Short Research Paper #2

Diane Gilzow

CYSE 300 Introduction to Cybersecurity

Dr. Sandip Roy

September 15, 2024

Security is an integral part of any organization or enterprise. Any company that handles sensitive data is responsible for ensuring that it's protected to the upmost degree. As cyber threats become increasingly prevalent, security policies need to be up to date and focused on providing the highest level of security. Failure to uphold good security practice increases the chance of a cyberattack, which can lead to loss of trust, reputational damage, and financial loss. A good security policy should address the following issues: data protection, data backup, security awareness, vulnerability management, and incident response.

When companies handle sensitive data, it is necessary that it is handled only by authorized personnel. The CIA (Confidentiality, Integrity, Availability) protocol ensures that data is protected and only accessible only to authroized users. Confidentiality ensures that data is viewed and handled by authorzied users. It should also be clearly defined which users have authority over specific data and what data can be shared with whom. Data also needs to have integrity by preventing it from getting corrupted or altered by outside means, which can be addressed through using encryption. Encryption allows data to be kept hidden from unauthorized access, whether it's stored at rest or in transit from one source to another. Availability allows the systems and data to be readily available at any time. Should there be downtime at any point can present a vulnerability in the system. In order to maintain availability, hardware should be properly maintained, regular updates should be performed, and a failover plan should be in place.

On top of keeping data secured, data also needs to be backed up in the case of disasters, system failures, attacks, or other unexpected events. All data that needs to be backed must be identified first and a secure location needs to be determined that can safely store backups. Losing data can cause critical damage for business and organizations, which is why having a secondary location is essential for data recovery. Security awareness is also vital for proper implementation

and adherence to security policies. Users need to be aware of the strategies used by attackers that can disrupt security and normal operations. Regular assessment ensures that users are vigilant and informed of evolving cyber threats, such as recognizing social engineering tactics like phishing emails. These assessments should be conducted periodically and adapted to evolving trends that threaten data security.

Vulnerabilities can arise at any time, which is why patch management is mandatory for proper security. Patch management allows systems and networks to perform optimally and to minimize the risk of an attack. Regularly updating the OS, firmware, drivers, and software on a timely schedule helps address any known vulnerabilities and keeps systems and data well-protected. However, despite maintaining good efforts on reducing vulnerabilities, the possibility of an attack still remains. In the event of an active cyberattack, users must be prepared to respond at any time. Incident response plans provide guidance to users on how to respond to an attack and outline what steps to take when it occurs. Responsibilities should be clearly defined, including tasks relating to identifying, responding to, and recovering from an attack. Users should also be informed about the aftermath of the attack and address any damages that may have occurred as a result. Having a well-thorough incident response plan in place can help an organization recover effectively from an attack.

Overall, constructing a well-rounded information system security policy allows employees within a business or organization to take proper steps to ensure top-notch security. Tactics such as keeping sensitive data secure, regularly patching systems, assessing users on security knowledge, and planning ahead in the case of an incident helps maintain proper security measures. These practices help mitigate risks and ensure preparedness for potential threats and

attacks. Therefore, they are essential in having a robust security policy and the overall integrity of a business or organization.

References

The 12 elements of an information security policy. Exabeam. (2024, July 3). https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/

U.S. Department of Health and Human Services. (n.d.). *Writing a Data Management & Sharing Plan*. National Institutes of Health. https://sharing.nih.gov/data-management-and-sharing-policy/planning-and-budgeting-for-data-management-and-sharing/writing-a-data-management-and-sharing-plan#after

Information Security. (n.d.). *Data security policy*. https://security.duke.edu/policies-procedures-and-standards/data-security/data-security-policy/

What is data backup? The Complete Guide. Cloudian. (2024, September 5). https://cloudian.com/guides/data-backup/data-backup-in-depth/

Patch management helps IT teams eliminate bugs, promote productivity. (n.d.). *What is patch management? benefits and best practices*. Intel. https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/patch-management.html#:~:text=Patch%20management%20is%20the%20process,performance%20of%20systems%2C%20boosting%20productivity.

Cybersecurity Incident Response: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response