Centrum Rzeczoznawstwa Budowlanego

Inżynieria Bezpieczeństwa Obiektów Antropogenicznych 2 (2024) 1-8
https://inzynieriabezpieczenstwa.com.pl/

Inżynieria Bezpieczeństwa Obiektów Antropogenicznych

Simplifying security processes in large organizations while maintaining an appropriate level of security

Aleksandra PYRKOSZ[1], Sabina SZYMONIAK[1*]

[1] *Department of Computer Science, Częstochowa University of Technology, Częstochowa, Poland*

Abstract

This paper presents an approach to simplifying security in large organizations, ensuring that the work of ordinary employees is more accessible without negatively impacting the organization's security. Access to the Internet is becoming increasingly important in various aspects of human life, including interpersonal communication, professional work, and business operations. Enterprises have digitized information on their devices, which can be of interest to attackers. Incorrect security measures can expose companies to various losses, such as financial costs or image losses. As the number of enterprises connected to the Internet grows, IT system security is gaining importance. Cyberattacks are malicious actions by individuals or organized groups with motives such as financial gain, employee dissatisfaction, or government interference. Attackers aim to access financial data, customer lists, financial data, and customer databases. Cybersecurity should be the basis of every organization, regardless of its size. The number of attacks each year is related to increased investments in cybersecurity strategies and focusing on finding and stopping hackers. Information security protects information to prevent unauthorized access, use, and disclosure. It includes implementing policies and procedures to protect information and prevent data loss or theft. However, implementing security measures can be challenging for ordinary employees, leading to decreased security.

Keywords: security policy, organization security, security tools, cyberattacks, security

1 Introduction

From year to year, access to the Internet is becoming increasingly important in all spheres of human life. First, the Internet is used for interpersonal communication, sharing opinions, news or achievements. We use the Internet to

* **Corresponding author:** E-mail address: (sabina.szymoniak@icis.pcz.pl) Sabina SZYMONIAK

https://dx.doi.org/10.37105/iboa.186
Received 16 October 2023
Available online 10 June 2024
ISSN 2450-1859, eISSN 2450-8721
Published by Centrum Rzeczoznawstwa Budowlanego

purchase, pay bills or book doctor appointments. Internet access is equally essential for professional work. Virtually every company, regardless of its size, has an Internet connection. This makes it easier for business owners to run their businesses and for clients to collaborate (Steingartner et al., 2021; Szymoniak, 2021).

Enterprises have digitized information on their devices, such as customer, contractor and employee data, information about sales and financial results, and much more. All of the previously mentioned data may be of interest to enterprise attackers. Incorrectly taking care of security can expose companies, regardless of their size, to various losses, such as financial costs or image losses. In times when the number of enterprises connected to the Internet is growing, taking care of the security of IT systems is gaining importance. A vast selection of solutions on the market ensures security and minimizes the likelihood of an incident that could affect the functioning of the business (Ainslie et al., 2023).

Cyberattacks are malicious and deliberate actions by an individual attacker or an organized group of criminals. Their effects may include software corruption, data leakage, or the use of compromised hardware as a starting point for an attack on another system. The attackers perform the attacks for the following reasons. First, they seek a financial purpose by stealing money from online bank accounts, stealing data or disrupting business operations (criminal motivation). Second, they are dissatisfied with current or former employees, so the attack can disrupt company systems (personal motivation). Next, the attack interfered with the functioning of, among others, government information systems to create chaos among the inhabitants of the attacked country. Targets of attacks in cyberspace (political motivation). The attacker aims to access financial data, customer lists, customer financial data, and customer databases, including data that uniquely identify customers, access data such as logins and passwords, trade secrets and product designs, IT infrastructure access to IT services and sensitive personal information (Steingartner et al., 2022; Szymoniak and Kesar, 2023).

A security breach can occur in many different places with different activities. Information security protects information to prevent unauthorized access, use and disclosure. It includes implementing policies and procedures to protect information and help prevent data loss or theft. Information security is based on three essential elements: confidentiality (information is available only to authorized entities), integrity (any unauthorized or undesirable modifications of information are prohibited) and availability (information can always be accessed if allowed by the security policy information). They are commonly called the CIA triad (Sarker et al., 2021).

All the security measures that an organization must implement to ensure an appropriate level of security may often prove too demanding and challenging to comply with by ordinary users, i.e. employees of the organization, and may also contribute to lowering the level of security. For example, a poorly adjusted policy for creating and changing employees' passwords may result in subsequent passwords of the same employee differing from each other by one character. Bearing in mind both the appropriate level of security of organizations and their data, as well as the comfort of working in the organization's environment, in this article, we will present our approach to simplifying security in large organizations. Simplifying security to make the work of ordinary employees easier will not have a negative impact on the level of security of the organization and its data.

The main contributions of this paper are as follows:

- the analysis of solutions that are worth implementing to make organizations more resilient to the challenges posed by the increasing dependence on Internet access,
- considerations on the appropriate level of security, system protection and business continuity, liability after an attack,
- analysis and proposals for solutions that simplify and increase security.

The organization of the rest of this paper is as follows. Section 1 presents the literature review of research on security in organizations. In section 2, we present an overview of typical cyber-attacks that are dangerous for organizations and their employees. Section 3 describes the role of security in organizations. In the last section, we present our conclusions.

2 Literature review

We can consider the process of simplifying security in large organizations while maintaining an appropriate level of security in a few cases. The two prominent are security policies, legislation, and other guidelines for organizations' security and supporting tools.

Mishra et al. in (Mishra, 2023) highlighted the need to safeguard organizations' IT infrastructures. They suggest that security policies are one of the security measures that protect an enterprise's cyberspace. Also, they pointed out that security policies depend on the business sector because each has its own rules. Thus, in (Mishra et al., 2022), Mishra et al. defined critical attributes for cybersecurity issues (telecommunication, network, Cloud computing, online banking, E-commerce, identity theft, privacy, and smart grid). The authors pointed out that each nation has its own rules and guidelines, and some focus on some more than others. Saeed in (Saeed, 2023) suggested that employees use computing equipment more cautiously when aware of potential security breaches and vice versa. This could result in more sustainable and secure workplace technology usage. The author identified essential constructs for improving security in the model: password management, infrastructure security management, email management, organizational security policy, and security perception.

The organizations' security is also ensured by many tools and frameworks. Mishra et al. in (Mishra et al., 2023) proposed a framework that enhanced cloud data storage privacy-preserving attributes. This framework employs a one-time password authentication method and a multi-layer encryption storage structure. Mishra in (Mishra, 2023) proposed the artificial intelligence-based technique to prevent unexpected risks from devouring a business in the financial sector. Kamariotou (Kamariotou and Kitsios, 2023) proposed an International Telecommunication Union guidelines-based model for successfully developing and implementing a cybersecurity strategy.

Also worth mentioning are other tools created to improve security in organizations. Intrusion Detection Systems look for abnormal activity and send out alarms when it does for analysis and appropriate incident handling (Yang et al., 2023; Dina et al., 2023; Altaf et al., 2023). Also, the tools for verifying security protocols can improve security levels and confirm if the protocol is secure for communication (Szymoniak et al., 2018; Cheval et al., 2023).

3 Security optimization

When implementing IT systems, finding a kind of golden mean between the appropriate level of security and the comfort of using such a system is desirable. When approaching security design, an exciting solution may be to start from the industry in which the organisation operates. A different approach may be in the healthcare, governmental, military or private sectors. Therefore, the level of security should be adapted to the type of system and context in which it is used. However, the common denominator will be the appropriate security of such systems so that users can perform daily duties efficiently. A careless and careless approach to security can lead to an increased likelihood of a cyberattack on the organisation and, consequently, data loss and/or encryption. Figure 1 summarizes organisations' network threats and network security.

On the other hand, when the level of security is too complex, it may make it difficult for the user to use the system or lead to attempts to bypass such security measures. For example, if the user is asked to authenticate too often, he will set a password that is easy to type, which may make it easy for brute-force attackers to guess the password. To counteract such practices, the IT department could introduce restrictive password policies, and if they were too strict, users would write their passwords on sticky notes, which is also unacceptable from a security point of view. Forcing users to enter their credentials frequently can also lead to user frustration as they will be forced to constantly re-login to the services they use for work. Whitelisting acceptable websites that a user may visit at work is a good solution, while IT can also block access to domains that may be useful from the user's point of view. The website www.youtube.com can serve as an example - it poses no threat to the organisation. However, the company's management may consider it a potential source of wasting time for the user who watches movies instead of performing his duties. Such seemingly legitimate restrictions may lead an irritated user to look for workarounds to such security measures.

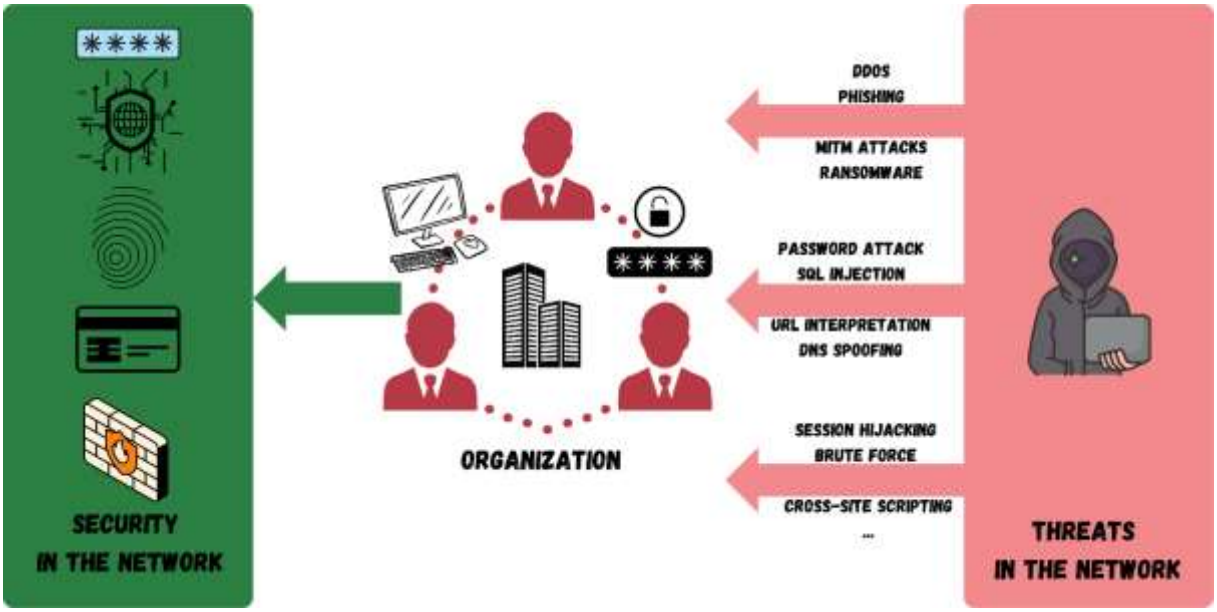

Figure 1. *Summary of network's threats and network's security in organizations*.

Monitoring user activity on the corporate network and recording event logs is one of the most important aspects of maintaining a secure infrastructure. However, there is the user's privacy issue, who is constantly monitored for his work activities.

The user may feel uncomfortable knowing that everything he does is recorded and is constantly monitored. The use of password managers can significantly improve the user experience. Thanks to them, users do not have to remember all their passwords because the software for storing passwords will be responsible for this activity. The user only needs to remember the access data to the device and the master password for the password manager.

SSO (Single Sign On) also improves the user experience by eliminating the need to remember multiple passwords, speeding up login times, and ensuring consistent login sessions. This makes it easy for users to use different services, saving time and minimising the hassle of the authentication process.

When collecting logs, it is good practice to anonymise them. This protects users' privacy and positively affects the sense of greater user comfort. Removing or replacing unambiguously identifying information helps prevent the identification of specific people based on the collected logs.

4 Simplifying security to optimize cybersecurity practices

The cybersecurity landscape is constantly changing, so building the right level of security is not easy. One way is to observe current threats and try to counteract them constantly. A ransomware attack is one of the most common threats against which a company must defend itself. This attack aims to encrypt hardware or steal data and then try to extort money. If the company does not pay, the attackers block the infrastructure, and the data they stole may be made public.

To defeat your opponent, we must use a strategy that reflects his mindset. Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a knowledge base of attackers' tactics and techniques based on real-world observations and used to develop threat models. The Mitre model consists of 14 tactics and their associated attack techniques. Reconnaissance is gathering the information needed to plan future activities, while resource preparation prepares the tools and necessary resources to carry out the attack. Gaining access refers to initial access to the victim's network or system, and execution refers to introducing malicious code. Persistent access refers to maintaining a presence on the network even when the computer is turned off, and privilege escalation is an attempt to gain higher privileges, such as administrator privileges. Masking includes practices aimed at avoiding detection, and obtaining login data refers to obtaining logins, passwords, PINs, etc. Recognition of the environment involves identifying available resources, and movement is based on navigating the victim's network from one infected device to another.

Harvesting is about collecting various types of data, and remote control involves establishing remote control over an infected system. Exfiltration refers to obtaining data in a way that is difficult to detect, such as through encrypted tunnels, while the impact is the effects of an attacker's actions on the victim's system, such as encrypting data in the case of ransomware.

Thanks to the Mitre model, we can present a specific attack that is a potential threat to the organization and identify security measures against it. The analysis of such an attack makes it possible to assess the vulnerability of individual system components, critical devices, and software that may play an essential role in interrupting or disrupting an attack.

Incorporating the Mitre ATT&CK model can bring many benefits. Access to the database is used by the Red Team and research teams to identify specific issues and allows management to gain a clear understanding of future security challenges. Through this access, it is possible to obtain answers to questions such as which attack groups are focused on a particular industry, what techniques and tools they use, whether it is possible to detect these techniques and what to use to mitigate these techniques. ATT&CK secured area mapping not only provides a clear picture of what we can protect against but is also the first step in improving your ability to detect and respond to incidents. Staff training using the Mitre model enables the implementation of tactics based on systematic analysis and techniques for prioritizing information on the most likely threats. The most effective approach to using the ATT&CK framework is to test defence solutions and check their effectiveness indicators.

Thinking about simplifying security while maintaining an appropriate level of security, it is possible to remember about correctly configuring Windows. There are many solutions on the market for which we have to pay. Therefore, it is worth looking at what Microsoft offers as part of the built-in security tools implemented in the operating system. One such tool is Windows Sandbox. A sandbox environment is an isolated virtual machine where potentially dangerous software code can run without affecting network resources or local applications.

Another exciting solution is SmartScreen, which protects against phishing sites, malware and downloading potentially harmful files. Analyze the websites we visit and check them against phishing lists and malware. In addition, it evaluates downloaded applications and files, checking their reputation and matching them with known threats. Microsoft Defender SmartScreen warns users about suspicious sites and files, supporting the fight against phishing, scams, malware and drive-by attacks. It also protects against dangerous URLs and applications by assessing the reputation and blocking addresses related to potentially unwanted applications. It is integrated with Windows 10 and 11, uses heuristics and diagnostic data, and allows management through Group Policy and Microsoft Intune.

Thinking about simplifying security while maintaining an appropriate level of security, it is possible to remember about correctly configuring Windows. There are many solutions on the market for which we have to pay. Therefore, it is worth looking at what Microsoft offers as part of the built-in security tools implemented in the operating system. One such tool is Windows Sandbox. A sandbox environment is an isolated virtual machine where potentially dangerous software code can run without affecting network resources or local applications.

Windows Defender Exploit Guard is another security tool. The four components of Windows Defender Exploit Guard are designed to protect the device from various attack vectors and block behaviours commonly used in malware attacks while allowing enterprises to balance security risks with productivity requirements.

BitLocker Drive Encryption, or BitLocker, is a security and encryption feature. It allows users to encrypt all data on the drive where Windows is installed, protecting it from theft or unauthorized access.

Microsoft BitLocker improves file and system protection by limiting unauthorized access to data. It uses the advanced AES encryption standard with 128 or 256-bit key lengths. BitLocker combines an on-disk encryption process and special key management techniques.

BitLocker uses a specialized chip called the Trusted Platform Module (TPM). The TPM stores RSA (Rivest-Shamir-Adleman) encryption keys specific to the target system used for hardware authentication. The computer's original manufacturer installs the TPM and works with BitLocker to protect your data.

In addition to TPM, BitLocker can block the boot process until the user enters a PIN or inserts removable media, such as a flash drive with a boot key. BitLocker also creates a recovery key for the user's hard drive if they forget or lose their password.

AppLocker is an application control feature available in enterprise editions of Windows. The tool allows us to manage the applications and files that users can run. With AppLocker, we can control various types of applications

such as executable files (.exe and .com), scripts (.js, .ps1, .vbs, .cmd and .bat), Windows installer files (.mst, .msi and .msp), DLL files (.dll and .ocx), and packaged applications and packaged application (.appx) installers. We can define policies based on file attributes from the digital signature, including publisher, product name, file name, and file version. For example, we can create a policy based on a publisher attribute that persists during updates, or we can create a policy for a specific version of a file. Assign policies to a security group or individual user. Create policy exceptions. For example, we can create a policy that allows all Windows system processes except Registry Editor (Regedit.exe). Use audit-only mode to implement the policy and understand its impact before implementing it.

Windows Firewall is a network traffic control mechanism built into the Windows operating system. Its primary task is to monitor and block unauthorized network traffic to and from our computers. It offers many security features, such as blocking incoming connections, port management, configuration of security rules and advanced filtering options. The advantage of implementing a Windows Firewall is that it is built into the operating system. Installing additional software is unnecessary, which can lead to time and resource savings. Windows Firewall offers a simple user interface that allows us to easily manage security rules and configurations. Administrators can create and customize network access rules for individual applications and services. It offers advanced features like filtering network traffic based on IP addresses, ports and protocols, and web content. It can also run in network protection mode, monitoring real-time traffic and blocking suspicious connections. Windows Firewall has been optimized for performance and minimal use of system resources. Thanks to this, it does not burden the computer or the network, which is essential for companies with many users.

In addition to tools that can be managed within the infrastructure, it is also worth using cloud-based solutions because cloud services often offer advanced security and data protection mechanisms. Local solutions (on-premise) give greater control over data and resources, while cloud services give access to new tools that increase cyber security.

One such tool offered by Microsoft is Intune. It is used to manage devices such as phones, tablets and laptops. Intune can also control apps by configuring specific policies. For example, it can prevent access to sensitive corporate data from unknown login locations. Provides support for multiple mobile environments and secure management of iOS/iPadOS, Android, Windows and macOS devices. Provides the ability to set rules and configure settings for data and network access on devices owned by individuals and organizations, including deploying security agents and endpoint policies. It provides deployment and verification of applications locally and on mobile devices. Protects corporate information by controlling how users access and share it. With Intune, we can ensure that our devices and apps meet security requirements.

Another tool worth noting is Microsoft Defender for Cloud. It is used to manage the level of security and protection against threats for cloud services such as microservices and applications. Integrated with Microsoft Defender plans, they provide additional security for cloud resources and protect workloads running on Azure, hybrid and other cloud platforms. Defender for Cloud allows us to assess security. The higher the rating, the lower the risk. Proposes a recommended configuration to improve security. Defender for Cloud detects resource and workload threats and displays alerts in the Azure portal. It can also send alert emails to the appropriate people and forward them to SIEM or SOAR solutions, enabling integration with Defender for Endpoint.

Microsoft Defender for Endpoint is an endpoint security platform for enterprise networks that helps prevent, detect, and respond to advanced endpoint threats. Microsoft Defender for Endpoint uses behavioural analysis, machine learning, and artificial intelligence to detect suspicious activity and targeted attacks. It can recognize advanced malware, privilege escalation attempts, phishing attacks, ransomware and many other threats. The platform monitors the activity of end devices and analyzes suspicious activities, such as attempts to change the system registry, suspicious system calls, unauthorized changes to files, etc. This allows for early detection and response to attacks. Integrates with other company security solutions such as Defender for Cloud, Defender Antivirus, and Intune. Moreover, it also provides tools for incident analysis, security management, and remediation. It helps identify, understand and respond to attacks and mitigate the impact of incidents.

Microsoft's Data Loss Prevention for Endpoint (DLP) tool is part of the Microsoft Defender for Endpoint service. It protects the organization against data loss and unauthorized flow outside the company's infrastructure. DLP is configured at the level of end devices, such as computers and mobile devices, and monitors user activity to detect potential security breaches. The DLP tool identifies potential data leaks by monitoring user activity on end devices. It can analyze the content of files, e-mails, instant messengers and other applications to detect sensitive information such as personal information, financial data or confidential documents. If irregularities are detected, the DLP tool can take preventive actions, such as blocking the sending of messages and warning users. DLP for Endpoint enables organizations to define and apply compliance rules that meet legal requirements and internal data protection policies. We can set up rules for different categories of data, such as personal information, sensitive documents, or financial

information, and specify the actions that will be taken if these rules are violated. An additional advantage of DLP is the possibility of integration with AIP. It provides the ability to monitor user activity, such as sending e-mails, copying files or using applications, to detect potential activities that do not comply with security policies. It can also restrict access to specific resources, such as folders or servers, based on user roles, access hours or geographic location to prevent unauthorized activities. It provides analytics and reporting capabilities that enable organizations to monitor user activity, allowing them to better understand the risk of data loss and take appropriate remedial action.

To integrate the corporate environment with cloud solutions, it is necessary to migrate Active Directory (AD) to Azure Active Directory (Azure AD). Azure AD is a cloud identity and access management service. Allows employees to access external resources such as Microsoft 365, the Azure portal and thousands of other SaaS applications. Azure Active Directory also helps us access internal resources, such as applications on your corporate intranet and cloud applications developed for your own organization. The organization also has the option of a hybrid Azure AD deployment with Azure AD Connect, which synchronizes data between on-premises domain controllers and the cloud. AD Connect allows us to synchronize user accounts from the local system to the Azure tenant. It allows users to have the same user ID and password on-premises and in the cloud, making it easier to manage a hybrid environment.

Azure Information Protection (AIP) is a cloud platform service that enhances cybersecurity by classifying, labeling, encrypting, and controlling data access. It allows organizations to assign labels to documents and files based on content and relevance, ensuring data is easily identified and managed. AIP also enables data access rights based on classification and labelling, allowing for strict control over access. It also provides auditing and monitoring features for tracking sensitive data activity.

SIEM (Security Information and Event Management) is a comprehensive security system that helps organizations detect threats and minimize attack impact. It collects logs and events from various infrastructure components and aggregates them into a central platform. SIEM categorizes data, facilitating investigations. Alerts are sent to relevant security teams, with different priorities set using predefined rules.

SIEM systems collect and store logs, providing real-time information on security system operations. These logs are processed by agents or applications on monitored systems, allowing for the correlation of events with security incidents. The system uses built-in rules and predefined attack scenarios to identify relevant information. Visualization of data and events is crucial for identifying trends and anomalies, ensuring the overall health of the environment. Regularly monitoring SIEM events can identify problems or irregularities in an organization's network environment, detecting Shadow IT, which refers to the use of information systems, devices, software, applications, and services without IT department consent.

Shadow IT can benefit employees using platforms and tools that increase productivity, improve efficiency and positively affect business operations. However, Shadow IT also introduces significant risks to organizations. Suppose corporate data is placed on unapproved services or platforms like cloud storage or a communication platform like Slack. In that case, that data is beyond the visibility and control of IT and security teams. If the security settings of this platform are misconfigured, for example, by publicly sharing cloud drives, sensitive corporate data may be compromised. Shadow IT is a risk in any organization because employees can benefit from unapproved services and transfer sensitive data to them. IT shadow protection is essential to gain visibility into the unauthorized use of IT services and protect corporate data from unauthorized access and disclosure.

5 Conclusions

In this paper, we provide valuable guidance for the organization on the approach to security issues, taking into account the elements that should be paid attention to when increasing the level of security, as well as suggestions regarding techniques and tools that can facilitate the implementation process to some extent.

Nowadays, being connected to the network has become commonplace, so being aware of the importance of organizational security is extremely important. However, it should be remembered that determining the appropriate level of security can be difficult, as it depends on the specifics of each organization. Nevertheless, balancing maximum protection and minimum impact on employees and business continuity is crucial.

Cybersecurity is a highly complex field, but it cannot be underestimated. Failure to do so can lead to severe consequences, such as loss of confidential information, reputation, customer trust, and business disruption. Therefore,

it is essential to always allocate a sufficiently large budget for cybersecurity, not only in the event of incidents. Proactive actions and prevention of attacks are much more beneficial than reacting to their effects.

Information security employees should stay updated on the latest attack methods and vectors, using frameworks like Mitre ATT&CK or Cyber Kill Chain. Implementing safety recommendations and utilizing existing company resources can save significant financial savings.

It is necessary to remember that IT and users must work together and make joint efforts to ensure cybersecurity. Appropriate security at the physical and logical level is essential, but with proper training in the field of cybersecurity, even the best security may be enough. Properly trained employees are the best barrier against attacks because they can recognize and react to threats appropriately.

Bibliography

1. Ainslie, S., Thompson, D., Maynard, S., Ahmad, A. (2023). Cyber-Threat Intelligence for Security Decision-Making: A Review and Research Agenda for Practice. Computers & Security, 103352.
2. Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R.P., Braun, R. (2023). A new concatenated Multigraph Neural Network for IoT intrusion detection. Internet of Things, 100818.
3. Cheval, V., Cortier, V., Debant, A. (2023). Election Verifiability with ProVerif. In: 2023 2023 IEEE 36th Computer Security Foundations Symposium (CSF)(CSF), pp. 488–503. IEEE Computer Society.
4. Dina, A.S., Siddique, A., Manivannan, D. (2023). A deep learning approach for intrusion detection in Internet of Things using focal loss function. Internet of Things, 100699.
5. Kamariotou, M., Kitsios, F. (2023). Information Systems Strategy and Security Policy: A Conceptual Framework. Electronics, 12(2), 382.
6. Mishra, A., Alzoubi, Y.I., Anwar, M.J., Gill, A.Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120, 102820.
7. Mishra, A., Jabar, T.S., Alzoubi, Y.I., Mishra, K.N. (2023). Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework. Concurrency and Computation: Practice and Experience, 7831.
8. Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences, 13(10), 5875.
9. Saeed, S. (2023). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. Sustainability, 15(7), 6019.
10. Sarker, I.H., Furhad, M.H., Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 1–18.
11. Steingartner, W., Galinec, D., Kozina, A. (2021). Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. Symmetry, 13(4).
12. Steingartner, W., Možnik, D., Galinec, D. (2022). Disinformation Campaigns and Resilience in Hybrid Threats Conceptual Model. In: 2022 IEEE 16th International Scientific Conference on Informatics (Informatics), pp. 287–292. IEEE.
13. Szymoniak, S. (2021). Amelia—A new security protocol for protection against false links. Computer Communications, 179, 73–81.
14. Szymoniak, S., Kesar, S. (2023). Key Agreement and Authentication Protocols in the Internet of Things: A Survey. Applied Sciences, 13(1), 404.
15. Szymoniak, S., Siedlecka-Lamch, O., Kurkowski, M. (2018). On some time aspects in security protocols analysis. In: Computer Networks: 25th International Conference, CN 2018, Gliwice, Poland, June 19-22, 2018, Proceedings 25, pp. 344–356. Springer.
16. Szymoniak, S., Siedlecka-Lamch, O., Zbrzezny, A.M., Zbrzezny, A., Kurkowski, M. (2021). SAT and SMT-Based Verification of Security Protocols Including Time Aspects. Sensors, 21(9).