Larry Arndt

CS-405

January 11, 2023

Journal: Defense in Depth

Defense in depth is creating several layers of defense to guard against attacks to your data computer system network. It can involve several aspects such as physical, technical, administrative controls. These work together as a defensive shield, but each has a cost and begs the question how deep is too deep. This question is going to be unique to each organization. Why, because the of the next question: what is the tradeoff? What type of data are you protecting how sensitive is it? How much is your budget? What is your timeline? What are your system requirements? These are some of the questions that will factor into how deep is too deep for your solution. If you can’t afford it, it is impractical, or stalls your system performance below your limit thresholds you are going to deep.

The higher level of your defense in depth the more reputation your company will most likely have, security breeches will lower your company reputation. Security costs money and time. Building a secure site can take a short time or years depending on what you are doing. Building the pentagon or installing a metal detector and some security cameras for your building that you rent out. Likewise, the costs are that much different, do you have a security system with no guard on duty, or a whole security force armed to defend. The equipment itself, is it just a few servers hooked together in your basement or are you running ten server rooms with a thousand servers per room all encrypted, and behind a state-of-the-art firewall, with biometric scanning for access. These are just some of the considerations.

Each situation is unique, and you can become dependent on certain personnel, it is good to always have a person in reserve that can handle the system if the main person with access goes down or is missing, but at the same time this means greater access to more people, which is a greater liability. Hiring practices are key and getting the right people and how they authenticate on the system is key as well. Today, two-factor is often implemented, perhaps with a biometric component. People can lose their authentication devices which can become a liability, or if you do not do proper background checks and other hiring practices your employees themselves can become a liability.

Data handling procedures, software security, and confidentiality policies will all differ from organization to organization but must be robust enough to meet the needs of that entity. Non-Disclosure clauses for employees working at high-end technology companies are standardized, security clearances are used in the government for sensitive information, but a small business with a few employees might not even bother with any of that type of information protection. Who as access to what level of information, and system commands should be restricted to the principle of least privilege in all situations but depending on the technical level of the employees its implementation may be mishandled; passwords and usernames must be protected regardless of the organization type.

References

Petcu, Alina. “Everything You Need to Know about Defense in Depth Layers.” *Heimdal Security Blog*, 29 Jan. 2021, heimdalsecurity.com/blog/defense-in-depth-layers/. Accessed 11 Jan. 2023.