ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 2, pp: (43-45), Month: April - June 2021, Available at: www.researchpublish.com

Cybersecurity: Proactive Prevention and Controls

Rawabi Mohammed Alshobrami

Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **With the growth of interconnected technologies and services, the use of computers and the internet become an essential part of our lives to accomplish tasks either at home or in business. Recently, cybercrime becomes a real threat for organizations which might lead to disrupt services or destroy business. Therefore, the current protection and controls of cybersecurity require regular assessment and update to achieve a high level of protection for organizations. This research paper defines what to secure and how to secure for IT environment including physical, hardware, software, and network. Also, it presents the approach of security measures from reactive to proactive.**

Keywords: **Cybersecurity, Prevention, Cybercrime, Countermeasures, Threat.**

I. INTRODUCTION

Cybersecurity becomes a vital concern to organizations especially with the rapid evolution of the internet. Cybersecurity is the protection of information and information resources from unauthorized access, attack, and theft. These resources include physical, hardware, software, and network. The main goals of implementing the security are prevention which is preventing the gain of unauthorized access to the resources, detection occurs when discovering someone who is trying to access the resources without authorization, and recovery which is to return back to the normal operations after compromising or damaging the resources. Now, to build strong security controls, and prevent occurrence of cybercrimes, the CIA triad has to be in-place. CIA triad consists of "Confidentiality", "Integrity" and "Availability". Confidentiality assures that confidential information is not disclosed to unauthorized users, Integrity means that the information is stored and transferred as intended without any unauthorized modification, and Availability refers to the information available to authorized individuals. In this research paper, proactive security measures and prevention controls are addressed in order to attain a high level of cybersecurity.

II. WHAT TO SECURE AND HOW TO SECURE

A. Physical Security

Physical Security is the first step to protect information, property, and facilities from unauthorized access, theft, and damage. Based on the sensitivity of these assets, various measures and layers have to be in place to ensure appropriate protection is achieved. Each place that hosts information is a target by attackers, hence it has to be well defined, evaluated, classified, and protected. This place includes DataCenter, storage, network, backup, electrical, mechanical, and security rooms. The following security controls are required in physical security:

- Install a very strong fence surround the datacenter and provide enough lighting to have clear visibility for security guards.
- Install CCTV surveillance to monitor the site and detect any threat proactively.
- Mantrap and security gate to control the physical access of employees and visitors.
- Segregate the physical access of rooms based on their criticality since a server room is different than an electrical room.

- Enable biometric authentication to access the needed area. The biometric authentication can be implemented using fingerprint, retina and voice recognition.
- Install sensors to detect any physical threat including safety hazards.
- Utilize a reliable security system to control the physical access. This system has to run on a different network to mitigate any network risk.
- Conduct regular backup, reviews, and audits to ensure physical security compliance.

B. Software Security

Software Security is the process of assessing, mitigating, and protecting software systems from vulnerabilities. These processes are required to prevent attacks and assure that the software continues to operate safely. There are two types of software: Operation System and application, and each type of them needs a specific methodology to implement security controls. The following security controls are mandatory to secure OS:

- Operating System Hardening: more security controls can be implemented to achieve a high level of OS protection. It includes installing and patching the OS, installing and configuring Antivirus, firewalls, and intrusion detection system.
- Authentication: implementing the appropriate authentication enables the authorized users to access the needed resources in the system legally. This authentication can be implemented via different techniques including username and password, biometric authentication, and multifactor authentication.

After installing the operating system, the other application software has to be installed and patched to the most recent versions. The following security measures are desired for application security:

- Redundancy: to keep the needed software/service available to intended users.
- Digital Signature: to validate the authenticity and integrity of a message.
- Encryption: to convert plaintext the ciphertext to ensure data confidentiality.
- Auditing: to be conducted regularly in order to assess and prevent any vulnerabilities.

C. Network Security

Network Security is the protection of network resources from unauthorized individuals access, interruptions, and attacks. The network resources include routers, switches, firewalls, cables and connections. In the fact, threats of network security are not limited to physical theft. It also can damage network/computer resources. Network threat is divided into the following categories:

- Unstructured Threat: occurs by a person who doesn't have enough experience to attack. He/she use hacking tools and basic scripts.
- Structured Threat: carries by very well experienced attackers by utilizing advanced tools and techniques to launch network attacks.
- Internal Threat: occurs by an employee who has authority to access network resources and leak data to external parties.
- Physical Threat: can happen due to natural such as earth quick or storms. Also, it might occur when there is a power or cooling interruptions.

Network security measures can be diverse based on the network design of the organization. However, there are multiple security measures recommended to be in place. Here are some of them:

- Firewalls: utilizing an appropriate firewall to control the incoming traffic to the network. The firewall can be either an appliance to be hosted in the datacenter or software to be installed and configured.
- Virtual LAN: implementing VLANs help manage network segmentation.
- Load Balancing: using load balancers to distribute the load of network traffic, besides preventing denial of service attack.

- Monitoring Tools: installing intelligent network monitoring tools to monitor and observe network traffic and devices state.
- Demilitarized Zone: DMZ is an important security measure. It enables external clients to access data on private systems, such as web servers without compromising any other system in the internal network.
- Packet Filtering: it is a technique operated by the router that use a set of ACL (Access Control List) to control the traffic by either allowing or denying it through the router.

III. CONCLUSION

This paper aimed to define the cybersecurity and its goals to satisfy individuals and organizations since the cybercrime became a real threat particularly with the rapid evolution of internet. The cybercrimes intends to disrupt services and destroy business, hence it enforces organizations to face challenges to operate within an expected level. Protecting the information and information resources require huge efforts, tools and cost. Not only these factors, but the way of selecting and implementing the security controls are very important. In fact, companies are required to identify the resources they own, evaluating them against their confidentiality, integrity and availability, classifying them based on their sensitivity. After that, implement the appropriate security controls to safeguard the resources. Continuous monitoring and maintenance is an important key to sustain protected. Another crucial factor is to regularly review and audit existing controls to ensure full compliance of cybersecurity. Finally, organizations have to bear in mind that users' awareness of cybersecurity is the first defence line of their resources, and they have to provide mandatory courses to raise their knowledge and demonstrate positive behave in terms of cybersecurity.

REFERENCES

[1] Smith and Marchesini, The Craft of System Security (2007, Addison-Wesley).

[2] William Stallings, "Cryptography and Network Security": Principles and Practice, 7th Edition, Prentice Hall, 2013.

[3] Joseph M. Kizza, "Guide to Network Security", 3rd Edition, Springer.

[4] Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", Air Force Academy, Colorado, USA.

[5] Microsoft. "Fundamentals of Network Security". https://www.microsoft.com

[6] Erdal Ozkaya (2019), "Cybersecurity: The Beginner's Guide", Packt. https://www.packtpub.com/

[7] Mark Dowd, John McDonald, Justin Schuh, "The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities" (2007, Addison-Wesley).

[8] Kaufman, Perlman and Speciner, "Network Security: Private Communications in a Public World", second edition (2003, Prentice Hall).

[9] Behrouz A. Forouzan, "Data Communication & Networking", 5th edition, McGrow-Hill.

[10] David Hutter, "Physical Security and Why It Is Important", 2016, SANS Institute.

[11] Microsoft (2018) "Microsoft Cybersecurity Defense Operations Center". https://www.microsoft.com.

[12] McGraw, Cigital, Inc (2004), "Software Security". www.ieee.org.

[13] Stefan Thelberg, (2021), "Why Security Monitoring", https://www.holmsecurity.com.

[14] "2020 Cyberthreat Defense Report". CyberEdge Group, https://cyber-edge.com/resources/2020-cyberthreat-defense-report-portfolio/