THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Viswanath Srinivasan Chirravuri
D.Eng. | DC7 | G34657239 | September 2nd, 2024

CSCI 6015: Homework-2: Containing the Damage: A CIA triad approach to a cybersecurity breach

Introduction

When a CISO (Chief Information Security Officer) of an organization faces a cybersecurity breach involving the exfiltration of client data to an external source outside the U.S., it is important to act quickly and effectively to *contain* the damage. The primary focus will be on protecting the confidentiality, integrity, and availability (CIA) of the compromised data while identifying and mitigating the further impact of the breach. This document presents a strategic approach to limit the damage associated with this breach.

Protecting Confidentiality

Confidentiality ensures that sensitive information is only accessible to those authorized to view it. For this breach, immediate steps must be taken to protect the confidentiality of client data.

Isolate Affected Systems
The first step is to isolate the affected systems to prevent further data leakage. This can be done by disconnecting compromised systems from the network (physically or virtually), and configuring firewall to block connections to it. Isolation will help contain the breach and prevent the attacker from accessing additional sensitive information.

Access Control Management
Review and restrict access permissions to sensitive data. Revise and re-apply the *principle of least privilege* to ensure that any unauthorized employee or system cannot data it. Using multi-factor authentication (MFA) adds an extra layer of security by requiring multiple forms of verification before granting access to sensitive information.

Data Loss Prevention (DLP) Tools
Deploy DLP tools to monitor, detect, and block the unauthorized transmission of sensitive data. These tools can automatically prevent the movement of confidential data to external locations, thus mitigating the risk of further exfiltration.

Ensuring Integrity

Integrity involves maintaining the accuracy and trustworthiness of data. Post-breach, it is crucial to ensure that the data has not been altered or tampered with.

File Integrity Monitoring (FIM)
Implement FIM solutions (e.g. Tripwire) to track and alert any unauthorized changes to critical system files and data. By monitoring changes in real-time, the organization can quickly identify and respond to attempts to alter data.

Hashing and Checksums
Use hashing algorithms (e.g. SHA256) to create checksums of critical data files. Compare the current checksums with the original values will help detect any unauthorized modifications. This can ensure that any tampering is identified promptly.

Digital Signatures
Utilize digital signatures for validating the authenticity of documents and data. Digital signatures provide a way to verify that the data has not been altered and that it originated from a trusted source.

Maintaining Availability

Availability ensures that data is accessible when needed by authorized users. Following a breach, it is crucial to maintain or restore the availability of business services and data.

Backup and Recovery
Use backup strategy that includes regular and automated backups of critical data. Ensure that backups are stored securely and are isolated from the primary network to prevent them from being compromised in a breach. In the event of data corruption or loss, having reliable backups enables the restoration of data with minimal downtime.

Redundancy and Failover Systems
Deploy redundant systems and failover mechanisms to maintain service availability. If primary systems are affected by the breach, redundant systems can take over, ensuring that services remain accessible to clients and employees.

Distributed Denial of Service (DDoS) Protection
Given that breaches may be accompanied by DDoS attacks to disrupt service availability, implementing DDoS protection mechanisms such as rate limiting, traffic filtering, and the use of CDNs (content delivery networks) can help mitigate such threats.

Conclusion

Containing the damage of a cybersecurity breach requires a comprehensive approach that addresses all aspects of the CIA: confidentiality, integrity, and availability. By implementing measures such as isolating affected systems, utilizing file integrity monitoring, and maintaining robust backup and recovery processes, the organization can effectively mitigate the impact of the breach. Access control management, and a well-utilized continuous monitoring systems further ensure that the organization is prepared to protect its clients' data and maintain trust in the face of cybersecurity threats.

References

National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg, MD: U.S. Department of Commerce, 2018. Available at: https://www.nist.gov/cyberframework.

Center for Internet Security (CIS). *CIS Controls v8*. New York, NY: Center for Internet Security, 2020. Available at: https://www.cisecurity.org/controls/v8.

Microsoft. *Implementing Data Loss Prevention (DLP)*. Redmond, WA: Microsoft Corporation, 2022. Available at: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies.