Zero Trust Security

Ioan-Alexandru DUMITRU
Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest, Romania
dumitrualex2004@yahoo.com

Abstract

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, whether they are inside or outside the perimeter of the network. No specific technology is associated with the Zero Trust architecture; It is a holistic approach to network security that incorporates several different principles and technologies. The traditional security of the IT network is based on the „castle-and-moat" concept. In that model, it's hard to gain access from outside the network, but everyone on the network is trusted by default. The problem with this approach is that once an attacker gains access to the network, he has free rein over everything inside.

Index terms: access management, cybersecurity, Zero Trust architecture

1. Introduction

Zero Trust is a network security model based on a strict identity verification process. The framework stipulates that only authenticated and authorized users and devices can access applications and data. At the same time, it protects those applications and users from advanced Internet threats.

This model was first introduced by an analyst at Forrester Research and, while not a completely new theory, has become increasingly important for modern digital transformation and its impact on the security architecture of business networks. As the modern workforce becomes more and more mobile, accessing applications from multiple devices outside the business perimeter, businesses have adopted a "check, then trust" model, which means that if someone has the correct user credentials, they are allowed on any site, application or device they request. This has led to an increased risk of exposure, dissolving what was once the company's trusted control zone and leaving many organizations exposed to data breaches, malware and ransomware attacks. Protection is now required where applications and data are located, as well as users and devices.

Users, devices, applications and data move outside the enterprise perimeter and control area. New business processes driven by digital transformation increase risk exposure. "Trust, but verify" is no longer an option, as the advanced threats are moving around the perimeter of the company [1].

Traditional perimeters are complex, increase risk and are no longer compatible with current business models. To be competitive, companies need a reliable network architecture capable of protecting enterprise data wherever users and devices are located, while ensuring that applications run quickly and seamlessly.

2. Zero Trust security - history and importance

The term "Zero Trust" was coined by an analyst at Forrester Research Inc. in 2010, when the concept model was first presented. A few years later, Google announced that they had implemented

Zero Trust security in their network, which led to a growing interest in adoption in the technology community. In 2019, Gartner, a global research and consulting firm, listed Zero Trust security access as a core component of Secure Access Service Edge (SASE) solutions.

More than the lack of resources, cyber security seems to be suffering from a lack of an effective approach, especially as the climate of work changes. The emergence of remote work as the norm for many companies comes with new cyber security challenges. Remote work results in less control over the organization's resources, which increases the risk of data breach. Therefore, it is more important than ever to approach cybersecurity from a risk-based perspective.

The idea of Zero Trust has gradually grown over the years, especially with the rise of SaaS and remote work. It has also become more feasible as the technologies and tools built into its framework become commonplace. Zero Trust is rooted in the belief that nothing should be trusted, whether it is online or offline. Instead, always check.

Zero Trust architecture is not a quick fix, nor is it a tool. Rather, as an aviation certification guide, it is a general framework for network security. Because trust is essential for remote teams, it is worth investigating whether eliminating this cybersecurity factor can contribute to greater protection.

3. Main principles and technologies behind Zero Trust security

The philosophy behind a Zero Trust network assumes that there are attackers both inside and outside the network, so no user or machine should be trusted automatically.

Another principle of Zero Trust security is access with the least privilege. This means giving users only access to what they need, such as an army general who provides soldiers with information based on their need to know. This minimizes each user's exposure to sensitive parts of the network.

Zero Trust networks also use micro segmentation. Micro segmentation is the practice of dividing security perimeters into small areas to maintain separate access for separate parts of the network. For example, a network of files that live in a single data center using micro segmentation may contain dozens of separate and secure areas. A person or program with access to one of those areas will not be able to access any of the other areas without separate authorization.

Multi-factor authentication (MFA) is also a core value of Zero Trust security. MFA simply means the need for more evidence to authenticate a user; just entering a password is not enough to gain access. A common application of MFA is 2-factor authorization (2FA) used on popular online platforms such as Facebook and Google. In addition to entering a password, users who activate 2FA for these services must also enter a code sent to another device, such as a mobile phone, thus providing two proofs that they are the ones they are claiming to be.

In addition to user access controls, zero trust also requires strict device access controls. Zero Trust systems need to monitor how many different devices are trying to access their network and ensure that each device is authorized. This further minimizes the attack surface of the network [1].

4. Identity and access management

According to the Verizon 2021 Data Violation Investigation Report, the use of stolen credentials of over-privileged users remains one of the biggest risks and targeting user credentials is the most favored technique of cyber-criminals. It is clear that access management on the device is outdated and insecure. A Zero Trust model provides access based on identity verification, rather than simply confirming the device. This is the idea behind multifactor authentication [2].

But Zero Trust does not stop there; It also includes continuous verification, a useful feature if a legitimate user session becomes hijacked. Zero Trust authentication is adaptive, contextual, and risk based. The most popular Zero Trust model for security authentication is the software-defined

perimeter (SDP). An SDP operates and grants access based on the need to know described above. It is already appreciated as a kind of next generation virtual private network (VPN).

Cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. It is also known as information technology security or electronic information security. The term is applied in a variety of contexts, from business to mobile computers and can be divided into several common categories.

Network security is the practice of securing a network of intruder computers, whether they are targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application may provide access to data designed to protect you. Successful security begins at the design stage, long before a program or device is implemented.

Information security protects the integrity and confidentiality of data, both in storage and in transit.

Operational security (OPSEC) includes processes and decisions for handling and protecting data assets and is a security and risk management process and strategy, and it encourages IT and security managers to look at their operations and systems form an outside perspective. The permissions users have when accessing a network, the procedures that determine how and where and which data can be stored or shared are taken into account [3].

Disaster recovery and business continuity define how an organization responds to a cybersecurity incident or any other event that results in the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan that the organization fits into while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber security factor: people. Anyone can accidentally introduce a virus into an otherwise secure system without complying with good security practices. Learning how to delete suspicious e-mail attachments, not connect unidentified USB drives, and various other important lessons is vital to the security of any organization.

5. The scale of the cyber threat

The global cyber threat continues to evolve at a rapid pace, with an increasing number of data breaches each year. A Risk Based Security report showed that a shocking number of more than 22 billion records were exposed as a result of 4,145 security breaches made public. Although the number is down about 5% from the previous year, the amount of compromised confidential data is the second highest since 2005.

Medical services, retailers and public entities have reported the most violations, and malicious criminals are responsible for most incidents. Some of these sectors are more attractive to cybercriminals because they collect financial and medical data, but all companies that use networks can be targeted for customer data, corporate espionage, or customer attacks [4].

As the scale of the cyber threat continues to grow, governments around the world have responded to the growing cyber threat with guidance to help organizations implement effective cyber security practices.

In the United States, the National Institute of Standards and Technology (NIST) has created a cyber security framework. To combat the proliferation of malicious code and help detect it early, the framework recommends continuous real-time monitoring of all electronic resources.

The importance of monitoring the system is reflected in the "10 Steps to Cybersecurity", provided by the UK Government's National Cyber Security Center. In Australia, the Australian Cyber Security Center (CCAA) regularly publishes guidance on how organizations can counter the latest cyber security threats.

Computer security has become an important part of computer science as it deals with identifying and searching for solutions to remove the main risks involved in accessing the virtual environment through various devices, such as computers, telephones, and mobile devices. The criteria for ensuring information security are availability and accessibility, integrity, identification and authentication, confidentiality, permanence and electronic archiving.

Availability ensures the strengthening of the security of the network or networks of computer systems and the provision of backups. It represents the possibility of using this information system at any time and is a first criterion for measuring the quality and security of the system. Availability is measured by the "number of nines". "Five nines uptime", which is the most common, means that, over a year, a system has been operational or in standby 99.999% of the time, or all but 5 minutes and 16 seconds within the full 365 days. In correlation with availability, there is also the criterion of accessibility, an important factor for data discovery, characterized by: the level of organization of data by classification according to importance or sophistication and the quality of cyber infrastructure that the organization has.

The integrity of the information represents "confirmation that the data transmitted, received or stored by an individual or collective user, are complete and have not undergone any changes", according to the European Union Agency for Cybersecurity. This criterion is so important in information security that it must be approached from 3 directions: technical, legal or organizational. The technical part states that any modification of a simple bit can affect the integrity of the system, the legal criterion focuses on maintaining the meaning of the information in the documents, and from an organizational point of view, the meaning, content and information available to users become relevant.

Identification and authentication are criteria that directly target the user who is to access and obtain information data. The identification of a user is represented by the establishment of his identity, following which the authentication is performed through a series of methods, among which:

- user name - login and password system;
- OTP system (One time Password) - the user receives a password with a limited duration (usually a few minutes) on a special device (token), which can only be used once for authentication;
- digital certificate - usually stored on a medium (USB); can be activated by PIN code;
- biometrics (fingerprint, iris of the eye, etc.).

Confidentiality is represented by the fact that only authorized persons or entities, under certain predetermined conditions, can have access to information characterized by this feature. Confidential information that is disclosed through various means (hacking or even simply human error) can affect the organization.

The permanence of the information system means its preservation over time, through specialized coding in order to provide access to information and to facilitate their quality management. This permanence is achieved through archiving, ensuring 3 important requirements:

- represents a proof of the activities of the organization during its existence, defending its interests.
- creates an information database that includes different situations, analyzes and studies accumulated from the organization's experience, in order to be used in future planning.
- ensures the preservation of intangible information throughout the existence of the organization [5].

6. Data loss prevention

Zero Trust applies the principle of minimum data access privilege. The model is a security concept that requires authentication to perform a particular task for users, before being granted access

to only the necessary data and resources. In order to prevent data leakage, matching risk with trust given to a particular user or device is essential.

Zero Trust requires three fundamental steps, applied at the level of applications and services within the network:

- Verify the user (authentication, step 1);
- Verify the device (authentication, step 2);
- Verify access privileges (authorization).

These three layers of verification are accomplished through a series of compliance checks based on the characteristics of each. These compliance checks can include information ranging from device encryption to user patterns of behavior and can continue to expand as more information about users and devices is collected [6].

The correct user permissions and network segmentation have the same end goals but approach them in different ways. In the event of a breach or direct attack, both help to limit the impact area, with zero trust on a more granular scale. A zero-trust policy helps to develop a robust process for detecting and responding to incidents by reducing the time it takes to detect, probe, and address a data breach.

7. Visibility control and endpoint access

One of the most important cyber security challenges for remote companies is maintaining a comprehensive visibility in a network of various endpoints, while "visibility is the key to defending any valuable asset." [7]

With a secure web gateway (SWG) we can close this gap by applying zero trust policies to secure endpoints using a database to filter incoming and outgoing traffic for individual devices.

A key factor in enforcement of zero trust policies is that visibility must be intelligent and real-time. That is, the user and application identity attributes for different endpoints must be continuously monitored for suspicious or malicious activity. In addition, it is also important to strengthen the functions of the various modern security resources for simplified access control. Here comes a margin of Secure Access Service Edge (SASE). An SASE integrates SD-WAN with cloud security services such as SWG, Cloud Access Security Broker (CASB), and next-generation firewall (NGFW). The result is a more productive security delivery that enable organizations to protect their critical data.

8. Compliance with cyber security policy

The consequence of implementing the policies explained above is to achieve a greater compliance of cybersecurity strategies. With the transformation of the digital cloud between industries, the creation and enforcement of cybersecurity policies is inevitable. In aviation cyber security, for example, there are companies like AFuzion that are leading the industry in the direction of new regulations for flight safety.

A SWG is more than just a URL filtering tool; It is also used to log all security events to enforce a company's cybersecurity policy regarding Internet access. A SWG works by accessing the permission and credentials regarding the URLs and describe a table for granting or denying access. This means that an employee web access is blocked from unwanted content using the organization's network resources. In this way, SWG works like a CASB, with the major difference being that the latter covers a wider range, enforcing security policies and cloud protection beyond the traditional limits of a firewall. CASB or SWG and NGFW integrated, both help the organization deal with the obscure IT challenges.

For effective Zero Trust implementation, monitoring of all network assets is necessary as the days of relying on perimeter-based controls to stay compliant and secure are long gone.

9. Conclusions

On the one hand, business - especially remote companies - is booming with confidence. On the other hand, this idea of "zero trust" seems to threaten the foundation of business operations.

Zero Trust removes all implicit trust and continuously validates every stage of a digital interaction. But Zero Trust does not equate with mistrust. Forrester, who pioneered the term in 2010, insists that it is not a question of tracking everything like a hawk, but of acknowledging that not all data is created equal. Some data or applications need more security and governance than others, and while certain assets need to be watched and controlled closely, others can be left with minimal controls.

The Zero Trust security compensates for the reality that threats could be anywhere, and that the Intranet of your organization is likely no safer than the Internet. Despite the name, Zero Trust means more about trust than just trust.

References

[1] D.S. Reveron, Cyberspace and National Security - threats, opportunities and power in a virtual world, Georgetown University Press, Washington DC, 2018.

[2] R.A. Grimes, Hacking Multifactor Authentication, Wiley, September 2020.

[3] K. Geers, Strategic Cyber Security, NATO Cooperative Cyber Defense Center of Excellence, 2011.

[4] IBM Security, Cost of a Data Breach Report 2021, https://www.ibm.com/downloads/cas/OJDVQGRY.

[5] E. Smit, J. Van Der Hoeven, D. Giaretta, Avoiding a Digital Dark Age for data: why publishers should care about digital preservation, Learned Publishing, Volume 24, Issue 1, Jan 2021.

[6] K. DelBene, M. Medin, R. Murray, The Road to Zero Trust (Security) [White paper], https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF.

[7] Forescout, Total visibility: The Master Key to Zero Trust Security [White paper], https://www.forescout.com/resources/total-visibility-the-master-key-to-zero-trust/.

[8] J. Garbis, J.W. Chapman, Zero Trust Security - An Enterprise Guide, Apress, 2021.

[9] S. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero Trust Architecture, NIST (SP) 800-207, 2020.