Proceedings of the 1st International Scientific and Practical Conference «Modern Knowledge: Research and Discoveries»

(May 19-20, 2023). Vancouver, Canada

No 155

MANAGEMENT

DOI 10.51582/interconf.19-20.05.2023.003

The impact of the war in Ukraine on cybersecurity

Duneva Emiliya[1]

[1] Chief Assistant Doctor Department of Management;
University of National and World Economy; Republic of Bulgaria

Abstract.
The article analyzes the communication technologies and malicious digital tools. The purpose of the present study is to outline and analyze the impact of the war in Ukraine on business communications in our country and on cyber security, to show the impact of the use of communication channels, social networks and misinformation without pretensions to exhaustiveness. We have used data from various media, newspapers, magazines, research and briefings in and around the country. Findings from the survey and survey research could help tailor policies and outcomes in our country.

Keywords:
cyber security
war in Ukraine
business communications

MANAGEMENT

As communication technologies and malicious digital tools continue to evolve, crisis communications must be updated accordingly and made more resilient to new and emerging threats in order to retain their value. New threats to crisis communications in the 21st century include cyberattacks and highly sophisticated electronic warfare tools, as well as the need to operate in environments with degraded operational characteristics.

Russia began its war against Ukraine on February 24, 2022, but Russian cyber attacks against Ukraine have continued since Russia's illegal annexation of Crimea in 2014, intensifying just before the 2022 invasion. During this period, public, energy, Ukraine's media, financial, business and non-profit sectors suffered the most. Since February 2022, limited Russian cyberattacks have undermined the distribution of medicine, food and humanitarian supplies. Their impact ranged from preventing access to essential services to data theft and disinformation, including through deep fake technologies.

Other malicious cyber activity includes sending phishing emails, distributed denial-of-service attacks, and the use of data-wiping malware, backdoors, surveillance software, and information thieves. Organizations and governments around the world are not indifferent to the hybrid risks created in this way. Initiatives led by the EU, the US and NATO have been carried out to neutralize cyber threats and protect critical infrastructure. As part of these initiatives, the EU is activating its rapid response teams in cyberspace (a project under the Permanent Structured Cooperation (PESCO)[1] in the area of security and defense policy) to support Ukraine's cyber defense. Non-governmental and private players have supported Ukraine through various cyber resilience activities. Since the beginning of the invasion, a significant number of counterattacks by independent hackers have been launched, affecting Russian state, security, banking and media systems. The Wordfence team[2] identified a massive attack on Ukrainian universities that coincided with Russia's invasion of Ukraine and resulted in at least 30 Ukrainian university websites being

[1] https://www.consilium.europa.eu/bg/press/press-releases/2021/11/16/eu-defence-cooperation-council-launches-the-4th-wave-of-new-pesco-projects/

[2] https://www.wordfence.com

MANAGEMENT

compromised. Companies are at risk of becoming victims of crime, especially outside of normal business hours, when their employees share information from digital devices that do not guarantee 100% confidentiality. The main types of cyber security threats companies face today are:

- malware
- social engineering
- supply chain attacks
- denial of service attacks
- business email compromise/email account compromise - an opportunity that gives criminal structures to extract banking or other sensitive information about the company.

After the literary review of various sources, we can summarize that in our country the pressure from a cyber attack is felt along the lines of:

- penetration of the Russian state into NATO systems through our country, on the occasion of the acquisition of important information according to experts in the field.

According to the sources, the attack began on 15.10.22. with the hacking of the president's website, which was inaccessible for several hours. After that, the same thing happened to the websites of Bulgarian ministries. According to the Ministry of e-Governance, the crash was due to a single targeted cyber attack. However, the problem was fixed on the same day, the Bulgarian authorities hastened to announce. Proven with a security breach is a "Trojan horse". Cybersecurity is also no longer just about computers, smartphones, servers, clouds, routers and wireless networks. The penetration of digitization into any object makes it susceptible to cyber attack.

Smart watches - problems

The security of smartwatches is related to cyber risks, as there are with all other devices in the field of E&O. It turns out that despite existing protections on some smartwatches, there are a number of vulnerabilities that can apply to a given smartwatch.[3]

- Factory reset passwords are a tool that is used to

[3] Боянов Л., Дигиталният свят - промяната, Глобалната дигитална трансформация - обогатяване или обедняване на човечеството, ISBN 978-619-239-637-4, изд. «Авангард Прима», София 2021, 188 стр. Монография.

MANAGEMENT

access IO devices. Because they remain unchanged, after acquiring these devices, hackers can find the password online or buy it (default passwords) on the dark web;

- SMS Hacking – there are children's smart watches that can be hacked by sending SMS.

Kaspersky advice in general[4] are to buy smartwatches from trusted manufacturers, watch out for compromised models, restrict access to various apps, use only approved/official apps, and make regular updates.

The list of threats also includes Distributed Denial-of-Service (DDoS), Ransomware, Cyber Bot, Blended Threats, Malware, Viruses, Worms, Malware, Spyware, Botnets, Spam , spoofing, phishing, and potential state-initiated cyberwarfare. According to Mr. Canzanese, the "wiper" malware, entirely aimed at destroying and erasing the contents of computers, was caught in Ukraine this year, and newer and more destructive versions have since been discovered. Other malware/worms found are HermeticWizard, designed to distribute another and NotPetya with massive damage.

Car problems

As the digitization of cars and vehicles increases, vulnerabilities in the software and hardware of these vehicles become increasingly important. Hackers are finding a way to access the operation and control of cars using cellular networks, Wi-Fi and wired connections. From their inception until a decade ago, vehicles were designed with the basic idea of having the highest possible level of safety (brakes, bumpers, airbags, etc.). Cybersecurity is a new factor and cause for concern that has become more prominent in the concerns of automakers only a few years ago. Since then (in 2015) dates the popular case of taking remote control and management of a Jeep. This was done by the two hackers, who demonstrated on camera how they controlled the vehicle's systems, from the audio system and air conditioning to the braking system and the car's steering. This case received huge publicity (it has over 4,200,000 views on public channels such as YouTube) and reminded of the scary scenarios recreated in movies and books when villains take control of innocent

[4] https://www.kaspersky.bg

MANAGEMENT

people's cars or good heroes who are powerless against hackers. Chrysler has recalled 1.4 million vehicles to patch the vulnerabilities that allowed the hack. Since then, motor vehicle manufacturers have gone to great lengths to keep their product out of such footage.

Security is also considered at the highest political level these days. In August 2021, American President J. Biden is meeting with major US IT firms about their involvement in the country's cybersecurity. The meeting was held shortly after a series of lawsuits, including against the manager of specialized software SolarWinds, which fulfills various government contracts, as well as against the pipeline company, which is important for the United States, Solnial Rirelne. Companies such as Google and Microsoft have announced their intentions to invest tens of billions of dollars, and in addition to the development of new security standards, software and hardware means, great attention will be paid to training specialists in cyber security.

Zero trust security

In addition to the blockchain, Zero Trust Security has recently become popular. It is a security architecture that restricts access to resources through strict identity and device verification procedures. Zero Trust is based on the concept of "never trust, always verify", due to the inefficiency of some of the traditional security models. With her, there is no trust for anything and everything must be verified. Zero Trust uses technologies such as multi-factor authentication, identity and access management (IAM), analytics, encryption, setting access levels and file system permissions. Zero trust also requires governance policies, such as giving users the minimum access (least privilege) they need to perform a specific task. It goes through strict control. Currently, such an approach is quite cumbersome and inconvenient for the users of such systems, because it makes it difficult and slows down the use of some system or resource, but with the passage of time and the application of new and faster technologies, this may change.

Conclusion

It is necessary to analyze and evaluate the false and misleading information, messages promoted by the media in our

MANAGEMENT

country with Russian and other ownership and with established close ties to Russia. It is necessary to strengthen the participation of the radio and the national television in ensuring the objective transmission of information from the Ukrainian conflict, the situation of the government and the influence of NATO and the EU. A positive communication strategy would balance misleading information messages.

References:

[1] EU defence cooperation: Council launches the 4th wave of new PESCO projects https://www.consilium.europa.eu/bg/press/press-releases/2021/11/16/eu-defence-cooperation-council-launches-the-4th-wave-of-new-pesco-projects/
[2] A Comprehensive Security Solution For WordPress https://www.wordfence.com
[3] Боянов Л., Дигиталният свят - промяната, Глобалната дигитална трансформация - обогатяване или обедняване на човечеството, ISBN 978-619-239-637-4, изд. «Авангард Прима», София 2021, 188 стр. Монография.
[4] Cybersecurity that is always one step ahead https://www.kaspersky.bg
[5] Вечната кибервойна: атаките между Русия и Украйна ще надживеят войната на фронта https://www.bloombergtv.bg/a/8-novini-ot-sveta/104105-kibervoynata-rusiya-ukrayna-shte-nadzhivee-voynata-na-fronta