

КИБЕРБЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

М. Хуссейн¹, Е.А. Аникеев¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В статье рассматриваются ключевые аспекты обеспечения кибербезопасности в условиях цифровой трансформации экономики и социальной сферы. Проведён анализ современных киберугроз, включая практический случай атаки программой-вымогателем, описаны архитектурные и технологические подходы к защите информационных систем, а также рассмотрена роль нормативно-правовой базы и человеческого фактора в построении комплексной системы информационной безопасности организации.

Ключевые слова: кибербезопасность, цифровая трансформация, программы-вымогатели, архитектура нулевого доверия, защита данных, искусственный интеллект, информационная безопасность.

CYBERSECURITY IN THE AGE OF DIGITAL TRANSFORMATION

M. Hussain¹, E.A. Anikeev¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The article examines the key aspects of ensuring cybersecurity in the context of the digital transformation of the economy and social sphere. An analysis of modern cyber threats is carried out, including a practical case of a ransomware attack, architectural and technological approaches to protecting information systems are described, and the role of the regulatory framework and the human factor in building a comprehensive information security system of an organization are considered.

Keywords: cybersecurity, digital transformation, ransomware, zero trust architecture, data protection, artificial intelligence, information security.

The transition to digital economy and smart government services where many processes are migrated to cloud computing and Internet of Things become prevalent have significantly altered the cybersecurity threat landscape. Previously, information

security was considered an issue of technologies that resided only in the IT department. Nowadays, cybersecurity has transformed into one of the crucial elements of running business, and the global cost of cybercrime is expected to reach more than \$9.5 trillion in 2024 according to Cybersecurity Ventures [1].

Thus, the digital transformation involves the reconsideration of business models, operations in supply chain management, and collaboration among humans and technologies. Every newly introduced technology, cloud-based application, or connected thing increases the risk of successful attack. Hence, there is a need to abandon purely perimeter-based solutions in favour of comprehensive cyber security strategies.

Cybersecurity has a history that is very similar to the history of digital technologies. The first computer viruses came out in the 1980s. In the 2000s, organized cybercriminal groups took their place. In the 2010s, state-sponsored advanced persistent threat (APT) actors joined them. There are a few main vectors that make up the threat landscape today.

Ransomware is now one of the most damaging types of attacks for businesses. The double-extortion model, which involves encrypting data and threatening to publish it at the same time, has given attackers a lot more power. The 2021 attack on the Colonial Pipeline, which stopped fuel supplies across the eastern United States, and the 2024 attack on the Change Healthcare payment processor, which stopped the processing of prescriptions at thousands of pharmacies, show that ransomware is now a systemic threat to critical infrastructure [2].

Ransomware attacks don't just happen to big companies and important infrastructure; they also work just as well on individual users. The author of this article wrote about the following case, which shows how a modern ransomware attack on a personal computer usually works and how it uses social engineering.

The attack started when someone downloaded a program from a third-party website that was not authorized. When the malicious program ran, it silently installed ransomware that changed all the files on the device, including documents, images, and other personal data, into shortcut files. The attacker had to use their decryption tool to get to these files. There was no warning during or right after the infection; the data just seemed to disappear and be replaced by shortcut icons that looked the same. After the encryption phase, the victim was told to pay 800 US dollars to get a proprietary recovery software that the attackers said would bring back all the affected files.

In this case, there is a known ransomware propagation technique that involves distributing malware-infected software using third-party websites for downloads. This particular ransomware attack demonstrates several features that are consistent with

what researchers have observed in previous studies on cybersecurity. For example, the use of shortcuts to hide files instead of deleting them is a planned social engineering strategy intended to induce confusion in the victim's mind and increase the chances of payment. Moreover, a ransom value of 800 USD falls into the category of ransomware attacks that target individual users or small enterprises. In other words, it is sufficiently large to generate a profit while remaining affordable for some individuals or small business owners. Finally, the claim that the “recovery software” will enable the user to recover their files appeals to the victim's instinct to restore their system, although ransomware distributors cannot be certain that decryption software will work.

This case highlights a significant and often undervalued risk factor: the utilization of software from unverified sources. Legitimate application distribution channels, such as official vendor websites, verified software repositories, and platform-managed stores, offer significant, albeit not infallible, protection against this attack vector. The incident further confirms that individual cybersecurity awareness is just as important as organizational and technical controls. This is because end-user behavior is still the most common way that ransomware gets into systems [3].

Even now, phishing and social engineering remain the most widespread methods to penetrate enterprise networks. The role of human element remains significant despite advancements in email scanning solutions and endpoint security tools. FBI statistics reveal that in 2023 BEC schemes cost more than \$2.9 billion in financial losses to the United States economy. BEC schemes exploit sophisticated spoofing techniques that result in leaking user passwords and unauthorized transfer of money. With the development of generative AI technologies, cybercriminals can generate fake yet convincing content even more easily [1, 3].

Supply chain attacks are particularly risky since they leverage the trust established between companies and software and hardware providers. A vivid example was provided by the Solar Winds incident back in 2020 when malicious code inserted into an official IT monitoring and management software package penetrated hundreds of organizations and even some US government agencies. Nowadays software supply chains grow increasingly complex due to reliance on open-source and third-party software packages. Thus, it is easier to deliver malware through them [4].

The fact that traditional perimeter-based security models don't work well with cloud computing, remote work, and mobile devices has sped up the move to Zero Trust Architecture (ZTA). The Zero Trust model, which is explained in NIST Special Publication 800-207, is based on the idea of “never trust, always verify”. This means that no

user, device, or network segment is automatically trusted, and every access request must be explicitly verified, authorized, and continuously validated [3].

There are a few important technologies and practices that make Zero Trust work in real life. Multi-factor authentication (MFA) greatly lowers the chance that someone will get access to your account by stealing your password. An attacker needs the extra factor to get in. Micro-segmentation breaks the network into small, separate areas, making it harder for an attacker who has already broken through the perimeter to move around. The principle of least privilege says that users and systems should only be given the permissions they need to do their jobs. This lowers the risk of damage from a hacked account.

Misconfigurations are among the leading causes of cloud data breaches, and CSPM tools provide an automatic scan and resolution of the problem, a significant advantage for companies working in the cloud environment. The 2024 IBM Cost of a Data Breach report estimates that the average cost of a breach due to cloud misconfiguration is \$4.14 million, highlighting the importance of configuration validation in multi-cloud environments. [5]

In contrast to the conventional security strategy, DevSecOps regards cybersecurity as an integral component of the software development process and not an add-on. Integrating security practices such as SAST, DAST, and SCA into CI/CD workflows enables the identification and resolution of security vulnerabilities at the earliest, most economical stage possible [2, 3].

In fact, AI is changing the face of cybersecurity not only for hackers but also for organizations. In terms of machine learning, cybersecurity solutions become capable of analyzing huge amounts of telemetry information and discovering any deviations that could be overlooked by basic security rules. AI-powered SIEM and XDR systems detect even the most complex and multi-staged cyber-attacks by connecting all the dots between endpoints, networks, and cloud services.

UEBA creates unique behavior patterns for every user or device and detects any deviations, such as atypical hours of logging into the system or unusual access to certain data resources. At the same time, natural language processing technologies allow cybersecurity experts to automatically analyze various threat intelligence feeds, vulnerability databases, and dark web resources to obtain valuable insights into the latest threats.

At the same time, enemies are using AI more and more to make their attacks bigger, faster, and more effective. Generative AI tools are used to make phishing emails

that are very specific to each person, find software flaws automatically, and make polymorphic malware that can't be found by signature-based detection. The arms race between AI-powered attacks and AI-powered defenses is one of the most important things about modern cybersecurity. Researchers at top Russian universities are also working on systems that use neural network models to find strange patterns in network traffic. These systems are being added to national cyber security platforms [6].

As the recognition of the relationship between cybersecurity and national security and economic stability increases, laws and regulations take an expansionist path across Russia and the globe. In Russia, Federal Law No. 187-FZ “On the Security of Critical Information Infrastructure” introduces mandatory requirements for protecting information systems in key industries, such as healthcare, financial institutions, transport systems, and the energy sector. The requirements include categorization of critical infrastructure according to its security level, protection methods, and notification of every cyber-attack to the National Coordination Center for Computer Incidents (NCCCI) referred to as (NKTsKI) [2].

The latest update of the NIST Cybersecurity Framework (CSF 2.0) introduced in 2024 continues to be the go-to solution to design cybersecurity efforts based on six fundamental pillars: govern, identify, protect, detect, respond, and recover. In Europe, the implementation of the NIS2 Directive became effective from January 2023, extending the scope of responsibilities to ensure cybersecurity to providers of essential services and digital service providers.

There have been numerous changes made in relation to cybersecurity governance within corporate organizations. CISOs have transitioned from taking care of technological tasks to playing a more strategic role, reporting directly to the board. Boards of directors are now expected to play an active role in managing cybersecurity risk for companies operating in diverse geographical locations. This shows that cybersecurity risk is basically a business risk which needs to be tackled by top management. [1, 3].

At a time of rapid digital transformation, modern cybersecurity requires a comprehensive, flexible approach based on state-of-the-art technology, effective governance, and continuous skill-building of people. The ransomware case highlighted in the current article proves that the scope of cybersecurity threats extends beyond single individuals to include important national infrastructure. It also proves that the number one entry point for a cyber-threat is a human being whose actions have caused a vulnerability. The involvement of non-sanctioned distribution channels of software, data concealment practices associated with social engineering tactics and, finally, a rational economics of ransom demand are all factors making human involvement crucial.

Transitioning to Zero Trust Architecture, using machine learning and artificial intelligence to detect and mitigate cyber threats, integrating security into software development, and engaging proactively with the changing regulatory landscape constitute some key aspects of achieving cyber resilience. Cybersecurity as a strategic priority for both individuals and organizations puts them in the best possible position in the context of reaping benefits and mitigating risks of digital transformation.

Список литературы

1. Хидаятуллах Д.Е.Р., Кунти Р., Харвахю Р. Проектирование и анализ управления рисками информационной безопасности на основе ISO 27005: пример внедрения в системе управления аудитом (AMS) отдела внутреннего аудита XYZ // Международный журнал электротехники, компьютерных и биомедицинских наук. – 2024. – № 3, том 2. – DOI: 10.62146/ijecbe.v2i3.81.
2. ФСТЭК России. Методические рекомендации по обеспечению информационной безопасности критической информационной инфраструктуры // ФСТЭК России. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2456> (дата обращения: 10.03.2025).
3. Сумин, В. И. Использование ситуационного моделирования в разработке систем принятия решений для сложных организационных систем / В. И. Сумин, А. С. Кравченко, А. В. Толкачев // Моделирование систем и процессов. — 2024. — Т. 17, № 3. — С. 71–79. — DOI 10.12737/2219-0767-2024-69-77. — EDN FBBHJO.
4. Тираканок С., Уэхара Т., Инохата А. Миграция к архитектуре нулевого доверия: обзоры и проблемы // Security and Communication Networks. – 2021. – № 1, том 2021. – С. 9947347. DOI: 10.1155/2021/9947347.
5. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. — М.: ДМК Пресс, 2021. — 592 с.
6. Хрящев В.В., Ненашев А.В. Эффективность внедрения одноранговой распределенной системы хранения и обработки защищаемой информации (TheOOL Project) // Моделирование систем и процессов. – 2021. – № 3, том 14. – С. 82–89. DOI: 10.12737/2219-0767-2021-14-3-82-89.

References

1. Hidayatullah D.E.R., Kunthi R., Harwahyu R. Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department // International Journal of Electrical, Computer, and Biomedical Engineering. – 2024. – No. 3, Vol. 2. – DOI: 10.62146/ijecbe.v2i3.81.
2. FSTEC of Russia. Methodological Recommendations for Ensuring Information Security of Critical Information Infrastructure // FSTEC of Russia. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2456> (date of reference: 10.03.2025).
3. Sumin V.I., Kravchenko A.S., Tolkachev A.V. The use of situational modeling in the development of decision-making systems for complex organizational systems. Modeling of systems and processes. 2024. Vol. 17, No. 3. pp. 71–79. DOI 10.12737/2219-0767-2024-69-77. EDN FBBHJO.
4. Teerakanok S., Uehara T., Inomata A. Migrating to Zero Trust Architecture: Reviews and Challenges // Security and Communication Networks. – 2021. – No. 1, Vol. 2021. – P. 9947347. DOI: 10.1155/2021/9947347.
5. Shangin V.F. Information protection in computer systems and networks. Moscow: DMK Press, 2021. 592 p.
6. Khryashchev V.V., Nenashev A.V. Efficiency of Implementing a Peer-to-Peer Distributed Storage and Processing System for Protected Information (TheOOL Project) // Modeling of Systems and Processes. – 2021. – No. 3, Vol. 14. – P. 82–89. DOI: 10.12737/2219-0767-2021-14-3-82-89.