SIM Global Education

Cyber Security

Individual Assignment

Apr 2024 Semester

Name: Jeslyn Ho Ka Yan:

ID: 1024 1485

Table of Content

1 Summary

"Cyber threats evolving? Zero Trust adapts!"

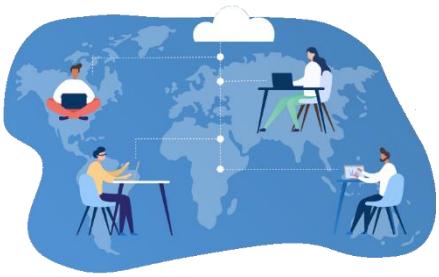
The traditional perimeter security firewall guards the network perimeter but creates an assumption that anyone inside the network can be trusted. However, these firewalls struggle with today's remote work environment.

Zero Trust disrupts this paradigm by embracing the principle of "never trust, always verify." It is a security framework that will rigorously verifies every user and devices before granting access to the application and data. Essentially, Zero Trust equips enterprises with a more resilient and flexible security posture, readying them for the always changing threats.

Zero Trust is a leading security strategy, a recent industry report has reported that about two-thirds of the organizations globally have adopted the zero trust strategies, either fully or partially in their security approach.(CyberSecurity Drive 2024)

Examples of Zero-Trust Use Case:

Remote Workforce Security



Zero Trust eliminates implicit trust within the network and authenticates each and every attempt at access, irrespective of the device or location. This guarantees that, even while working remotely, only authorized people and devices have access to sensitive data.

According to a research, a workforce consisting of over 35,000 individuals became more mobile and remote, especially after the COVID-19 pandemic, prioritizing zero trust. (Zscaler 2021)

Controlling entry to valuable company applications

Zero Trust removes implicit trust, securing high-value applications. Each and every attempt at access is thoroughly verified. Users are granted the least amount of access necessary. By reducing attack surfaces and possible data breaches, this ongoing monitoring protects sensitive data in vital applications.

Cloud Security with Zero Trust:
Microsegmentation divides the complex cloud environments into smaller segments. This keeps attackers from traveling laterally even after they penetrate one section and isolates important assets.

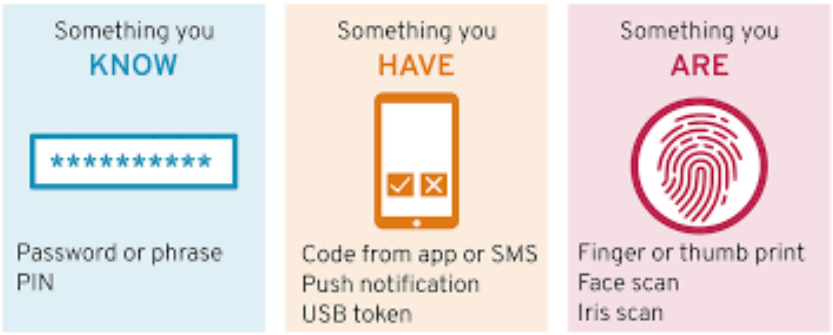
Securing IoT Devices:
Zero Trust authenticates and manages every device access, including unreliable Internet of Things devices. This lessens the possibility that hacked devices may serve as entry points for hackers.

2 How Zero Trust Works

Continuous Authentication and Authorization:

Authentication and authorization are not one-time events. Users will face connections and logins frequently expire, requiring users and devices to be continually confirmed again.

Multi-Factor Authentication (MFA):



Zero Trust extends beyond standard logins using a username and password. Two or more factor authentication is required for MFA. Such as biometric verification, one-time code which will be delivered to a registered mobile number. MFA provides an additional security layer. This substantially reduces the likelihood of unauthorized access, even in the extremely improbable case that hackers manage to get their hands on a password.

Device Posture Checks:

Zero Trust checks the level of security on any device trying to access resources. The check may involve verifying if the device complies with pre-established security configurations, is encrypted, and has the most recent security updates installed. Devices that don't fit these requirements might only be given restricted access or not at all.

Context-Aware Access Control (CAAC):

When assessing access requests, Zero Trust considers a number of contextual criteria. Such as information about a user, device characteristics, location, access time, and the resource's level of sensitivity are all taken into consideration. For example, only authorized devices and particular places may be able to access sensitive data during regular work hours.

Microsegmentation and Least Privilege Access:

Microsegmentation :
A network is microsegmented when it is divided into discrete, tiny pieces, each with its own security policies and access control.This strategy limits an attacker's ability to move laterally within the network, potentially lessening the effect of a breach. Because access constraints are implemented at each microsegment, an attacker who gets access to one segment finds it difficult to move laterally to other segments.

Least Privilege Access:
Users are granted only the minimal amount of access rights necessary to effectively carry out their designated tasks. By doing this, the possible harm from stolen credentials or illegal access is reduced. For example, a marketing staff member may not have access to financial data, only consumer contact information. Reducing access rights reduces the possible harm that might be done by insider threats or compromised credentials.

Continuous Monitoring and Threat Detection:

Session Monitoring:
Zero Trust extends beyond the point of first authentication. Suspicious activity is constantly observed in user activity during authorized sessions. Analyzing user login timings, access trends, and downloaded data may be necessary for this. A deviation from the norm may result in notifications and maybe even account suspension for further review.

Endpoint Security:
Zero Trust makes advantage of endpoint security programmes installed on consumer hardware. These solutions keep an eye out for any unusual activity on the device itself, including viruses and unauthorized programmes. Real-time threat detection and response are made possible by integration with central security platforms, which may help stop breaches before they happen.

3 Benefits that Zero Trust can bring

Enhanced Security Protocols

Zero trust requires verification of all identity and device context for all access attempts, minimizing unauthorized access and lateral movement. In order to provide adaptive security measures, access choices are made depending on policy guidelines and endpoint circumstances. By limiting user access to certain resources, granular access restrictions improve network security as a whole.

Simplified Access Control

Zero Trust implementing tools like Single Sign-On (SSO). SSO allows users to access various applications by using a single set of credentials. It improves the user experience overall and reduces login fatigue. With solutions like SSO, it streamlines management while improving security with granular access and micro-segmentation. Users benefit from easier access, while businesses benefit from a more secure environment.

Enhanced Remote Access Protection

Remote work has become increasingly prevalent in today's world. Traditional security strategies are under threat due to the increase in remote employment. Zero Trust is a good fit for the dispersed workforce of today, as it focuses on confirming user identification and device health regardless of location.

Improve Compliance

Every access request is assessed and recorded by Zero Trust, to ensure continuous compliance by tracking time, location and applications. This simplified audit trail reduces audit efforts, increases governance effectiveness, and has a beneficial effect on the bottom line.According to an IBM study, compared to organizations that don't, businesses that employ security AI and automation save USD 1.76 million. (IBM 2023)

Smaller Breaches' blast radius:

Reducing the effect of a breach is crucial in the event that one happens. By reducing the range of credentials or access points that an attacker may use. Zero trust gives systems and users more time to respond to threats effectively and therefore reducing the possible harm and disturbance brought on by security events.

Improved Threat Identification and Reaction:
Zero Trust lessens the potential harm and disruption brought on by security events by reducing the ways in which attackers might compromise the system. Analytics and ongoing monitoring are a necessary components of Zero Trust. Constant monitoring and investigation of suspicious activity enables quicker reaction times and the reduction of possible risks.

4 My Thoughts on Zero Trust Apporach

I believe that many of us perceive cybersecurity as a sophisticated mechanism operating in the background, discreetly. A relatively recent development in security called "zero trust" illuminates something shockingly familiar: the routine security procedures we all routinely use. Zero Trust feels both inventive and at ease for the following reasons:

Familiar Foundation:
Zero Trust builds upon the principle of "least privilege." This concept applies not only in the digital world but the real world.

For example, I once lent my neighbor a wrench for a particular purpose, but I wouldn't give them access to your whole toolbox.

This is mirrored by Zero Trust, which does not provide users complete system rights but rather gives them temporary access to select tools or apps required for a given project.

Adjusting to a Changing Environment:
Most of our interaction in our daily life consists of using technology, it has become more dynamic over the years. We are able to access our work from any location and time using multiple devices. Since more and more companies provide flexible work arrangements like remote access and bring your own device (BYOD), the danger landscape is always growing. Because Zero Trust verifies continuously, it helps to make remote access safer. It responds and adjusts itself quite well to changing circumstances.

The Reassurance of Zero Trust
With the adoption of Zero Trust, I am able to feel more comfortable and confident in utilizing technology. Similar vulnerabilities exist with passwords in the digital realm. This combination password can be easily guessed, a bad actor could use scanning tools like nessus to find the type of password the user has. However, Zero Trust moves beyond passwords, it adds a layer of security. I can navigate the digital world more comfortably and with more peace of mind thanks to this assurance.

The Accessibility of Zero Trust Principles

Zero Trust builds upon well-known security principals while providing familiar security concepts. This evolution aims to enhance and refine existing practices to meet the demands of today's technology landscape. Because of this familiarity, Zero Trust is a powerful tool that is useful to all users of technology, not just security specialists. I can all take more proactive steps to safeguard our digital assets by implementing the fundamentals of Zero Trust in my daily life.

Total words: 1522

5 References

CyberSecurity Drive (2024) Majority of businesses worldwide are implementing zero trust
Available at:
https://www.cybersecuritydive.com/news/majority-businesses-zero-trust-gartner/713856/
(Access on: 10 May 2024)

Zscaler (2021) Safeguarding the Hybrid Workforce with a Zero Trust Approach
Available at:
https://www.zscaler.com/resources/industry-reports/hybrid-workforce-protection-zero-trust.pdf
(Access on: 10 May 2024)

IBM (2023) Cost of Data Breach Report 2023
Available at:
https://www.ibm.com/reports/data-breach
(Access on: 10 May 2024)