Designing a Secure Network

Easton Jarboe

ODU

CYSE 300

Dr. Kovacic

1/28/24

When the security of a data center is involved many things must be considered. Most of all access control, data encryption, security audits and monitoring, incident response, and the most important employees training. The first thing that should be done is making sure the server is secure.

This can be done via setting up a DMZ or demilitarized zone; this involves setting up a firewall as a sort of defense and putting the server on the inside. This can help prevent potential threats (Cherry, 2015). This combined with using a public IP address outside of the DMZ and a private inside will help with the overall security of the network. Firewalls work well with the built-in security features of a server. One thing many people neglect is leaving open communication ports that are unused turning those off would allow access only through permitted ports and lessen the attack vector.

Navigating the internals of the server is very important, but making sure the server is physically secure is also a huge part of security. Using a mantrap where someone has to go through two doors ino order to enter via their key card will make sure the least privilege is applied and only authorized persons can get through the door to access the server. Along with this a two factor security measure such as a code sent the the authorized persons phone would mitigate people tailgating and having a chance to access the server. Audits of the security features should be regularly taken. Audits can pinpoint the weaknesses in the physical and virtual security. This can “patch up the walls” leading to a stronger overall defense. The best form of finding vulnerabilities would be a penetration tester. Hiring a professional individual to act as a criminal and break in using vulnerabilities would give a good edge to the security of the building and server.

If the time arises where a person breaks in security alertness and incident response are paramount in mitigation of damages. Intrusion detection and prevention systems would be the best to layer behind the firewall before the attacker can reach the server allowing for a faster response time. Then the damage can be mitigated and the employees can repair the damages and lessen the time to having the server online. By far the weakest link in the cyber security chain is people. In order to stop this there should be education sessions for the employees. This can lead to a lesser chance for social engineering to work and allow hackers access to the building or internal network.

Overall servers are very complicated devices and they need to be handled with extra care when it comes to security. Having a DMZ allows for a public and private network therefore strengthening security. Adding a mantrap helps with physical security and keeping out unwanted individuals. Security audits and security testing allows for the vulnerabilities to be exposed and in exposing them can make the server stronger after patching the problems. Adding intrusion detection allows for the server to be monitored and reduces the time between an attack and when someone would be alerted. The employees should all be trained to handle threats and understand how they could be exploited. In doing all this a server would be very hard to break into and would be overall more secure.

References

Cherry, D. (2015). ***Securing SQL Server: protecting your database from attackers*****. Syngress.**