Running Head: SECURING THE DATA CENTER

Securing the Data Center: Physical, Digital, and a Culture of Security

Jered McClure

Walden University

Securing the Data Center: Physical, Digital, and a Culture of Security

PPI’s data center is quite effectively, the heart and brains of the organization. If it is compromised or maliciously attacked, the effects will reverberate throughout the entire company. As such, the security and wellbeing of all data and equipment therein must remain a top priority. With this in mind, PPI should focus their attention on three specific areas of concern: Physical access restrictions, digital access restrictions, and developing a culture of security.

The primary form of physical access restriction takes the form of RFID key cards which employees must use to gain access to the data center. PPI also need to make sure that access to the server room is via an “airlock.” That is, the data center is behind two distinctly separated closed doors which both require key card access whereby one cannot open if the other is not closed. CCTV should also be considered so as to monitor the coming and going of all data center personnel (clear signage should be posted so employees know they are being filmed).

RFID Key cards control access through security permissions in the same way that a directory controller can control network user security rights. Only those staff in the correct group can access the data center, and only during times specified in the key card system. This enables PPI to track the coming and going of staff in the data center through key card logs, as well as, ensure room access to only those staff with a valid reason to be there. The cost of such a system is relatively cheap these days, but the security assurances they provide greatly outweigh any capital losses.

The dual door entrance and the CCTV both have the same reasoning as the RFID card. The dual lock system ensures that people cannot sneak into the room. It also serves the purpose of guaranteeing that if one lock fails, the other is a backup. The primary concern with CCTV is with employee privacy, this should be addressed in the employee policy as well as the organization’s security policy.

Key cards, “airlocks,” and CCTV all protect against physical intrusion and malicious attacks. However, they do not protect against attacks sent through viruses or black hat hackers. These types of attacks must be treated separately. Although, with the same force and aptitude as what has been done with physical security.

Digital access restrictions must ensure the confidentiality, integrity, and availability of all data in the data center. These take the form of user access rights (user names and passwords), firewalls (physical and digital), and virus scanners (Trojans, worms, spyware, etc.). All of should already make up PPI’s network, but must be reconsidered from a data center perspective.

User access rights for data center systems must keep in mind that virtualization means multiple application sessions and core systems operate off of shared hardware. As such, systems should remain transparent to users with their being able to gain access to shared resources which their user rights do not allow. This can be done through a three-fold method of: directory rights management, application rights management, and system’s rights management.

Directory rights management is the controlling of user access to the network itself and what files and directories are available to them. Applications rights management is the individual security permissions granted for each application subclass (e.g. email rights and core applications rights). System’s rights management is security permissions pertaining to specific schemas and protocols (e.g. access to specific servers, database schemas, or system tables).

Firewalls, as stated, take the form of physical and digital. Physical firewalls exist between the gateway/switch and the servers they protect. They effectively segregate external and internal data so that only authorized connections can access PPI’s systems. All physical firewalls should exist in a redundant array so that if one firewall goes offline, another can take its place.

Digital firewalls are the applications installed on each data center server and each of PPI’s workstations. These firewalls block out any intrusions which may not have been stopped by the physical firewalls, or which are not specifically monitored by the physical firewalls (e.g. vLAN segregation which allows only certain users can access specific servers).

Virus scanners should be installed on any workstation and any server in the data center and should run on a scheduled scan once a night. The scanners should be robust and updates should be controlled from a central server and updated as soon as new definitions become available. Virus scanners are, in essence, the last line of digital defense.

Digital access protection comes with licensing costs for firewalls and virus scanners, all of which are, once again, outweighed by the governance afforeded through data security assurance. That being said, digital access does not cover what users themselves are capable of doing to PPI’s data. That is, no form of protection can keep a trusted user from damaging the network from the inside.

PPI should build a culture of security around data center access and PPI systems security. Training and development should be done for all new employees to PPI explaining to them the how, why, and what of security. That is, why data must be protected, how it affects the organization and what they can do to keep breeches from occurring.

Customer data and PPI proprietary knowledge exists in the data center. Having the confidentiality or integrity of this data violated means that customers are likely to move to a competitor, or that PPI be the brunt of litigation from disgruntled stock holders. Data security ensures corporate governance. Staff can ensure this by keeping their passwords secure, locking any system they access before leaving it, and following the organization’s security policy.

The cost of training is subjective, and remains in-house. As such, this should never be overlooked. In essence, a staff culture of security consciousness is worth all the key card locks and physical restrictions combined.

Reference

Alger, D. (2005). *Build the Best Data Center Facility for Your Business.* Indianapolis: Cisco Press.

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases.* John Wiley & Sons, Inc.