Alyana Barrera

Professor Saunders

CEG 3400-01

25 January 2021

DF #3: Lessons Learned

In this discussion, I learned about Google’s Zero Trust Architecture, the idea of micro-segmentation within ZTAs, and that a ZTA doesn’t require a trusted system. For my first learned lesson, I newly learned that Google has their own ZTA called BeyondCorp. I wasn’t able to find this information within by own research but through this discussion I learned that they did have a ZTA which was an interesting fact. For my second learned lesson, I learned about micro-segmentation where “a ZTA allows for data and services to be split up and organized very specifically on a ‘need to know’ basis” (Ryan Miller from DF). This was new to me because I didn’t realize that ZTAs can be sectioned rather than implemented completely. For my third learned lesson, I have learned that a ZTA doesn’t require a trusted system. At first, I believed that there had to be a trusted system in order for a ZTA to be created around the information, but I learned that it doesn’t require a trusted system and can be built without it. This thought made sense to me because I know that it is very hard for some companies to implement when they have already working systems, so building one from the ground up prior may be easier to implement.

The answers we came to during our discussion are:

1. Zero Trust Architecture is an architecture based on the principal that nothing can be trusted. Under this philosophy, no device, user or application attempting to interact with your architecture can be considered to be secure.
2. We found that Google as an example of a company that has successfully implemented a ZTA.
3. 3 common challenges associated with implementing a ZTA: 1) policies and permissions would have to be created for all the devices that would be on the ZTA (which is very time consuming and costly). 2) ZTAs need consistent and lasting administration over roles, privileges, etc. 3) there are lapses in security when replacing older systems and room for threat.
4. One positive advantage trusted systems can have on a ZTA is it would be an easy access for those who are working under it (employees or IT management) to help enforce the policies and allow employees to continue to be productive without significant impedance. A negative impact would be that someone would have to check the trustworthiness of the system regularly because there is still a chance another can get access to the trusted system and then the ZTA.
5. A company does not need to have a trusted system in order to implement a successful ZTA.