Priscilla Gomes-DaCosta

Southern New Hampshire University

CS-405-T2852 Secure Coding

11/6/2022

Defense in depth is a security concept that applies to physical and online security, where a hardened “core” is guarded by different layers of protection. The costs of Defense in Depth include protecting wider areas from layer to layer against less specific threats. Another flaw includes the difficulty of implementing basic tenets of security: confidentiality, integrity, and availability, with increased defense confidentiality is increased, integrity is more difficult to implement, manage, and makes availability harder to be provided. (Silverstone & CISSP, n.d.) Building and maintaining physical, technical, and administrative layers can take a long time and get expensive while not guarantying protection against attacks. Physical layers can include anything that physically limits access to a certain area, technical layers can be hardware or software tools with the purpose of protecting systems and resources, while administrative layers include controlling policies and procedures for an organization.

Depending on the situation, the system can grow in complexity, increasing the possibility of additional issues being created. The combination of different tools integrating together in combination of physical devices that may also be in place poses challenging troubleshooting procedures when an issue arises. Besides the considerations needed to implement all of the layers of protection, is important to remember these systems will need to be upkept, by knowledgeable staff while still being able to provide end users/customers the services they expect.

References

*Defense in depth (computing)*. (2022, August 14). Wikipedia, the free encyclopedia.

Retrieved November 5, 2022, from https://en.wikipedia.org/wiki/Defense\_in\_depth\_(computing)

Silverstone, A., & CISSP. (n.d.). *Where defense in depth falls short*. CSO

Online. https://www.csoonline.com/article/2124452/where-defense-in-depth-falls short.html