Joshua Farias

Professor Cooper

SEC 605

18th February 2024

Assignment 1: Analyzing Critical Security Controls

Introduction

As a publicly traded financial investment firm, Cooper & Kumar is subject to a myriad of regulations that require regular auditing to ensure the necessary compliance standards are met. This report identifies five critical security controls, as outlined by the SANS CIS Critical Security Controls, to verify during a compliance audit and proposes a summary plan to enhance the security of the firm's IT infrastructure.

Findings and Recommendations

The SANS Institute's CIS Critical Security Controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices designed to prevent the most pervasive and dangerous cyber-attacks. Considering Cooper & Kumar's operational and security requirements, the following five controls have been identified as critical for verification during compliance audits:

1. **Inventory and Control of Hardware Assets**: Hardware asset management ensures only authorized devices access the network, mitigating risks posed by unauthorized devices. Regular audits of hardware inventory allow for the timely detection and management of potential vulnerabilities.
2. **Inventory and Control of Software Assets**: Software asset management prevents unauthorized software from introducing vulnerabilities such as malware. A comprehensive software inventory supports patch management and compliance, reducing the attack surface.
3. **Data Protection**: Protecting sensitive data, especially client financial information, is critical. Implementing encryption, access controls, and data loss prevention (DLP) mechanisms ensures data confidentiality, integrity, and availability.
4. **Continuous Vulnerability Management**: Regular scanning and remediation of vulnerabilities are crucial in preventing exploitation by threat-actors. Cooper & Kumar should implement a program that continuously identifies, classifies, prioritizes, and remediates vulnerabilities.
5. **Controlled Use of Administrative Privileges**: The misuse of administrative privileges is a common attack vector. Implementing access controls that follow the principle of least privilege, monitoring, and controlling administrative credentials can significantly reduce the risk of breaches.

Summary Plan to Strengthen IT Infrastructure:

- Develop and maintain comprehensive inventories of all hardware and software assets within the organization's network to ensure visibility and control.
- Implement robust data protection measures such as encryption and DLP strategies, to protect sensitive client information against unauthorized access and breaches.
- Establish a continuous vulnerability management program that actively identifies and addresses vulnerabilities through regular assessments and patch management.
- Enforce strict administrative privilege controls following the principle of least privilege, credential management, and monitoring of administrative actions to minimize insider threat risks.
- Regulatory staff training and awareness programs to ensure all employees understand their role in maintaining cybersecurity and are equipped to recognize and respond to security threats.

Conclusions

The implementation of the identified SANS CIS Critical Security Controls will significantly enhance Cooper & Kumar's security posture, ensuring the firm has strong defensive measures in place to protect against the ever-evolving cyber threats while maintaining compliance with regulatory requirements. These controls not only protect sensitive customer information but also establish a foundation for a strong security culture within the organization. Continued commitment to these practices will safeguard Cooper & Kumar's reputation, client trust, and ultimately, its competitive edge in the financial sector.

Citations:

- SANS Institute. (2023). CIS Controls. Retrieved from https://www.cisecurity.org/controls/cis-controls-list
- Rapid7. (2023). Critical Controls. Retrieved from https://www.rapid7.com/solutions/compliance/critical-controls/