Zero Trust Architecture in Corporate Cybersecurity Systems

Moskvin Kostiantyn
Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, kostiantyn.moskvin@nure.ua

Sievierinov Oleksandr
Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, oleksandr.sievierinov@nure.ua

Abstract. *The Zero Trust architecture is described as a modern approach to cybersecurity based on the principle of a complete lack of trust in any network elements. The main principles of Zero Trust and implementation stages are considered. The advantages of Zero Trust for corporate systems, such as increased security, flexibility, compliance with regulatory requirements, and reduced attacks, are identified. The problems of implementation are considered and recommendations for the successful integration of Zero Trust in organizations are given.*

Keywords: *Zero Trust Architecture, Continuous Verification, Multi-Factor Authentication (MFA), Micro-Segmentation, Insider Threats, Modern Cyber Threats, Artificial Intelligence and Machine Learning*.

I. Introduction and Problem statement

In the digital age, information has become one of the most valuable assets of companies. However, as technology advances, so do cyber threats. According to research by IBM Security, the average cost of a data breach in 2023 was $4.45 million, the highest in 20 years [1]. Traditional cybersecurity models based on protecting the network perimeter can no longer effectively counter modern attacks. Attackers are finding ways to bypass perimeter defences through phishing, software vulnerabilities and other methods.

The increasing number of remote employees and the use of personal devices to access corporate resources creates additional risks. In such conditions, it is necessary to rethink approaches to security and move to a model that takes into account modern realities. One of the solutions is the use of Zero Trust architectures in corporate cyber security systems. Therefore, the research of the principles of this architecture, the main steps of implementation, advantages and disadvantages is a relevant direction.

II. Problem solution and Results

The Zero Trust architecture, proposed by Forrester Research in 2010, is a response to these challenges, offering a new cybersecurity paradigm based on a complete lack of trust in any network elements.

The analysis made it possible to determine the main principles of Zero Trust architecture [2-4]:

– Lack of trust by default. The basic principle of Zero Trust is a complete lack of trust in any user or device, regardless of their location. This means that even if a device is connected to the company's internal network, it does not automatically get access to resources. Each access request must be verified and authorised. This approach significantly reduces the risks associated with insider threats and account compromise;

– Continuous verification. Zero Trust requires continuous authentication and authorisation of each request. The system must take into account various factors such as user identity, geolocation, time of day, device status, and other attributes. For example, if a user usually works from an office in Kyiv and suddenly tries to connect from another country, the system should detect this anomaly and request additional verification. This approach provides dynamic security adapted to the context of each request;

– Least Privilege Access. Users and devices are granted only the level of access necessary to perform their tasks. This means that even if an attacker gains access to an account, their capabilities will be limited. For example, an accountant should not have access to network equipment configurations, and an IT administrator should not have access to financial data. This approach reduces the attack surface and potential damage from compromise;

– Network segmentation. Dividing a network into isolated segments or zones helps limit the horizontal movement of attackers in the event of a compromise. This is achieved through VLANs, software-defined networking (SDN), and micro-segmentation, where each application or service runs in an isolated environment. For example, database servers can be isolated from web servers, and only certain services are allowed to access them. This makes it difficult for attackers to spread across the network and gain access to critical resources;

– Monitoring and analytics. Continuously collecting and analysing data about network activity is critical to quickly detecting and responding to threats. Modern systems use artificial intelligence and machine learning to analyse user and device behaviour, detect anomalies and potential threats in real time. This allows not only to respond to incidents but also to predict possible attacks. For example, if the system detects unusual activity, such as a large number of database queries at an unusual time, it can automatically block access and notify the administrator.

The stages of Zero Trust implementation include several key steps that need to be taken to effectively implement this architecture [4, 5]. First of all, it is important to conduct a detailed inventory of all resources, users, devices, applications and data on the network. This involves creating a network map, identifying critical assets and understanding the data flows between them. Without a complete understanding of what needs to be protected, it is impossible to implement Zero Trust effectively. In addition, vulnerabilities and potential entry points for attackers should be identified so that potential attacks can be prevented.

The next step is to implement multi-factor authentication (MFA), which is one of the most effective ways to prevent unauthorised access. In addition to using a password, the user must confirm their identity using additional factors, such as a fingerprint, SMS code, hardware token, or mobile app. This

makes it much harder for attackers to crack the password, even if they have it. It is important that MFA implementation is user-friendly to avoid resistance to change and ensure widespread adoption of the technology across the organisation.

Next, you need to create detailed and flexible access policies. These policies should take into account the user's role in the organisation, the level of trust in the device, geolocation, access time, and other relevant attributes. For example, access to financial systems may be allowed only from certain devices and only during business hours. Policies should be dynamic and automatically adapt to changing conditions to ensure a high level of security and compliance with business processes.

The use of micro-segmentation technologies is another important aspect. This allows you to create isolated environments even within a single server or application, which reduces the attack surface and makes it difficult for attackers to move horizontally across the network. Software-defined networking (SDN) technologies provide the ability to dynamically manage network segmentation based on established policies and context. For example, if a particular application should not interact with other applications, you can set up appropriate firewall rules to limit such interaction.

Implementation of monitoring and analytics tools is an integral part of the Zero Trust architecture. Security information and event management (SIEM) systems, endpoint detection and response (EDR) solutions, and network traffic analysis tools allow you to collect and analyse data from various sources. This allows you to correlate events and detect anomalous activity in real time. The use of artificial intelligence and machine learning increases the accuracy and speed of threat detection. For example, a SIEM system can automatically alert you to suspicious activity and suggest specific actions to take, allowing you to quickly neutralise potential threats.

Finally, attention to the human factor is critical, as it remains one of the weakest points in cybersecurity. Regular training for employees on new policies, procedures and current threats helps to increase staff awareness and responsibility. This includes training on how to recognise phishing attacks, how to use multi-factor authentication correctly, and the importance of adhering to established security policies. Conducting attack simulations and testing staff readiness can be effective methods for assessing and improving the level of cybersecurity in an organisation.

Thus, a comprehensive approach to implementing a Zero Trust architecture, including technical solutions and human resources, can significantly increase the level of protection of corporate systems against modern cyber threats.

As a result of the analysis, the advantages of Zero Trust for corporate cyber security systems were revealed:

– Increased security. Zero Trust significantly reduces the risk of both external and internal threats. Lack of default trust and constant verification make it harder for attackers to get in and limit their options. Even if an attacker gains access to an account, their actions will be limited by minimum privilege policies. This reduces the potential damage from compromise;

– Flexibility and adaptability. Zero Trust architecture is flexible and can adapt to changes in business processes and technologies. It supports remote work, the use of cloud services and mobile devices, while ensuring a high level of security. This is especially relevant in modern conditions, when many companies have switched to remote work. Organisations can quickly scale their systems without losing control over security;

– Compliance with regulatory requirements. Many industries are subject to regulatory requirements for data protection, such as GDPR, HIPAA, PCI DSS, and more. Implementing Zero Trust helps to comply with these standards by controlling access to data, logging events, and responding quickly to incidents. It also helps to increase trust from customers and partners [6];

– Reducing the consequences of attacks. In the event of a security breach, Zero Trust limits the attacker's ability to move easily across the network and access critical resources. This reduces potential damage and gives administrators more time to identify and eliminate the threat. This approach increases the organisation's resilience to cyberattacks.

Challenges and recommendations [2-4, 6]:

– Complexity of implementation. Transitioning to Zero Trust requires significant resources, both financial and human. It is a complex process that includes infrastructure upgrades, the introduction of new technologies and changes in business processes. It is recommended to start with small projects, gradually expanding Zero Trust across the organisation. It is also important to involve management and ensure support at all levels;

– Integration with existing systems. Compatibility with your current infrastructure can be an issue. Some older systems may not support the necessary security features. It is important to audit the infrastructure and plan for the migration or upgrade of such systems. Working with vendors can help you find the best solutions;

– Resistance to change. Employees may resist new policies and procedures, especially if they make their jobs more difficult. It is necessary to conduct awareness campaigns, explain the importance of the changes and involve staff in the implementation process. Incentives and recognition can be used to increase motivation.

III. Conclusions

Zero Trust architecture is a modern and effective approach to cybersecurity that meets the challenges of the digital age. It provides a high level of protection for information resources, supports business agility and helps meet regulatory requirements. Despite the challenges associated with implementation, the benefits of Zero Trust make it an attractive solution for organisations looking to improve their cybersecurity and be prepared for future threats. Investing in Zero Trust is a strategic move that can ensure long-term business security and success.

References

[1] IBM: average breach costs hit record $4.88M in 2024, up 10% from last year URL: https://10guards.com/en

[2] He, Yuanhang, et al. "A survey on zero trust architecture: Challenges and future trends." Wireless Communications and Mobile Computing 2022.1 (2022): 6476274

[3] Teerakanok, Songpon, Tetsutaro Uehara, and Atsuo Inomata. "Migrating to zero trust architecture: Reviews and challenges." Security and Communication Networks 2021.1 (2021): 9947347.

[4] Gartner: Continuous Adaptive Risk and Trust Assessment (CARTA). URL: www.gartner.com

[5] Forrester Research: Zero Trust eXtended Ecosystem. URL: www.forrester.com.

[6] NIST SP 800-207: Zero Trust Architecture.