4-4 Milestone Two: Checklist Analysis and Modification

Southern New Hampshire University

CYB-300-11432-M01 System and Comm Security

Professor Robert Chubbuck

23 July 2024

The Milestone Two Checklist, modeled after the NIST SP 800-70 guidelines, plays a critical role in ensuring the security of IT products by providing a structured approach to security configurations. However, certain aspects of this checklist could benefit from updates to better align with current technological advancements and security practices. For instance, as specified in the checklist, the current use of TLS v1.2 needs to be updated compared to the more secure and efficient TLS v1.3. Upgrading to TLS v1.3 is recommended because it offers enhancements in security features that protect against modern threats, reduce the attack surface, and improve performance through faster connection times. Furthermore, the checklist lacks specific strategies for encryption and the automation of certificate revocation processes, which are essential for maintaining robust security measures. Detailed protocols such as AES-256 for encryption should be explicitly defined to ensure robust data protection. Similarly, establishing automated triggers for certificate revocation in response to security breaches can significantly enhance the system's responsiveness to threats. Integrating these specific protocols and automation processes will not only streamline operations but also bolster the overall security posture of the IT environment (Quinn et al., 2018).

Regarding applicability, the checklist covers fundamental areas crucial for securing a Certificate Authority (CA) server, such as system identification, account management, and authorization controls. However, the checklist could be more effective if it incorporated precise guidelines for implementing and maintaining these security controls. More detailed instructions on configuring and updating security protocols are necessary to ensure consistent enforcement and compliance with security standards. Adopting modern security technologies like the Security Content Automation Protocol (SCAP) could reduce vulnerabilities by automating security updates and managing configurations more effectively. To conclude, while the checklist provides a solid security management foundation, it must be updated to reflect the latest security protocols and technologies. Enhancements in the TLS protocol version, encryption methodologies, and the automation of security processes are crucial for keeping up with the evolving cybersecurity landscape. By addressing these areas, the checklist can better minimize vulnerabilities and secure IT products against potential threats (Quinn et al., 2018).

References

Quinn, S. D., Souppaya, M., Cook, M., & Scarfone, K. (2018). *National checklist program for IT products - guidelines for checklist users and developers*. https://doi.org/10.6028/nist.sp.800-70r4