Security policy: for protecting on-site data servers

Dae'lyn Bellamy

Department of cybersecurity

CYSE 300

Dr. Joseph Kovacic

9/8/2024

Today, we will formulate a security policy for protecting on-site web, application, and data servers. I will be going over five important issues that must be addressed to ensure the protection of an organization's physical servers and hardware. The five important security measures that must be implemented that I will be covering is access control, hardware security, surveillance systems, and lastly backing up your server data.

The first thing that must be done in order to ensure the protection of your servers and hardware is to manage who can access your servers. This can be done in a few ways, one of them being establishing physical barriers around your building such as fences to make it harder for nonemployees to access the premises. Another thing that should be done is to restrict access to the server room using ID cards or any other type of authentication device to ensure that only authorized personnel are able to enter the server room (Anant et al., 2024). This means that even if someone managed to sneak into the building they would still need an ID card to get inside, you could also extend this to the entire building itself so that only employees can enter making it even harder for non-employees to sneak their way into the building. Now another thing that should be implemented is surveillance systems.

Installing cameras in and around your building will also help secure your systems by allowing you to monitor the activity inside and outside of your building. Cameras themselves may not do anything on their own to stop or deter intruders, but it does allow you to have situational awareness in and around your organization. The cameras can also be used to monitor activity inside the server room to make sure that nothing is being done that isn't allowed, such as plugging in USB and such. surveillance systems will also allow one to identify anyone who is doing illegal or suspicious activities which can then be sent to the police for further investigation.

Another thing that should be done is to implement hardware security protect your systems from physical damage and tampering if someone was able to gain access to the server room or any other technology systems. One thing that should be done is to use a rack enclosure which is used in case your servers as well as any other sensitive equipment(Anant et al., 2024). Another thing that should be done is to remove or seal USB ports of office computers and as well as any unnecessary ports in the server room

to eliminate or limit the possibility of someone planting a malicious USB stick into one of your computers causing a breach. Locking cables are also an important thing that should be done to make sure no one can remove or disconnect your cables from your servers (Anant et al., 2024).

Now the last important issue that needs to be addressed in this security policy is server backups, if anything were to go wrong within your server room or if someone is able to delete your data you will need a way to recover most if not all of your data. There are different types of backup methods such as full and incremental backups(Crape, 2024). You should look to implementing these backup methods to have a full range of data recovery. Full backups take a long time and are expensive so they're usually done infrequently whereas incremental backups are faster and may be done once every month, this means that newer data can be backed up faster and without having to back up your entire server every time it's done saving you time and storage. Overall implementing a backup schedule will increase your survivability in the event of a diaster occuring.

In summary, today we looked at five important issues that need to be addressed when trying to protect your on-site systems and servers. We looked at things that can be done to limit access to your organization building such as fences and ID cards, we also discussed the importance of surveillance systems to monitor and record activity in and around the premises to ensure there is no suspicious activity going on whether that be outside, inside, or inside the server room itself. We also looked at ways to protect system hardware such as in casing your servers in other sensitive equipment inside of rack enclosures as well as removing or disabling the USB ports on your computers and any other hardware that may have them. Lastly, we discussed the importance of implementing a backup schedule to ensure that any lost data can be recovered.

SOURCES

Anant, D., Akbari, S., & Güzel, O. (2024, February 24). ***What are the best ways to ensure the physical security of your server?*****. How to Ensure the Physical Security of Your Server.** **https://www.linkedin.com/advice/3/what-best-ways-ensure-physical-security-vu47c#:~:text=To%20ensure%20server%20physical%20security%2C%20start%20with,and%20have%20a%20comprehensive%20disaster%20recovery%20plan.**

Crape, M. (2024, January 11). ***Guide to server backups: Creating a backup strategy: VEEAM*****. Veeam Software Official Blog. https://www.veeam.com/blog/server-backup-guide.html**