Centrum Rzeczoznawstwa Budowlanego

Inżynieria Bezpieczeństwa Obiektów Antropogenicznych 1 (2022) 7-15
https://inzynieriabezpieczenstwa.com.pl/

Inżynieria Bezpieczeństwa Obiektów Antropogenicznych

The impact of the covid-19 pandemic on business entity cyber security

Joanna ANTCZAK*[1]

[1]Military University of Technology, Warsaw, Poland

Abstract

Cybercriminals during the COVID-19 coronavirus pandemic have redefined both their targets and the form of their cyberattacks. The increased dependence of people around the world on the Internet is driving increasingly bold hacking attacks. Business unit managers are forced to implement better and better security of data resources, which should be organized and at the same time characterized by confidentiality, integrity, and availability. The purpose of the article was to identify and analyse the impact of the COVID-19 pandemic on the cyber security of the business entity. In realizing the purpose of the article, the starting point was a theoretical introduction to cybersecurity. Then, based on the Cybercrime: Covid-19 Impact report developed by Interpol, it was indicated that the coronavirus pandemic has a very high impact on the cyber threat panorama. To analyse the actual market situation, the effects of the cyber-attack on CD PROJEKT Capital Group were analysed.

Keywords: cyber security, hacking attack, pandemic, effects of cyber attack.

1 Introduction

Cybercriminals during the COVID-19 coronavirus pandemic have redefined both their targets and the form of their cyberattacks. Attacks have primarily targeted government organizations, health care institutions, or critical infrastructure entities. While the effects of cyber-attacks can threaten both the health and life of people by paralyzing medical facilities. Hackers mainly exploit people's fear of a pandemic leading to large losses for entities from various industries.

Business executives from various industries faced a rapidly changing environment of cyber threats (Figure 1) caused by a pandemic. The shift from stationary to remote work mode on the one hand requires paying more attention to the wave of potential hacking attacks on the other incurring additional costs in security.

According to Global Risk Survey 2020, 79% of executives admit that their organizations are not sufficiently prepared to deal with a crisis.

The purpose of this paper was to identify and analyse the impact of the COVID-19 coronavirus pandemic on the cyber security of a business entity.

In achieving the purpose of the article, the starting point was a theoretical introduction into cybersecurity. Then, based on the report Cybercrime: Covid-19 Impact developed by Interpol, it was indicated that the COVID-19 coronavirus pandemic has a very large impact on the cyber threat panorama. To analyse the actual market situation, the impact of the cyber-attack on CD PROJEKT Capital Group was analysed.

The following research methods and techniques were used in the study: analytical methods, deduction method as a form of generalization and inference, literature analysis [1–7, 14].

2 Cybersecurity

Most often cyber security is defined from the point of view of preventing damage, protecting and in the perspective of restoring the ability to correctly function computers, electronic communication systems or communication services

***Corresponding author:** E-mail address: (joanna.antczak@wat.edu.pl) Joanna ANTCZAK

https://dx.doi.org/10.37105/iboa.128
Received 2 February 2022
Available online 31 March 2022
ISSN 2450-1859, eISSN 2450-8721
Published by Centrum Rzeczoznawstwa Budowlanego

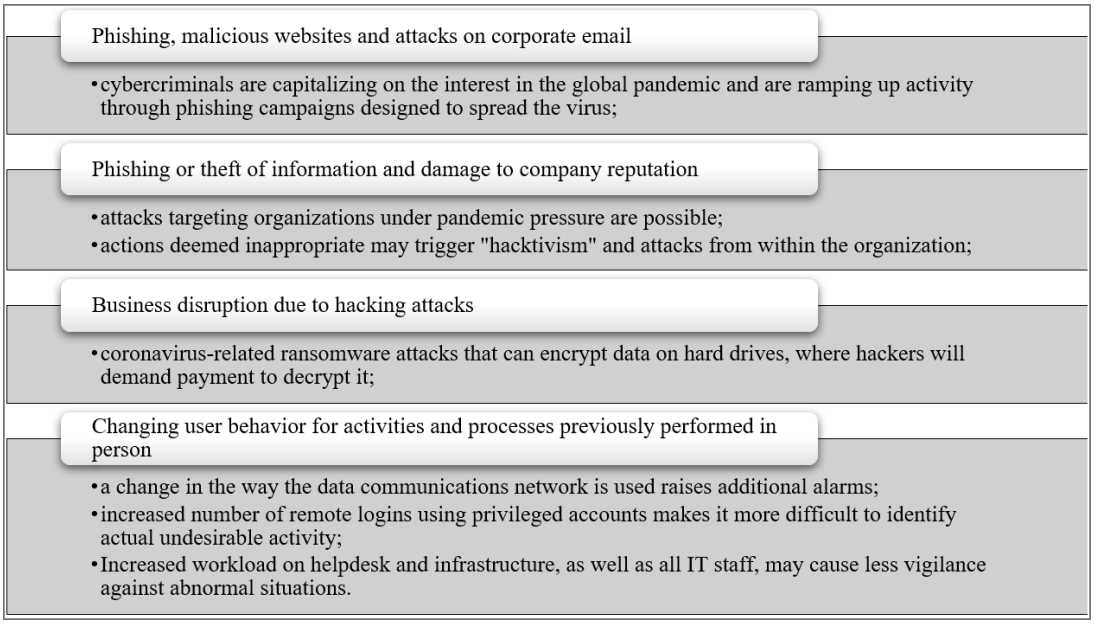

Figure 1. Threats and attacks in the area of cyber security

taking place in cyberspace. Cyber security is also the protection of information contained in the electronic communications space to ensure confidentiality while authenticating authorized individuals [11]. Cyber security is the management of information systems by individuals or organizations to manage the security behaviour of end users, based on personal perceived behaviour toward potential security breaches in and out of the work environment.

The concept of cybersecurity, or security in cyberspace, poses problems of definition, "which is a result of the blankness of the concept of security itself, which takes on different content depending on its quantifier and its subjects. As a normative concept, security is a typical general clause, justifying certain state actions taken in the public interest. The concept of security is at the same time a dynamic category, changeable, requiring constant redefinition and with an open scope" [9].

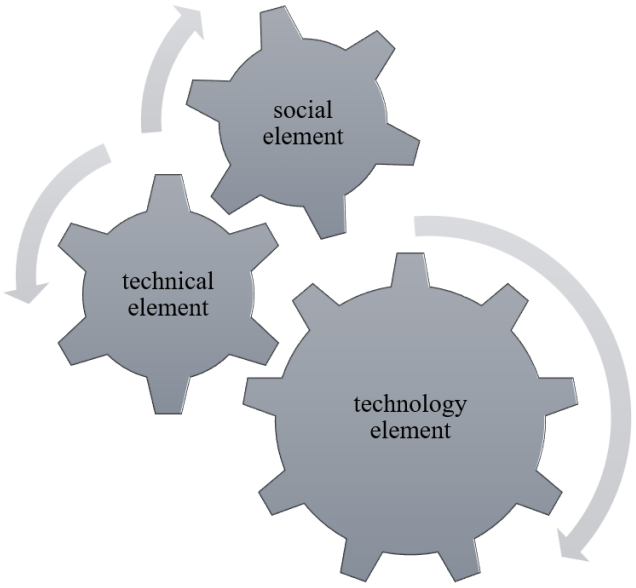

Figure 2. Elements of cyberspace

According to P. Sienkiewicz, cyberspace has both its "bright" and "dark" sides. Cyberspace is an area of both positive and negative cooperation. Positive cooperation is associated with an undeniable increase in the possibility of

comprehensive satisfaction of social needs, including the need for cooperation and self-development, in all areas of life, such as education, communication, economics, culture and security. Negative cooperation ("dark side") means that cyberspace has become a dangerous space of crises and conflicts, being a source of threats to external (international) and internal (national) security [12].

According to K. Dobrzeniecki, cyberspace is based on three elements: technical, technological and social (Figure 2) [10].

The NATO Cyber Defense Center of Excellence defines cyberspace as "a time-dependent collection of interconnected information systems and the people/users interacting with these systems"" [9].

The sphere of security of organizations is affected not only by threats aimed directly at the interests of a particular business entity, but also aimed at introducing destabilization in the cyberspace of the state. This in turn leads to the obvious conclusion that these events may be inspired not only by criminals, but also - directly or indirectly - by foreign governments and may take all of the previously indicated forms of cyber threats, including those related to cyber intelligence or cyberterrorism [9].

When considering threats in cyberspace, it is important to note cyberterrorism (Figure 3) and the two words that make up the term. The first, "Cyber," refers to information technology, which is related to terrorism in two ways. In the first approach, IT is a tool through which criminals can communicate, train, spread propaganda, and derive the information necessary to carry out an attack. On the other hand, IT can also be a target for terrorist attacks. The second word "Terrorism" is defined as the unlawful use or threat of violence against persons or property for the purpose of intimidating the government of a country or for political, religious, or ideological gain. [13].

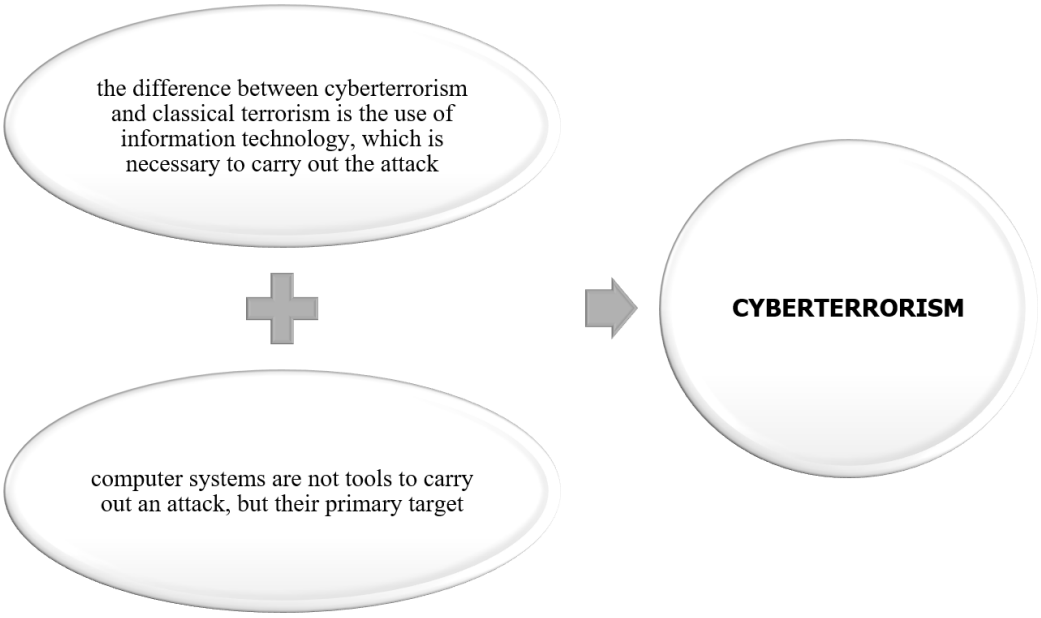

Figure 3. Cyberterrorism

The main objective of cyber terrorism is to deliberately disrupt the interactive yet organized flow of information in cyberspace. Users who plan to gain unauthorized access to another user's information system using cyberspace to cause fear or blackmail are called cybercriminals [8].

3 Cybercrime and the COVID-19 pandemic

Cybersecurity and the Pandemic COVID-19 The Cost of A Data Breach 2020 report, recently published by IBM, leaves no illusions. Nearly 80% of companies surveyed believe that a pandemic will worsen the state of cybersecurity. Among the more than 500 companies surveyed from a dozen countries around the world that fell victim to hackers, the average amount of damage caused by these attacks is nearly 3.9 million dolars. Although the report is published for a period only partially covering the time of the pandemic, its authors calculate that remote work alone caused

an increase in the average damage of 137,000 dolars. Even more alarmingly, the average time required to discover vulnerabilities and take effective action was 280 days - more than 9 months.

The Cybercrime: Covid-19 Impact report produced by Interpol indicates that the coronavirus pandemic is having a very large impact on the cyber threat panorama. As the report states, "The combination of a global health crisis and a surge in Covid-19-related cybercrime activity is placing a significant burden on law enforcement agencies around the world".

Interpol's assessment of the impact of the COVID-19 virus on cybercrime showed a significant shift in targets from individuals and small businesses to large corporations, governments, and critical infrastructure. The following reasons are cited in the report: organizations and businesses are rapidly deploying remote systems and networks to support employees working from home, criminals are also exploiting increased security vulnerabilities to steal data, generate profits and cause disruption. According to the Interpol report, hackers have also redefined their goals to generate the maximum possible profit for themselves while causing the greatest possible loss to the victim of the attack.

To provide a comprehensive analysis of the cybercrime situation during the pandemic, the report is based on information obtained from 194 member states and private partners. The study was conducted in the period April-May 2020 as part of the "INTERPOL Global Cybercrime Survey".

Interpol's analysis focuses on the following cyber threats: online fraud and phishing, malware cyber-attack such as ransomware and DDoS campaigns, data harvesting, malicious websites, and misinformation. The report indicates the relationship between cybercrime and the COVID-19 pandemic (Table 1).

Table 1. The impact of the COVID-19 pandemic on cybercrime

CYBERCRIME	THE IMPACT OF THE COVID-19 PANDEMIC ON CYBERCRIME
Disruptive Malware (Ransomware and DDoS)	• cybercriminals are increasingly using disruptive malware against critical infrastructure and healthcare institutions, due to the potential for high impact and financial benefit; • law enforcement investigations show that most of the attackers estimated quite accurately the maximum ransom amount they could charge the organizations attacked;
Online Scams and Phishing	• threat actors have revised their usual online scams and phishing schemes; • by deploying COVID-19 themed phishing emails, often impersonating government and health authorities, cybercriminals entice victims into providing their personal data and downloading malicious content;
Data Harvesting Malware	• the deployment of data harvesting malware such as Remote Access Trojan, info stealers, spyware and banking Trojans by cybercriminals is on the rise;
Malicious Domains	• taking advantage of the increased demand for medical supplies and information on COVID-19, there has been a significant increase of cybercriminals registering domain names containing keywords, such as "coronavirus" or "COVID";
Misinformation	• an increasing amount of misinformation and fake news is spreading rapidly among the public; • unverified information, inadequately understood threats, and conspiracy theories have contributed to anxiety in communities and in some cases facilitated the execution of cyberattacks;

According to the Interpol report, 907 000 spam messages, 737 malware incidents, and 48 000 malicious URLs-all related to COVID-19-were detected between January and April 2020 (Figure 4)

As stated in the report: approximately two-thirds of the member states that responded to the Global Cybercrime Survey reported significant use of COVID-19 motifs for phishing and online fraud since the outbreak. The first two weeks of April 2020 saw a surge in ransomware attacks by multiple threat groups that had remained relatively dormant for the past several months. Using information related to COVID-19 as bait, cybercriminals are infiltrating systems to take control of networks, steal data, extort money and create botnets. From February to March 2020, private sector

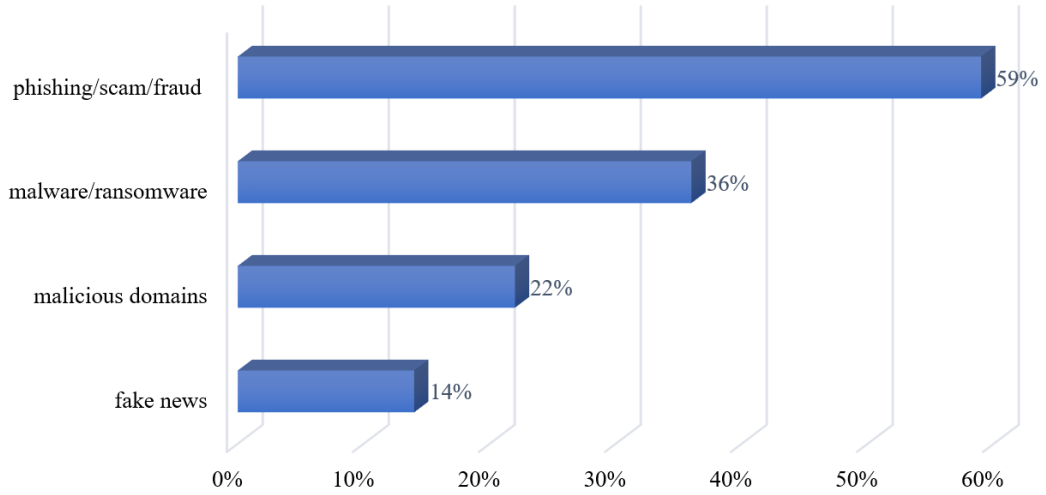

Figure 4. Cyber threats from January to April 2020

Table 2. Forms of cybercrime by region

REGION	DESCRIPTION
African continent	• electronic or cashless payments have increased since the start of the pandemic, creating an attractive field for cybercriminals; • an increased number of phishing attacks have been observed as a result of the need to shift to remote working mode; • circulation of COVID-19-related fake news on social media has increased;
North and South America	• phishing campaigns and scams related to the coronavirus pandemic increased; • one of the dominant forms of cybercrime was the theft of confidential data by gaining remote access to networks and systems; • a ransomware campaign conducted primarily through the LOCKBIT malware affected mid-sized companies;
Asia and the South Pacific	• coronavirus-related fraud and phishing campaigns; • illegal online sales of counterfeit medical supplies, drugs, and personal protective equipment; • cybercriminals exploiting security vulnerabilities in teleconferencing tools; • the spread of fake news about Covid-19 has been a very big problem;
Europe	• two-thirds of European member states reported a significant increase in malicious domains addressing the pandemic; • hackers are using Covid-19 as a lure to deploy ransomware in healthcare institutions, a cornerstone of the coronavirus fight; • copying of official government websites to steal sensitive user data, which can then be used in subsequent cyberattacks, is on the rise;
Middle East	• malicious social media campaigns that serve as a conduit for spreading fake news about Covid-19; • social media platforms are often a marketplace for illegal sales of pharmaceutical products for the coronavirus; • phishing attacks, online scams, and the creation of new fake domains that claim to share "real" pandemic data and information are on the rise;

entities detected and reported a 569 percent increase in malicious registrations, including malware and phishing, and a 788 percent increase in high-risk registrations. Nearly 30 percent of countries responding to the Global Cybercrime Survey confirmed the dissemination of false information related to COVID-19, with one country reporting 290 alerts in one month, most of which contained hidden malware. There are also reports of false information being linked to the illegal trade in fraudulent medical supplies. Other cases of fake news involved fraudulent cell phone text messages containing "too good to be true" offers such as free food, special benefits or big discounts at supermarkets. In the

report, Interpol indicated that forms of cybercrime vary by region of occurrence (Table 2).

4 Case study CD Projekt Capital Group

For over 25 years CD PROJEKT Capital Group has been operating in the dynamically developing electronic entertainment industry - video games, which during the COVID-19 pandemic became one of life during the COVID-19 pandemic. CD PROJEKT creates the highest quality innovative entertainment and at the same time, through its own digital distribution platform, provides players around the world a wide selection of titles available without the troublesome digital protection - DRM.

CD PROJEKT S.A. is listed on the Warsaw Stock Exchange and belongs to the WIG20 index, which associates 20 of the largest and most liquid companies on the Warsaw Stock Exchange. The company has offices in Warsaw, Krakow and Wroclaw, where teams responsible for the company's next productions work, as well as offices in Los Angeles, Berlin, Tokyo, Seoul and Shanghai, which coordinate marketing and sales activities in the United States, Germany, Japan, South Korea and China, respectively. The Group has employees from 44 countries.

On February 8, 2021, CD PROJECT was the victim of a cyber-attack in which some internal systems were breached. Unknown perpetrators in a message (Figure 5) informed that they had source codes for games: Cyberpunk 2077, The Witcher 3, Thread, and an unreleased version of The Witcher 3 for latest-generation consoles. Hackers also reported that they stole all accounting, administrative, legal, human resources and investor relations documents. Cyberterrorists threatened to share or sell these codes by giving the company 48 hours to contact them.

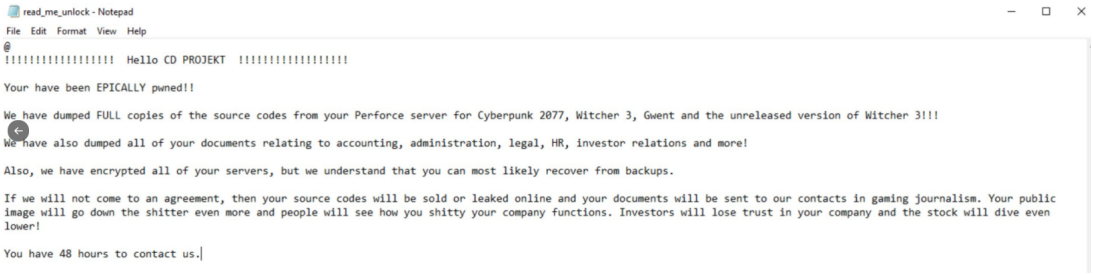

Figure 5. Message from hackers to CD Projekt
Source: https://twitter.com/CDPROJEKTRED/status/1359048125403590660/photo/2

CD Projekt RED 09.02.2021 via its social media, announced that it was the victim of a hacking attack (Figure 6) Stating that: noting that nothing has been lost, the company recovers data from backups and an investigation is underway. The company declared that it did not plan to negotiate with criminals.

CD PROJEKT CEO Adam Kiciński informed that: "The servers and the resources of CD PROJEKT Group located on them fell victim to the attack. To the best of our knowledge there was no leakage of personal data of players and other users of our services. We are currently focused on investigating the incident itself, securing the infrastructure and restoring the data which, in accordance with our internal procedures, are regularly backed up. So, it is too early to assess the long-term effects of the attack. It will certainly affect the pace of our development work in the short term. We are currently taking appropriate action, including investigation and verification, in connection with the attack. If the conclusions resulting from a comprehensive analysis by the management board of the identified consequences of the attack and their impact on the company's operations prove that it is justified for us to publish a current report - the report will be published immediately"

According to Wojciech Glazewski, Country Manager of Check Point Software, "from the available information, it appears that this was not a traditional ransomware attack, but a so-called double extortion, in which hackers first extract large amounts of sensitive information before encrypting the victim's databases, and then threaten to publish it if ransom demands are not met." He also notes that in Q3 2020, nearly half of all ransomware incidents had this pattern. In contrast, in January 2021, as many as 7% of companies and institutions in Europe encountered ransomware attacks1.

On 09.02.2021, the day after the attack, the shares of CD PROJEKT recorded a sharp decline of 6% from PLN 287.20, reaching at the critical moment PLN 268.90 per share. Since the hacking attack, the company's shares have

Figure 6. Communication from CD Projekt
Source: https://twitter.com/CDPROJEKTRED/status/1359048125403590660/photo/1

recorded a decline (Table 3). The lowest level of the share price was recorded on 11.05.2021 and was at the level of PLN 151.08.

When analysing the profit and loss account data (table 4), one may notice a significant decrease in both sales profit and net profit by 56% and 65%, respectively, comparing the first quarter of 2021 to the corresponding period of 2020 and amounting to PLN 43 171 thousand and PLN 32 487 thousand, respectively. Where in 2020, comparing y/y, sales profit recorded almost fourfold increase and net profit more than fourfold. Revenue from sales in the first quarter of 2021 increased by 2% compared to the same period of 2020 and amounted to PLN 197 632 thousand. Costs

Table 3. CD PROJEKT shares

Category of Change	Change	Change %	Reference price	Reference date
Change 1d:	-3.32	(-1.88%)	176.50	09.06.2021
Change 7d:	+11.60	(+7.18%)	161.58	02.06.2021
Change 1m:	+20.91	(+13.73%)	152.27	10.05.2021
Change 3m:	-31.13	(-15.24%)	204.31	10.03.2021
Change YTD:	-93.83	(-35.14%)	267.01	30.12.2020
Change 12m:	-209.01	(-54.69%)	382.19	10.06.2020

Table 4. Selected income statement data of CD PROJEKT for the years 2018-2021

Specification	first quarter of the year (in PLN thousand)				rate of change		
	2018	2019	2020	2021	2019	2020	2021
Sales revenues	75 435	80 905	192 972	197 632	7%	139%	2%
Cost of production of sold production	16 133	28 713	47 491	62 272	78%	65%	31%
Result from sales	27 723	20 353	99 153	43 171	-27%	387%	-56%
Net profit	22 892	17 797	91 979	32 487	-22%	417%	-65%

of production sold in the same period increased by 31% and amounted as at 31.03.2021. PLN 62 272 thousand.

5 Conclusions

The time of the COVID-19 pandemic has forced both state organizations and business entities and individuals to function in a new reality. The increasing dependence of people on the Internet favors the development of more and more daring cyber-attacks.

Cybercriminals, on the one hand, are constantly improving their hacking skills and, on the other hand, skilfully harness people's fear of the effects of the COVID-19 coronavirus pandemic, such as the unstable socio-economic situation.

Increasingly, cyber-attacks are carried out against entities that have a key role in fighting the pandemic like vaccine manufacturers or companies that thrive during a pandemic such as: CD PROJEKT, Inpost. The introduction of remote work, which forced employers to quickly implement systems, networks and applications that would allow such work, which resulted in their cybersecurity quality could not meet the highest standards, and this in turn contributed to the creation of gaps and vulnerabilities that were efficiently exploited by hackers.

The hacking attack carried out on CD PROJEKT 08.02.2021 affected the financial situation of the group. The company's shares immediately fell 6%. Both revenue and profit on sales at the end of the first quarter of 2021 compared to the same period in 2020 recorded declines of 2% and 56%, respectively. An interesting observation is that hackers made a successful attack on a computer company that should theoretically be well protected. The attack was carried out shortly after the release of the long-awaited product that is the game Cyberpunk 2077.

According to Interpol's Cybercrime: Covid-19 Impact report, there is a need for the public and private sectors to work more closely together if the threat that COVID-19 also poses to overall cyber health is to be effectively addressed.

References

1. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
2. https://businessinsider.com.pl/cd-projekt-padl-ofiara-hakerow-chca-okupu-kurs-akcji-w-dol/qzp0rcb.
3. https://crn.pl/aktualnosci/cyberatak-na-cd-projekt-beda-skutki-w-krotkim-terminie/?fbclid=IwAR2F9IXy4eZhqQA08TCWOjJfkg8ZO1a5Dr-URDpCmTHwS2coUOrpfw8UYmQ.
4. https://iuscase.pl/cyberbezpieczenstwo-a-praca-zdalna/.
5. https://twitter.com/CDPROJEKTRED/status/1359048125403590660.
6. https://www.biznesradar.pl/notowania/CD-PROJEKT#6m_bar_lin.
7. https://www.ey.com/pl_pl/covid-19/cyberbezpieczenstwo-w-dobie-covid-19.
8. Antczak, J. *Zarządzanie przedsiębiorstwem w cyberprzestrzeni* (ASzWoj, Warszawa, 2021).
9. Banasinski, C. *Cyberbezpieczeństwo zarys wykładu* (Wolters Kluwer, Warszawa, 2018).
10. Dobrzeniecki, K. *Prawo a etos cyberprzestrzeni* (Toruń, 2004).
11. Dunn, M. C. *Cyber-Security and Threat Politics. US Efforts to Secure the Information Age* (Londyn Routledge, 2008).
12. Sienkiewicz, P. *25 wykładów* (Akademia Obrony Narodowej, Warszawa, 2013).
13. Suchorzewska, A. *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem* (Oficyna, Warszawa, 2010).
14. Woldemichael, H. T. Emerging Cyber Security Threats in Organization. *International Journal of Information and Communication Sciences* **5** (2 2020).