Alyana Barrera

Professor Saunders

CEG 3400-01

22 March 2021

DF #3 – Zero Trust Architectures

1. I learned from “paloaltonetworks.com”, that Zero Trust Architectures “is a strategic initiative that helps prevent successful data breaches by eliminating the concept of trust from an organization’s network architecture. Rooted in the principle of ‘never trust, always verify’” (2). These architectures “leans heavily on components and capabilities for identity management, asset management, application authentication, network segmentation, and threat intelligence” and provides cybersecurity without the expense of user experience (1). Everything must be verified when working with a zero-trust architecture.
2. Cisco is an example of a company that has successfully implemented Zero Trust. In the link I have found they are expressing how useful it is for users of Cisco. They use it to provide a “comprehensive approach to securing all access across your applications and environment, from any user, device and location” by “establishing trust”, “enforcing trust-based access”, and “verifying trust continuously” (3).
3. I found that challenges include the effect in user experience (4), security concerns like “compromise of the zero-trust control plane” (4) and increase in management in users and devices (5). I have found more challenges, but I believe for the most part that I saw the ones I have listed as a reoccurring trend.
4. Trusted Systems might impact Zero Trust Architecture implementations negatively because there would have to be a multitude of changes and adding layers to the trusted system which can be costly and a big change. Implementing Trusted systems may impact Zero Trust Architecture positively because you would know what occurs in system so it may help implementation by knowing a general understanding of its “protect surface”.
5. From my understanding of the articles I have read, you need a trusted system with the information that you are wanting to protect to build a Zero Trust Architecture around. An article from “paloaltonetworks.com” explained that you can deploy zero trust by “identifying the protect surface”, “map the transaction flows”, “build a zero-trust architecture”, “create a zero-trust policy”, and ‘monitor and maintain” (2).

Works Cited

1. <https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture>
2. <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>
3. <https://www.cisco.com/c/en/us/products/security/zero-trust.html>
4. <https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/zta-project-description-final.pdf>
5. <https://www.infusedinnovations.com/blog/secure-intelligent-workplace/pros-and-cons-of-the-zero-trust-model>