Short Research Paper #2

Cybersecurity Policy Research

Jeggo Paolo V. DyCok

School of Cybersecurity, Old Dominion University

CYSE300_29216: Introduction to Cybersecurity

Dr. Joseph Kovacic

January 29, 2023

The average casualty cost of data breach attacks goes above 4.3 million dollars and critical infrastructure breach costs over 4.8 million dollars according IBM's *Cost of Data Breach Report 2022.* The cost of the breach could potentially be a lot higher if contingencies and securities are not properly implemented. These types of contingencies and securities are defined by well-built policies that dictate safe operation of organizational systems and proper handling of incidences that lead to expensive expenditures to limit collateral damages. This research paper will address some of the cybersecurity issues that will need to be covered in order to secure sensitive data that will be stored in the corporate system.

Before we begin, we must define what cybersecurity policy is. Cybersecurity policy is a detailed document dictating technical guidelines, ranging from acceptable use and handling of security incidents. Cybersecurity policies ensure the efficient and correct handling of information within a specific set of safety guidelines to enable organizations to function.

One of the biggest issues with cybersecurity is the social aspect. It is also one of the reasons why cybersecurity is partly studied as behavioral in its nature. The reason for that lies in the fact that plenty of cyber-attacks exploit the social element of a system. Social engineering and phishing attacks account for millions of people that become a victim to fraud, resulting in monetary and data loss. This is where acceptable use comes in. Cybersecurity resiliency comes in educating every person within an organization with proper use of computers as well as physical elements of an organization as they make up most of its services.

Handling of data comes as a big part of securing information. To ensure that only those with "need to know" would only have the privilege to see it, a policy regarding classification and material handling should be in place. Sensitive data is critical to any organization and can pose as a dangerous point of exploitation, therefore everyone in the organization should know how to

treat data of all types to make sure it doesn't fall into the wrong hands. This involves practicing safe transport and disposal of sensitive data.

One of the big issues in securing critical infrastructure is the exploitation of user privileges. The attacker can penetrate the system and change its configurations to match his or her intentions and cause damage. This can be done through bugs that can be found within a software's architecture or theft of administrative user account to obtain root access. A good policy must be in place to avoid this type of attack which can include proper physical security, safe handling of sensitive materials and continuous monitoring for potential vulnerabilities.

Passwords have been the most overlooked security feature. With recent advancements in encryption technology, passwords have become virtually unbreakable within a span of a lifetime and multifactor authentication has made it more resilient to attacks. The limit to this security is the lack of understanding of the effectiveness of passwords. Password policy must be implemented in order to ensure security compliance, which can be done by setting parameters for acceptable password configurations and to encourage users to avoid using common words.

The testament to an organization's resilience is partly due to its incident response. Organizations must work to build a strong policy regarding incident response. It covers a major part of the cybersecurity framework that is tailored to each organization. Incident response will include procedures in identifying the attacks and isolating the damages in order to prevent escalation and to ensure that services are back immediately. A good incidence response will aid in reputation, resulting in trust between companies and their customers.

Policies must always be updated to improve security and procedures must always be in place to mitigate threats. Advancements in technology and continuous reliance on technology

will open plenty of opportunities for attack and exploitation. The most important commodity today lies in consumer information and cyber-professionals and the general public must continue to get educated in matters of information security in order to reduce the chances of being a victim.

References

Henry, E. (n.d.). *How to create an effective cybersecurity policy*. 9ine. Retrieved January 29, 2023, from https://www.cm-alliance.com/cybersecurity-blog/how-to-create-an-effective-cybersecurity-policy

IBM Corporation. (2022, July). Cost of a Data Breach Report 2022. New York.

Policies & procedures protect against cyberattacks. Trellix. (n.d.). Retrieved January 29, 2023, from https://www.trellix.com/en-us/security-awareness/cybersecurity/cybersecurity-policies.html#:~:text=A%20cybersecurity%20policy%20sets%20the,data%20breaches%20are%20potentially%20costly.