Companies are forced to spend more and more resources and efforts to ensure the information component of personnel security, which involves the use of advanced information and communication technologies and modern software. Among the main security issues that have arisen in the organization of remote work, we can highlight the proper organization of the workplace, protection of information and company data, creating a secure remote network, creating an effective authentication system and response system to external attacks.

The problem of organizing a workplace for remote work remains a rather serious threat to information and economic security of enterprises. On the one hand, to avoid the threat of external attacks, the company is better to provide employees with equipment and devices from the company. On the other hand, it is quite expensive, so some companies prefer to allow their employees to use their own equipment, and provide only corporate software.

Using your own hardware increases the threat to company information and data. In particular, there is a risk of data loss due to breakdowns of the employee's own equipment. In order to minimize it, companies are creating separate cloud data storages to back up information. However, the risk of data leakage increases as remote workplaces creates additional access points for a possible attack.

To protect against the abovementioned threats, the company can create a secure remote network, which involves the development of security infrastructure, such as individual security protocols. This means that all devices on which remote work is performed are adequately protected from external intrusion, and only a secure connection is used to transmit corporate data. To do this, they use special software that detects viruses and suspicious connections. Another way of protection is the use of exclusively professional assistance of IT specialists in solving technical problems. Also, the issue of protection of communications between employees of the company, for example, during video meetings, is becoming increasingly important.

Another component of the protection against threats is to ensure an effective user authentication system. Because the employee's device accesses the company's information during remote work, it is important to avoid taking possession of this device by third parties. To this end, it is recommended that you create separate protocols for the use of devices, Internet connections, protection against malware, and other computer threats. In addition, the company must create a system to protect all remote workplaces from attacks, as well as a framework to respond to such attacks. This requires an independent backup of all company data and information in case the hackers seize the internal network for ransom.

According to experts, remote work is becoming a new reality that will not disappear with the end of the pandemic. The management of companies such as Twitter, Google, Facebook and a number of others have already stated that they will encourage their employees to work remotely on a permanent basis. This is due to the fact that, according to these companies, the productivity of their employees has increased, as on average each employee is able to work 400 hours more per year. But there is another problem. How to track employee productivity? There are many software products on the market that allow management to spy on their employees, who in turn try to avoid it, considering it an invasion of privacy. Experts believe that it is necessary to create a clear and transparent system that will allow management to monitor employee productivity, while preventing interference in their personal affairs.

References

1. Curran, K. (2020). Cyber security and the remote workforce. *Computer Fraud & Security*, *2020*(6), 11-12.
2. Hart, J. (2009). Remote working: managing the balancing act between network access and data security. *Computer Fraud & Security*, *2009*(11), 14-17.
3. Laker, B., Godley, W., Patel, C., & Cobb, D. (2020). How to monitor remote workers—ethically. *MIT Sloan Management Review*.
4. Malecki, F. (2020). Overcoming the security risks of remote working. *Computer Fraud & Security*, *2020*(7), 10-12.
5. Miele, F., & Tirabeni, L. (2020). Digital technologies and power dynamics in the organization: A conceptual review of remote working and wearable technologies at work. *Sociology Compass*, *14*(6), e12795.