Cyber Security Plan

CYBERSECURITY BACKGROUND SUMMARY

Introduction

Most companies review their security models and approach to protect the confidentiality, integrity and availability of their data and networks. The rising rate of cyber-attacks and existing vulnerabilities (Clement, 2019) mean that organizations should implement systems that detect and diagnose any threats. This project is an evaluation of existing security models and their features. It attempts to recommend a custom security strategy and plan based on the findings obtained from the evaluation of existing security models. Of special interest for this analysis is to evaluate the pros and cons of implementing specific security model attributes, based on the nature of the organization and employees. The ability to articulate security threats and risks and recommend a custom security plan that bridges these loopholes plays a central role in my position as the Chief Information Security Officer within the organization. The breach of the Office of Personnel Management OPM led to the compromise of millions of workers' data and personal information (OPM, n.d). As CISO, my role is to prevent the occurrence of such an incidence in the organization, through the careful application of a custom security plan that addresses all the risks and vulnerabilities.

Data Flows

The emergence of computer networks and information technology facilitates the flow of data across diverse networks (UMUC, 2019). While this flow of data is a multiplier force in running business operations, it presents significant challenges in the protection and safeguard of enterprise data and information. Data flow is a highly complex process involving both structured and unstructured data (Taylor, 2018). Most importantly is that these flows are impacted by both policies and people. This implies that organizations are likely to set policies that define the flow of data and those that set guidelines on how this data will be managed and protected. Data storage consists of numbers that make storage and processing easier and more flexible. The smallest storage unit is the bit [referred to as the binary digit], the bits can be described as the building blocks of major data. As a result, the bits are organized or arranged in different separate blocks of 8, each known as a byte. Both textual and non-textual data can be categorized or stored in the form of bits or bytes depending on the size, nature, and structure (Taylor, 2018). For instance, pictures and images are stored in the form of bits.

Basic Cybersecurity Concepts and Vulnerabilities

Cybersecurity vulnerabilities refer to potential threats that can potentially harm data or compromise the integrity of information systems (Goolik, 2019). Missing data encryption is a vulnerability that can easily expose unhidden information and data. OS command injection is another threat that can compromise the integrity of networks. Buffer overflows are also utilized by cybercriminals to gain unauthorized access to secured networks, data and information systems. Weak passwords and path reversal activities similarly pose mounting pressure on the integrity of systems, computers, and networks. Weak passwords can easily be cracked through detection software while path reversals may easily expose data flow to cybercriminals. The SQL injection represents another vulnerability or threat. Essentially, the SQL injection is a code injection that targets data-driven applications whereby malicious SQL statements are inserted or put into an entry point for implementation or execution. Other vulnerabilities include; broken algorithms, bugs, missing authentications, reliance on unauthenticated inputs, and the online downloading of codes without running integrity checks (Goolik, 2019).

Common Cybersecurity Attacks

Denial-of-service attacks DOS and delayed denial of service attacks DDOS are the most common cyber-attacks (Cisco, n.d). These involve deliberate attacks that delay services to create adequate time for cybercriminals to execute and conceal computer attacks. The Man-in-the-Middle attacks MIM attack is a computer-generated attack that involves two parties communicating with each other. The attacker alters communication and makes them believe they are talking to each other. SQL injection attack is another infiltration which involves the injection of a SQL statement to execute possible computer attacks. Password attacks involve the use of identifiers to detect password combinations or the use of bots to detect users' login credentials. Password attacks are mostly executed when computers or laptops are left unattended or by shared public cyberspaces. Drive-by attacks represent another category which involves the downloading of drives online that contain malware. Upon download, it plants a malicious script into the HTTPs and corrupts internet-connected systems and networks. Other common cybersecurity attacks include cross-site scripting, eavesdropping attack, phishing, and spear phishing (Cisco, n.d).

Penetration Testing

Penetration testing is seen as a form of security testing where assessors actually mimic real-world hackers and attempt to hack into an organization’s system (Cyberd, n.d). The goal of penetration testing is to circumvent the security models and security features of a system, network, or database. In cases where organizations have password expiry policies, penetration testing allows the running of password crackers to determine the passwords nearing the expiry. This form of penetration testing enables a firm or an organization to validate its password policy. Network Forensic Analysis Tools provide an intelligence cover that automatically detects or discovers any

alterations in systems and networks. The goal of Network Forensic Analysis Tool is to provide intelligence. Most importantly, it acts as a signal of detecting any slight attempts to penetrate systems.

[Stages of Penetration Testing] (Cyberd, n.d)

Discussion of Major Concepts of Enterprise Security

Concepts like the confidentiality of data are key in enterprise security. Confidentiality assures that all data are treated with respect and that they are not shared with third-parties. Data privacy is another concept and this relates to the parties authorized to access specific information sets. Data integrity involves the application of data to solve real-life problems. This means that data integrity provides means and approaches to use data in a safe and secure manner that protects the needs and interests of all parties and shareholders.

Security Principles of the Security Framework

Most security frameworks are pinged on common principles of confidentiality, availability, and integrity. Confidentiality ensures that all persons responsible for handling or storing specific sets of data exercise full responsibility over the safety of this data. It also means they are willing to take punishments for data exposures and theft. For instance, all electronic records management practitioners are held accountable for patient information, and hospitals are required to protect this data through HIPAA laws. The second principle is availability, all data is treated with respect and sharing can only be authorized by the patient. Informed consent is the final guideline and this means that due diligence must be conducted, and permission granted. Informed consent forms are often filled by visitors, caregivers, and patients as a means to authorized access to protected data or clinical information.

Types of Cybersecurity Threats

The Federal Process Standards FIPS sets aside three major types of cybersecurity risks likely to affect organizations. The loss of the availability, integrity, and confidentiality of sensitive information and data harbors far-reaching impacts on organizations, individuals, and consumers. For large enterprises like my organization, these risks can be categorized into distinct groups like; moderate, high-risk and low-risk (Schneier, 2004). The potential impact is low if the integrity, availability, and confidentiality of stored data are less affected by cyberattacks. For instance, the hacking of an organization's internet or Wi-Fi system may not pose significant threats or risks like the compromise of consumer information stored in management systems. High-level cybercrime risks include data theft, compromise on financial systems, intellectual property theft, and phishing.

Conclusion

This part of the security plan offers a description of the data flows. It identifies that data flow is a complex process involving both structured and unstructured data. Most importantly is that these flows are impacted by policies and people. This implies that organizations are likely to set policies that define the flow of data and those that set guidelines on how this data will be managed and protected. When examining major cyber security threats, the paper notes that weak passwords, missing data encryption, SQL injections and buffer overflows represent major security threats and hazards. The paper proceeds to examine penetration testing. It notes that penetration testing is a form of security testing where assessors actually mimic real-world hackers and attempt to hack into a system. The goal of penetration testing is to circumvent the security models and security features of a system, network, or database. The above analysis surmises the paper on the cybersecurity background information.

References

Cisco, (n.d). Cyber Attack - What Are Common Cyberthreats? (2019, August 14). Retrieved October 7, 2019, from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

Clement, J. (n.d.). Topic: U.S. consumers and cyber-crime.

Cyberd, (n.d). Penetration Testing. (n.d.). Retrieved October 7, 2019, from https://www.cyberd.us/penetration-testing.

Goolik, S. (2019, April 18). 2019 Cyber Security Vulnerabilities: Know Your Enemy. Retrieved October 12, 2019, from https://symmetrycorp.com/blog/8-cyber-security-vulnerabilities/.

OPM, (n.d). Cybersecurity Resource Center Cybersecurity Incidents. (n.d.). Retrieved October 7, 2019, from https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

Schneier, B. (2004). Secrets & lies – Digital security in a networked world. Retrieved October 7, 2019 from https://www.schneier.com/books/secrets_and_lies/

Taylor, C. (2018, March 28). Structured vs. Unstructured Data. Retrieved October 7, 2019, from https://www.datamation.com/big-data/structured-vs-unstructured-data.html.

UMUC, (2109). Data Flows Across Networks. (2019). Retrieved from https://lti.umuc.edu/contentadaptor/page/topic?keyword=Data Flows Across Networks.