2-3 Short Response: Breach Analysis Simulation One

Joshua Merren

Southern New Hampshire University

CYB-250-11621-M01 Cyber Defense

Professor Tchinda Mbuna

8 July 2024

Confidentiality is crucial as it directly impacts the security of data transactions on the e-commerce platform. The outdated SSL encryption system posed significant data integrity and confidentiality risks, making the system vulnerable to various attacks. Such vulnerabilities highlight the importance of transitioning to more robust encryption methods like TLS, which provides enhanced security features, including better encryption algorithms and secure handshake protocols. The change from SSL to TLS in the scenario is not merely a technical update; it is a critical shift towards strengthening the confidentiality of customer data as it travels across the internet. This upgrade is essential in preventing unauthorized access and ensuring that sensitive information remains protected from cyber threats. The move to TLS also aligns with best practices recommended by security professionals and standards organizations, which advocate for adopting up-to-date protocols that can effectively shield data against sophisticated cyber-attacks (Agrawal, 2024). Confidentiality is paramount in maintaining customer trust and safeguarding the company's reputation, which data breaches can severely damage.

SSL, once a standard for securing transactions over the internet, is fraught with numerous security issues that could compromise sensitive data. These issues include vulnerabilities to decryption attacks like POODLE and BEAST, which exploit weaknesses in encryption to intercept or alter data (Team, 2023). The development of TLS, which introduces more secure and efficient cryptographic techniques and protocols, has addressed these security flaws. TLS improves upon SSL by eliminating outdated algorithms and employing a more secure method of key exchange and data integrity checks, significantly enhancing the security and performance of data transmissions. By adopting TLS, organizations can ensure their communications are secure from eavesdropping, tampering, and other malicious activities. The adoption of TLS indicates an organization's commitment to cybersecurity and its proactive stance in addressing evolving cyber

threats. This transition secures data transactions and fortifies the organization's defenses against future vulnerabilities. Thus, TLS is not just an upgrade; it is a crucial investment in the organization's long-term security strategy, providing reassurance and confidence in the security of your data.

For small organizations, developing a robust Computer Incident Response Team (CIRT) is essential despite the size constraints. These organizations often face the challenge of limited resources, both in terms of personnel and technology. However, through strategic planning and efficient use of available resources, small organizations can establish a competent CIRT capable of handling a variety of cyber incidents. This involves training existing staff in basic and advanced cybersecurity practices, ensuring they can identify, respond to, and mitigate threats effectively. Additionally, small organizations can benefit greatly from partnerships with external cybersecurity experts and services, which can provide the necessary support and augmentation during critical incidents. These partnerships enable the organization to access specialized skills and knowledge, thereby enhancing its incident response capabilities. It is also crucial for these organizations to maintain a well-documented and regularly updated incident response plan. This plan, which helps in the swift and effective mobilization of resources during a security breach, provides a sense of preparedness and control in the face of potential cyber threats (Gitlan, 2024). By fostering a culture of continuous learning and improvement, small organizations can turn their size into an advantage, allowing for quicker decision-making and adaptation in the face of cyber threats.

References

Agrawal, S. (2024, June 14). The evolution of Secure Protocols: SSL and TLS transition and Advantages - Sanchit Gurukul1. *Sanchit Gurukul*. https://sanchitgurukul.in/ssl-and-tls/

Gitlan, D. (2024, April 2). *Is SSL Deprecated? Explore the Transition from SSL to TLS*. SSL Dragon. https://www.ssldragon.com/blog/is-ssl-deprecated/

Team, C. (2023, October 24). *A comparison between SSL and TLS: What you need to know - CacheFly*. CacheFly. https://www.cachefly.com/news/explore-ssl-your-guide-to-understanding-implementing-secure-socket-layers/