

ONE EXAMPLE OF IMPLEMENTING ZERO TRUST ARCHITECTURE

Marija Zajeganović¹ Milan Pavlović² Dragan Ristić³

Abstract: Zero Trust Architecture represents a response to increasingly complex and sophisticated threats in cyberspace, which traditional security models can no longer adequately address. ZTA is a comprehensive and holistic strategy that requires integration across various elements, including identities, endpoints, networks, data, applications, and infrastructure. Governance and compliance are essential for implementing the principles of Zero Trust. For these reasons, transitioning to a Zero Trust Architecture is not a straightforward process but one that must be carefully planned and gradually introduced. This paper presents the fundamental principles of Zero Trust Architecture (ZTA), key technologies supporting ZTA, and recommendations for transitioning from a traditional security model to a Zero Trust framework, illustrated through the example of a small enterprise.

Key words: Zero-Trust, asset, implementation, monitoring, MFA, IAM

1. INTRODUCTION

Zero Trust Architecture (ZTA) is based on the principle of "never trust, always verify." ZTA eliminates implicit trust within the network by requiring continuous identity verification, authentication, and authorization for every user request or access to resources [1]. It is acknowledged that no system is 100% secure, making the goal to enhance resilience against attacks by minimizing potential damage.

To implement a Zero Trust strategy, it is essential to deploy appropriate technologies such as Multi-Factor Authentication (MFA), micro-segmentation, Identity and Access Management (IAM), encryption, and continuous monitoring and analytics. The implementation of ZTA is complex, and standards exist to guide the transition from traditional security models to an optimal ZTA. Transitioning to ZTA cannot occur in a single step; it requires careful planning and gradual adoption.

This paper will present the fundamental principles of ZTA, the key technologies necessary for its implementation, and an example of transitioning to ZTA. Finally, the conclusion will provide guidelines for further improving security.

2. CORE PRINCIPLES OF ZERO TRUST

Zero Trust Security is a model aimed at significantly reducing security risks in large software systems accessed over a network. Its precise definition states: Zero Trust is a security approach for networked systems where each request is independently verified, regardless of attributes such as the request's source, while granting all actors the least privilege necessary [2]. This security model operates under the assumption that the network is already compromised. The core concepts of this definition are: verify explicitly, least privilege access, and assume breach.

No request is implicitly trusted. Each request must be independently verified. Upon receiving a request, its authenticity is validated based on all available information, such as the user's identity, location, device state, service or workload, and anomalies. The identity of the requester is authenticated using credentials, and the requester must have authorization to perform the requested action.

The principle of least privilege ensures that every entity accessing the system is granted the minimum permissions required to access the data and functions necessary for completing a task. This approach limits the potential damage to the system if an entity is compromised.

¹MSc, The Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Zdravka Čelara 16, Belgrade, Serbia, email: marija.zajeganovic@ict.edu.rs

²PhD, The Academy of Technical and Art Applied Studies Belgrade, Department School of Information and Communication Technologies, Zdravka Čelara 16, Belgrade, Serbia, email: milan.pavlovic@ict.edu.rs

³PhD, Telekom Srbija, Takovska 2, Belgrade, Serbia, email: ristic.dragan@gmail.com

The assume breach principle presumes that every access is a potential security breach. In practice, it has been shown that a determined attacker with sufficient resources can breach any system. For this reason, security teams should implement measures that enable rapid detection, minimize the scope of damage, and establish clear procedures for damage remediation for every authorized access to the system.

This approach is particularly effective against attacks involving stolen credentials. Attackers do not need to breach the system they exploit, and therefore, Zero Trust Security significantly reduces the risk of such attacks.

3. KEY TECHNOLOGIES THAT SUPPORT ZERO TRUST

Zero Trust (ZTA) architecture is a security model that relies on a strict approach to authentication and authorization to reduce the risk of attacks. Various aspects of this model allow organizations to implement security measures that make it much more difficult for attackers to compromise the network. The five key Zero Trust security technologies that form the foundation of this architecture are: Multi-Factor Authentication (MFA), Micro-Segmentation, Identity and Access Management (IAM), Encryption Everywhere, and Continuous Monitoring and Analytics.

Multi-Factor Authentication (MFA) is one of the most effective ways to improve security in a Zero Trust architecture environment. Instead of relying only on traditional authentication methods such as username and password, MFA requires additional security factors to verify a user's identity. These factors can include biometric data, such as fingerprints or facial recognition, physical tokens, or generated one-time codes (OTPs). The implementation of MFA in the Zero Trust model enables more accurate verification of user identity and significantly reduces the risk of attacks using stolen or wrong passwords. Each authentication attempt is analyzed based on various factors, ensuring that only legitimate users can gain access to resources, even if credentials are compromised. MFA uses what the legitimate user knows and has.

Micro-segmentation is a key aspect that enables detailed access control and limits potential attacks within the network. In traditional network models, once inside, attackers can easily access different network segments. With micro-segmentation, the network is divided into small, isolated segments where specific security policies are applied. Each segment functions as a separate entity, meaning that even if one segment is compromised, attackers will not have easy access to other parts of the network. This approach is particularly effective in protecting critical data and systems, as it enables fine-tuning of access rules based on user role, location, or even behavioral history. Using micro-segmentation means that access to resources is granted at a granular level, which significantly reduces the chances of an attack spreading from one part of the network to another.

Identity and access management (IAM) systems play a central role in the Zero Trust architecture. IAM allows organizations to centrally control who has access to which network resources. This system includes authentication, authorization and audits of user and device activities. Within the Zero Trust model, the IAM system ensures that only those users and devices that have been previously verified and have the appropriate privileges can access certain data or applications. This approach is based on the strict principle of least privilege, which means that users and devices are not granted broad privileges, but only those that are necessary for them to perform specific tasks. Also, IAM enables continuous monitoring and updating of access rights, which is crucial for timely response in case user accounts are compromised or user status changes.

Data encryption is necessary to protect confidential information and protect against attackers trying to intercept data in transit or while it is stored. In the Zero Trust architecture, encryption is implemented at all levels: both on the network, on devices and in applications. This means that all data, regardless of whether it is at rest or in transit, is protected by advanced encryption algorithms. Encryption reduces the risk of data access even if attackers take control of certain network segments. For example, if attackers intercept data as it is being sent between the user and the server, encryption ensures that the data remains unreadable without the appropriate decryption keys. Given that the Zero Trust model is based on the assumption that the network has already been compromised, encryption is key to ensuring data security at all times.

Continuous monitoring and analysis of all activities within the network enable quick detection of potential threats and taking appropriate measures before more serious system damage occurs. In the Zero Trust model, monitoring is constant, and analytical tools use sophisticated techniques such as machine learning and behavioral analytics to identify unusual activity and potential attacks. Every activity, whether it's accessing data, launching apps or connecting devices, must be amenable to real-time analysis. If the system detects an unusual behavior pattern, such as an unauthorized access attempt or a suspicious increase in traffic, the responsible security team reacts quickly to prevent or minimize the consequences of the attack. This proactive approach allows organizations to recognize threats at very early stages, before they can cause significant damage.

4. ZERO TRUST IMPLEMENTATION

One of the approaches when applying the Zero Trust model is the five-step approach[3]. The five-step approach to the Zero Trust strategy creates a logical, clear path to protecting your environment, data, applications, infrastructure, services and users. How the strategy is implemented depends on the asset being protected and the business requirements, but it is all implemented in a similar way: effective network segmentation to prevent lateral movement through the network if there is a security issue; protect critical business data and infrastructure from unauthorized applications and users to reduce attack vectors; protects business-critical applications from unauthorized access and use to reduce attack vectors; enforce a consistent security policy across the enterprise, networks, clouds and endpoints to simplify management and ensure the same level of access and security to users across all use cases. The same security policy is applied to users wherever they are on the network, so enforcement is consistent across the network.

The scope of zero trust can be large and encompassing, so breaking the process down into smaller, more manageable components is very important. The five-step process for implementing zero trust accomplishes just that. These implementation steps are designed to be flexible, repeatable, and technology independent. This process allows an organization to start with a small, limited initial protection surface (or set of Data, Applications, Assets, and Services - DAAS), go through the rest of the steps with that initial protection surface to establish their approach, and then add additional protection surfaces so the ZTA gradually matures and expands.

The first step is to define the protective surface, i.e., to identify DAAS (Data, Applications, Assets, and Services) elements that require protection. It is also essential to prioritize DAAS elements based on their sensitivity. For instance, there are low-sensitivity assets, moderate-sensitivity assets, and high-sensitivity assets. High-sensitivity assets include not only critical data but also critical services such as Active Directory (AD), DNS, and DHCP.

The second step is to map the flow of transactions. It is essential to understand how networks work by mapping transaction flows to and from the protection surface, including how the various DAAS components interact with other resources on the network. These transaction flows directly inform where appropriate controls should be placed.

The third step is to build a zero-trust architecture. This involves designing a zero-trust architecture tailored to the firewall or firewalls identified in steps 1 and 2. The way traffic moves across the network specific to the data in the firewall should determine the design. Architectural elements cannot be predetermined, although a good rule of thumb is to place controls as close to the protective surface as possible.

The fourth step is creating a zero-trust policy. Zero trust should be set as a level 7 (application) policy statement. In this case, it is recommended to use Kipling's method of writing a zero-trust policy to determine who or what can access the firewall.

The fifth step is network monitoring and maintenance. All traffic up to level 7 (application) needs to be inspected and logged. Telemetry from this process helps prevent significant cyber security incidents and provides valuable insights into improving security in the long term. As a result, each subsequent protective surface can become more robust and better protected over time.

Although ZTA brings significant advantages in the protection of data and infrastructure, the implementation of this model faces numerous challenges, which include technical, organizational and financial aspects.

One of the biggest challenges in implementing the Zero Trust model is harmonizing with existing legacy systems. Many organizations rely on legacy technologies that are not designed to support granular access control or continuous authentication and authorization. These systems often use static authentication methods, such as passwords, or are limited in terms of integration with modern security tools. Migrating or integrating such systems with Zero Trust principles requires detailed planning that includes identifying key vulnerabilities and estimating replacement or upgrade costs. In some cases, it is necessary to develop custom solutions that enable interoperability between legacy systems and new security protocols. This process can be expensive and time-intensive, especially for organizations that use a heterogeneous IT infrastructure.

The introduction of the Zero Trust paradigm often causes resistance within the organization, especially among employees and teams who are not accustomed to stricter security protocols. This model requires a significant change in day-to-day operations, including more frequent authentication, additional layers of authorization, and tighter control of access to resources. Such changes may be perceived as imposing additional obligations or limiting flexibility in work. Employee frustration can be compounded if changes are not adequately explained or if there is no clear communication about the benefits of this approach. To reduce resistance, it is crucial to implement education at all levels of the organization, explaining why Zero Trust is important for keeping data secure and how it contributes to protecting the business. Also, engaging employees in the planning and implementation process can increase their willingness to accept new procedures.

Zero Trust architecture introduces significant complexity in the management of security systems. Organizations must establish detailed access policies that define who, when, and under what conditions can access certain resources. In addition, it is necessary to implement systems for continuous monitoring of user activities, behavior analysis and automation of security processes. This complexity can increase the burden on IT teams, who are faced with additional tasks such as managing certificates, updating access policies and resolving incidents. Organizations that are not adequately prepared for these challenges may face implementation issues, such as inconsistent access policies or an increased risk of human error. It is therefore necessary to invest in employee training and develop standardized processes for managing complex security environments.

Implementing the Zero Trust model requires significant financial investment, which is often a challenge for organizations with limited budgets. Costs include acquiring new technologies, such as multi-factor authentication (MFA), intrusion detection and prevention systems (IDS/IPS), network segmentation, and identity and access management (IAM) tools. In addition, significant resources must be allocated for software licensing, hardware upgrades, and integration of various components. In addition to the financial costs, the investment of resources also includes the hiring of security experts, who are necessary to design, implement and maintain the Zero Trust architecture. The lack of qualified staff in the field of cyber security further complicates this process, as organizations must compete in the labor market to attract or train experts. Implementation costs can be mitigated by a phased approach, focusing on priority areas and using solutions that enable scalability.

In order for the implementation of Zero Trust architecture to be successful, it is necessary to follow several key steps, the most important of which are: identity and access management (IAM), prioritization of high-risk areas, implementation of continuous monitoring and gradual implementation of ZTA.

Identity and Access Management (IAM) represents the basis of the Zero Trust architecture. The first step is to establish a reliable infrastructure for authentication and authorization of users, applications and devices. Multi-factor authentication (MFA) is becoming the standard in securing access, as it reduces reliance on static passwords that are often compromised. In addition to MFA, the application of the principle of least privilege (Least Privilege) is key to restricting access to only resources that are necessary to perform certain tasks. That way, even if user credentials are compromised, the potential damage is minimal.

Before a Zero Trust architecture can be implemented across an organization, it is crucial to identify areas of high risk. These are typically segments that contain sensitive data, critical applications and business-critical infrastructure. Prioritizing these areas allows more efficient allocation of resources and focus on those components that have the greatest impact on the organization's security. Risk analysis should include the identification of potential threats, vulnerabilities and consequences that could arise in the event of a security incident. Using this information, the organization can define control measures that are tailored to the specific needs of each area, such as network segmentation, cloud data protection, and monitoring of privileged users.

Zero Trust architecture requires constant monitoring and analysis of user, device and application activities in order to detect anomalies and potential threats in a timely manner. This involves using advanced tools to collect and analyze real-time data, enabling organizations to recognize and respond to threats before they cause damage. The integration of analytics, automation and artificial intelligence (AI) tools further enhances the monitoring process. For example, Threat Detection and Response systems can identify unusual activities, such as attempts to access outside of business hours or unauthorized changes to data.

A Zero Trust architecture cannot be implemented all at once. A phased approach allows organizations to adapt to change without compromising operational continuity. This approach involves defining implementation phases, testing new policies and evaluating results before scaling up to the entire infrastructure. For example, the initial phase may include the implementation of the Zero Trust principle on network segments that contain sensitive data or have already been the target of previous attacks. After successful testing, the next step can be expansion to less critical parts of the network, with parallel education of employees and adjustment of procedures. A phased approach not only reduces risks during the transition, but also allows the organization to continuously learn from the experiences gained at each stage.

Zero Trust is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real time response to threats[4].

5. CONCLUSION

Zero Trust Architecture cannot completely eliminate threats, but this model can significantly reduce the risk of attacks and their impact when they occur. Attacks are inevitable, and instead of assuming that an impenetrable wall can be built around the network, the Zero Trust approach starts with the expectation that malicious actors will eventually breach the network. When this happens, the Zero Trust approach ensures that controls and solutions are in place to limit the damage that may result.

Although the introduction of ZTA is inevitable, many organizations hesitate to introduce it because of the challenges that exist along the way. Those challenges are of a financial nature, resistance among employees due to new procedures and the complexity of the implementation of the ZTA. It is extremely important that these challenges are overcome and that security awareness changes because what has been proven in practice is that Zero Trust limits the damage from phishing and ransomware, which are the most prevalent cyber attacks.

Monitoring and maintaining a Zero Trust infrastructure involves regular auditing of access privileges, continuous monitoring of network behavior, maintaining up to date security patches, conducting risk assessments and reinforcing user security awareness.

6. REFERENCES

- [1] Zajeganović, M.; Pavlović, M.; Ristić, D.: Possible threats to Zero-Trust architecture, in *Book of proceedings, International Multidisciplinary Conference "Challenges of Contemporary Higher Education" - CCHE 2024*. Kopaonik, Serbia, 2024, Vol 1. pp. 316-320.
- [2] Cybersecurity Division: *Zero Trust Maturity Model - Version 2.0*, Cybersecurity and Infrastructure Security Agency, 2023.

- [3] *Best Practices Implementing Zero Trust with Palo Alto Networks*, Palo Alto Networks, Inc., Santa Clara, California, 2024.
- [4] Weinert, A: *Evolving Zero Trust—Lessons learned and emerging trends*, Microsoft Corporation, 2021.