Zero Trust

Kerby Guillaume

CYSE 425W

5.31.2026

Zero Trust Architecture. Zero Trust Architecture, also known as ZTA, is one of the most effective policies implemented in cybersecurity practices. The base of this architecture is surrounded by zero day attacks which are critical and can seriously harm an organization's systems as well as lead to data leakage. With that being said, in order to fully understand Zero Trust Architecture, we must understand zero day attacks. Zero day attacks are cyber attacks performed by attackers that occur suddenly with no warning, giving stakeholders no time to prepare or mitigate that attack. "Zero" time to prepare. Due to how sudden the attacks are, systems can be exploited quickly.

I particularly chose this policy because I believe zero trust is a core cybersecurity policy that all cybersecurity analysts must be familiar with (similar to policies/frameworks such as the CIA triad or AAA for example). The motto for ZTA is simple: "never trust, always verify." (Paloalto Networks, 2019). As this is quite self explanatory, implementation of this within day to day systems could get a little complex.

Zero Trust Architecture is applied by requiring every user, device, and application to be verified before they are allowed access to company resources. Instead of automatically trusting someone because they are connected to the organization's network, Zero Trust follows the

principle of never trust, always verify. This means organizations use tools like multi-factor authentication (MFA), constant monitoring, and least privilege access to make sure users only have access to the data and systems they need. For example, if an employee logs in from a new device or location, the system may require additional verification before granting access. By continuously checking identities, Zero Trust helps reduce the risk of cyberattacks in addition to preventing attackers from moving freely through a network if a breach occurs (Paloalto Networks, 2019).

To add on, the ZTA plays an important role in both national and international cybersecurity policies as many countries are working to improve the protection of critical services. By focusing on identity verification, Zero Trust Architecture helps organizations build stronger defenses against cybercriminals and nation state attacks. As cyber threats continue to cross international borders, the adoption of Zero Trust contributes to a more secure global cybersecurity environment (Lindemulder & Kosinski, 2024).

References

Lindemulder, G., & Kosinski, M. (2024, June 20). Zero Trust. Ibm.com.

https://www.ibm.com/think/topics/zero-trust#1268897088

Palo Alto Networks. (2019). What is a zero trust architecture? Paloaltonetworks.com.

https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture