Security Program Implementation Plan

Tyler Higgins[1]

[1] University of Advancing Technology

Author Note

This paper was prepared for NTS201 - Security Essentials, taught by Mason Galatas.

Abstract

The purpose of this paper is to go over the layers of security needed to protect a data center. We will cover physical security, like traffic flow, for both cars and people, security guards, cameras and physical barriers. We will also go over access control for the building, and the different layers inside the building, like accessing the data center flow. Next we will cover the security of the equipment in the data center. We will go over the server configurations, backups for the servers, and the security setting on the servers. When setting up a new building, especially a data center, all aspects of security need to be looked at, physical and digital security.

Security Program Implementation Plan

Physical Security

The physical security of any building is very important, especially at a data center. The external physical security of a building is perhaps the some of the most important as it acts as the first line of defense against a physical attack, and physical reconnaissance.

External Physical Security

Lights. When it comes to physical security darkness is our weakness. That is why at 6 foot intervals high powered LED lights should be placed around the fence, inside the fence line. By placing the lights inside the fence line we can protect the lights from tampering. It would also be wise to use a thicker material like Lexan as a glass to protect the lights from being shot out with a low powered silent weapon.

External Fence. When it comes to an attack, once of the first things an attacker is looking for is how easy it will be to hit the target. If there is a high barrier around the perimeter of the property that can stop quite a few attacks as the breach will not be easy; that is why the first line of defense around the property should be a 6-8 foot high fence. This fence should should have razor wire around the top to deter someone from trying to clime over it. This fence should completely enclose the campus property with the only opening being the entrance into the campus. For food traffic, a standard door can be placed to allow those that are not driving to enter the campus without being put in danger.

External Physical Barrier. At the vehicle entrance to the campus multiple automatic retractable traffic bollards should be placed in front of the main gate. These can be used to stop a car from breaching the main gate in the event a threat is detected. There should also be a set of non-retractable bollards placed around the foot traffic entrance to prevent cars from smashing through that weaker point in the fence.

Security Guards. Security guards play a large role when it comes to physical security. Guards can patrol around the campus, monitor security camera's, check in visitors at the gate and at the main building. As well as patrol inside the building. At anytime there should be at least two security guards at the main gate, this will allow one guard to remain in the guard house monitoring the security camera's and watching for other threats while the second guard checks the ID's of the drivers and passengers of the vehicle's trying to gain access onto the campus.

External Security Camera's. While security guards are a great tool to have, it would take an army to properly protect any building from every threat. That is why security camera's should also be deployed around the perimeter. I would recommend two security camera's be placed at each corner of the perimeter fence, one pointing in each direction with a slight overlap in the middle, along with camera's being placed at even interval's along the fence line, approximately every 10-12 feet. These security camera's should be pan-tilt-zoom (PTZ) camera's and high a high definition. This will allow for the greatest protection.

External Access Control. Employees will be required to scan a badge before entering the perimeter of the campus, if they are driving into work they will have to scan their ID badge with the guard. The badge will pull of a limited employee file, including name, employee picture, and day and time of allowed campus access. While limiting days and time of campus access may not seam that important, it can be. As an example, if a badge is copied for a receptionist, and that receptionist does not need to be on campus on a Saturday it would be smart to put that in the access system. If this employee ID is scanned on a day they don't need to be on campus and it was not setup beforehand this could be a red flag for security. The same access control will be used for the foot traffic entrance, with the included security feature of a man-trap. The way a man-trap works is by having two doors to pass through, but only one door can open at a time and there is only enough space for one person in between the doors. This will prevent piggybacking and

adds a second layer of security, at this entrance I would recommend placing a bio-metric scanner, like a retina scanner along with an ID badge scanner to verify the correct person is gaining access. Any visitors that have been granted access to the campus will also be issued a visitors badge that must be scanned to gain entrance to the main building. This visitors badge will be programmed with the level of access the visitor needs; it will also be set up in the system to expire at a specific time, either at a planned time for the end of the visit, or at the end of the business day depending on why the individual is on the campus.

External Facing Building Doors. All doors except for the main lobby entrance will be exit only and alarmed. For maximum security the only door that will be usable to enter the data center building will be that one with access to the lobby.

Internal Physical Security

Now that we have covered the external physical security let us go over the physical security inside the data center.

Lobby Entrance. While having a wide open lobby may seam like a nice feature, and it may feel more inviting, it is not safe. Even though the people that have made it to the lobby entrance have been check by security, there is always a way security can be bypassed. That is why the lobby entrance should also be a man-trap. However, since visitors are not fully in the access control system, it is recommend that the access control on both sides of the man-trap be ID badge readers. This may seam redundant, but the protection of our customers data is at our top priority.

Lobby. Once inside the lobby there will be only two options for accessing the rest of the building. Either through another man-trap into the data center, that will require retina scanning along with an ID badge. Or access to the office space for all employees. This will provide only a singe entrance point for all data center access. A security guard will always be stationed in the lobby.

Internal Security Camera's. Security camera's will provide the security guards an extra set of eyes. All security guards will have access to the external security camera feeds, but the guards in the security office will also have access to all the camera's inside the main building. Camera's will be placed so there is no blind spot, every door will have a camera placed at it on at least one side. The only space that will not have any security camera's will be the data center floor itself, as this is a highly protected area. Just like the external security camera's, the internal camera's will be PTZ and high definition.

Internal Security Guards. Security guards will be required to patrol the building hourly, this will included an external walk around of the building checking to make sure all external facing doors are secured. It will also be expected of all security guards to check the ID badges of anyone they do not recognize, this will be accomplished with the use of a tablet that is tied into the access control system. This is done to insure someone has not been passed, or stolen, a different ID badge to gain entrance into a section they are not authorized to access.

Digital Security

Now that our physical security has been taken care of, let us move on to the digital security. In this section we will cover server configurations, backups, and redundancy.

Server Configurations

Accounts. All accounts, both on the servers and workstations, will be setup with the least amount of permissions they need. This means, if an account does not need administrative privileges, it will not have them. This also means all IT staff will use a standard user account for day to day activity and only use an administrative level account when absolutely needed. This will prevent an attacker from easily gaining administrative access to the network.

Passwords. All passwords for servers and services on the servers will follow complexity guidelines, meaning they must all be at least twelve characters long, have at least one number, one upper case, and one special character included. It will also be required that all passwords be changed at least once every ninety days. While this may seam drastic, it will prevent an attacker from observing what a password is and easily remembering what that password was. The password rotation will also prevent stale passwords from being used.

Backups. One of the most important processes we could deploy at the data center is the proper use of backups. When it comes to backing up the data at our data center, we will follow the 3-2-1 rule for data backup. This 3-2-1 rule states we must have at least three copies of our data. Two copies should be kept on two different types of media, in our case a backup server and tape storage. Finally at least one copy of the backup needs to be kept off site. One of the most important things to keep in mind is that backups do not just help in the recovery after a disaster, proper backups can also help in the recovery after a ransomware attack. It is important to remember, it is not if we will get attacked, it is when will be get attacked. It is for that reason the 3-2-1 backup method will be strictly followed at the data center.

Backup Power. To make sure the data center does not go offline in the event of a power failure, the data center will not only have its own power substation, it will also have multiple heavy duty power generators and a large supply of backup batteries to run the equipment in the data center. Solar panels will also be placed on the roof of the data center to charge to batteries as a way to help the planet go green. The data center should have enough backup power to last at least a week without city power, this will be another reason for solar panels on the roof of the building.

Redundancy. To make sure our systems are always online every critical system, database servers, web servers, access control servers, and anything else that need to never go down will have at a minimum two servers running in a cluster, if the two servers are

virtual, each virtual server must be hosted on a separate physical host. This will allow for the greatest up time. The web servers will all be part of a network load balanced cluster to allow traffic to easily flow.

Conclusion

When it comes to security at a date center, all aspects must be taken into consideration, physical and digital security. That is why I have put this comprehensive security plan together. When it comes to security the best defense is a good offense and the best offense is defense in depth.

References

Baker, T. (2018, October 31). The 3-2-1 Rule for Cloud Backup. Retrieved October 12, 2020, from https://www.keepitsafe.com/blog/post/3-2-1-rule-for-cloud-backup/

R (Version 4.0.2; R Core Team, 2020) and the R-package *papaja* (Version 0.1.0.9997; Aust & Barth, 2020)

Aust, F., & Barth, M. (2020). *papaja: Create APA manuscripts with R Markdown*. Retrieved from https://github.com/crsh/papaja

R Core Team. (2020). *R: A language and environment for statistical computing*. Vienna, Austria: R Foundation for Statistical Computing. Retrieved from https://www.R-project.org/