Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

Defensive Controls and Processes for Significant Threats

Folorunsho O. S
Washington University of Science and Technology
Vienna, VA, USA.

Ayinde A. Q
Northcentral University
Scottsdale, AZ, USA.

Yusuf A.S
New York Institute of Technology
Old Westbury, NY, USA

***Abstract*— Information technology is one of the critical infrastructures that is exposed to natural and artificial threats, either deliberate or accidental. The security stakeholders must identify threats and implement proper defense mechanisms to mitigate the damages the threat will cause to information technology. Due to an increase in cyber-attacks on information technology infrastructure, security stakeholders will devise a means to adopt standardized theories, frameworks, and models to respond to the vulnerabilities in the information technology infrastructure.**

Keywords*— Defense; cyber-attack; controls; planning; risk assessment.

1. INTRODUCTION

Core target systems are information technology systems and processes utilized by organizations and governments that enable the ability to store and process large volumes of data and to carry out their core activities and transactions in a secure manner which are susceptible to cyber threats and attacks. In the banking industry, which is the focus industry of this paper, core target systems typically include the core banking system (CBS), payments system, treasury system, risk management system and customer relationship management (CRM) system.

In addition, core target processes refer to business processes that have the highest priority and are essential for the successful operation of a business. Examples of core target processes include accounting and finance, human resources, customer service, operations, information technology, marketing and sales, research and development, and supply chain management. To maximize organizational effectiveness, these processes must be identified, documented, monitored, and continuously improved. In banking, core target processes include account opening and onboarding, loan origination, treasury operations, payments processing, customer service and relationship management, fraud and risk management, and compliance management [1].

2. FRAMEWORK, THREATS, VULNERABILITIES AND CONTROLS

There was a breach in the Colonial Pipeline employee credential, which targeted the billing system infrastructure of the organization. The Colonial Pipeline attack was very devastating, and it inflicted a lot of pain on the company and Americans that depended on fuel to commute from one place to the other. The threat actors settled in the Colonial Pipeline network infrastructure to attack the credential system that housed the employee's username and password. The threat actors deployed ransomware as a Distributed Denial of Service to attack the credential system of the organization [2].

The security team will develop a plan to respond to information technology attacks within the Colonial Pipeline network infrastructure. The response strategy must be prepared and timely action to be taken by security stakeholders and employees. The response plan must capture the roles and responsibilities of the security stakeholders. The security team at Colonial Pipeline must dedicate personnel to monitor the inbound and outbound traffic to track incidents in real-time. The personnel will be the ones to initiate the recovery procedure, and he will collaborate with law enforcement personnel to issue sanctions to the threat actor country [3].

The security stakeholders at Colonial Pipeline must understand and re-evaluate the information technology security controls timely. The security control must reflect the threat landscape and organization assets. Detective and deterrent controls are crucial to alert the stakeholders should an incident occurs and prevent the threat from exploring the vulnerabilities in the Colonial Pipeline information technology infrastructure. Colonial Pipeline's security team must adopt logical and technical controls to protect the organization's information technology infrastructure. This control integrates trusted platform modules (TPMs) such as credential authentication, encryption, and biometric reader. Operational controls must be deployed across the organization to track insider and employee activities in real time [4].

The cybersecurity framework for the Colonial Pipeline is divided into five: identity, protect, detect, respond and recover. The security stakeholders will create an asset inventory for the organization within the operational business environment. The security team needs to conduct a risk assessment on the inventoried asset. Cybersecurity governance must ensure a strategy is in place to manage the organization's security controls, risk, and accountability of the cybersecurity framework adopted by the Colonial Pipeline.

To protect the Colonial Pipeline infrastructure, appropriate controls must be deployed during the protection stage of the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

framework, as discussed in the paragraphs above. A security monitoring solution will be deployed to detect anomalies or incidents within the organization's infrastructure. The intrusion and detection system will track threat actors' activities, while the intrusion and prevention system will prevent the threat actors from exploiting the vulnerability in the organization's information infrastructure.

The response planning methodology has been discussed, and security stakeholders should ensure timely communication when analyzing the event logs for insider and outsider activities. The response plan must adopt a mitigation method to reduce the effect of an attack on the Colonial Pipeline infrastructure. During the recovery process, the recovered system must be improved by conducting a risk assessment of the newly recovered system [5].

3. AT RISK CORE TARGET SYSTEMS AT COLONIAL PIPELINE

Specific core target systems and processes at Colonial Pipeline may be at risk from global cybersecurity threats [6].

Billing applications: the billing applications are often the target of cyber-attacks due to their increased availability and convenience. Hackers can gain access to an employee's data, personal records, and billing processing systems.

i. Network infrastructure: The billing system is dependent on their IT infrastructure to deploy and maintain security measures. Hackers can use malicious software to gain access to this infrastructure, disrupting banking operations and affecting customer trust.

ii. Online vendor portals: Online portal services are the main point of contact between Colonial Pipeline and its customers. As such, they are highly vulnerable to cyber-attacks. Attackers can use malware, phishing tactics, and other methods to gain unauthorized access to customer data and accounts. The security stakeholders must ensure that customers are accurately identified to protect against fraud and unauthorized access. The security team must ensure that the online portal must be configured to use customer authentication protocols such as two-factor authentication (2FA) to provide an additional layer of protection and security.

iii. Network Systems: Network-based systems are typically targeted by malicious actors as they can provide access to important data and resources within organizations. Network systems should deploy strong security measures such as firewalls and antivirus software to prevent unauthorized access.

iv. Data Storage Systems: Data storage systems are often targeted as they tend to store large amounts of sensitive information. Organizations should use strong encryption and authentication protocols to protect their data, as well as backup systems to ensure critical data is not lost or destroyed in the event of a security breach.

v. Application Security: Applications contain sensitive data and can be used to gain access to other systems and resources. Organizations should deploy application security measures such as firewalls and authentication systems to prevent malicious actors from exploiting vulnerabilities.

vi. Identity Management: Identity management is important for ensuring that only authorized users have access to sensitive systems and data. Organizations should invest in identity and access management systems to ensure that user credentials are secure and authentication requirements are met.

vii. Endpoint Security: Endpoint security in banking are the specific measures and technologies adopted to safeguard bank networks and systems from malicious actors. Endpoint security encompasses a range of measures such as antivirus software, firewall protection, device authentication, and application whitelisting. These measures are designed to protect end-user devices and networks from malicious attacks, unauthorized access, and data breaches. Endpoint security is vital for banks as a breach of a single endpoint can have far-reaching consequences.

The systems, probable methods of entry, diffusion, exploration, and exfiltration options of cybersecurity attacks in Colonial Pipeline may include [7] thus:

i. Methods of Entry: Common methods of entry for security attacks include phishing, SQL injection, malicious emails, social engineering, spear phishing, credential stuffing, and brute-force attacks.

ii. Diffusion: Once an attacker has gained access to a system, they can spread their attack by exploiting vulnerabilities, privileging escalation, or by infecting other systems on the same network.

iii. Exploration: Attackers will then explore the system and networks to identify potential targets. This may include searching for financial information, customer data, and authentication credentials.

iv. Exfiltration: After gaining access to these data, attackers can use various methods to steal the information they have found. These could include packet sniffing, malware, and remote access tools.

CONCLUSION

The Colonial Pipeline security team must deploy a robust cybersecurity framework to monitor threat actors' activities. The security team at Colonial Pipeline must dedicate personnel to monitor the inbound and outbound traffic to track incidents in real-time. The security stakeholders will develop a recovery plan and collaborate with external law agencies to issue sanctions to the threat actor country.

Operational controls must be deployed across the organization to track real-time insider activities. To prevent threat actors from taking control of sensitive operations. The organization must include asset classification, cybersecurity awareness, training, and constant review of log files from all the organization systems and applications. To prevent a future attack on the Colonial Pipeline, the security stakeholders in the organization must comply with the points discussed in this paper.

REFERENCES

[1] Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: a systematic literature review. *Information & Computer Security*. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2836701

[2] 4.Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

[3] Piggin, R. S. H. (2014, October). Governance, risk and compliance: impediments and
opportunities for managing operational technology risk in industrial cyber security and
safety. In 9th IET International Conference on System Safety and Cyber Security (2014) (pp. 1-8). IET.

[4] Traci., S. (2019). How to respond to a cyber-attack. https://www.nist.gov/blogs/manufacturing-innovation-blog/how-respond-cyber-attack

[5] Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022). Cyber Security Threats on Digital Banking. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-4). IEEE.

[6] Brooks, T. (2022). The Professionalization of the Hacker Industry. *arXiv preprint arXiv:2207.00890*.

[7] Haruna, W., Aremu, T. A., & Modupe, Y. A. (2022). Defending against cybersecurity threats to the payments and banking system. *arXiv preprint arXiv:2212.12307*.

[8] Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

[9] Uddin, M.H., Ali, M.H. & Hassan, M.K. (2020). Cybersecurity Hazards and Financial System Vulnerability: A Synthesis of Literature. *Risk Management* 22, 239–309. https://doi.org/10.1057/s41283-020-00063-2.