3-1 Journal: Audit and Assessment of Users, Workstations, and LANs

Joshua Merren

Southern New Hampshire University

CYB-400-13637-M01 Security Assessment & Auditing

Professor Jillian Seabrook

11 November 2024

Auditing user environments is crucial for identifying and mitigating organizational security risks. By monitoring and analyzing user activities, audits help detect unauthorized access or policy violations, often indicators of internal threats or compromised accounts. Such audits ensure that all users stick to set security policies and that deviations are promptly addressed, thus maintaining a secure and compliant operational environment. Regularly auditing user actions helps prevent data breaches and ensures compliance with regulatory standards like GDPR and HIPAA, which demand strict control over access to sensitive information (Berezin, 2024).

Workstation audits are vital for securing endpoint devices that access corporate networks. These audits assess the security health of each workstation, checking for vulnerabilities such as outdated software, unauthorized applications, and other potential security threats. By ensuring that all workstations comply with the latest security policies and are free from vulnerabilities, organizations can protect themselves against malware infections and other endpoint-related attacks. Regular workstation auditing helps maintain system integrity and operational efficiency, optimizing IT resources' overall performance (*The Importance of Regular Security Audits and Assessments in IT*, 2024).

LAN auditing is essential for ensuring the security and performance of network infrastructure. This process involves scanning the network to identify unauthorized devices, potential security gaps, and performance issues such as bottlenecks. Effective LAN audits help maintain network integrity by ensuring that all connected devices and traffic fit into security protocols, which is crucial for preventing cyber-attacks and data breaches. Additionally, these audits significantly optimize network performance, ensuring that data flows efficiently without

interruptions, thus supporting seamless business operations (*What Is a Cyber Security Audit and Why Is It Important?*, n.d.).

References

Berezin, J. (2024, September 4). *The importance of regular cybersecurity audits and assessments*. CYOP. https://cyopsecurity.com/insights/the-importance-of-regular-cybersecurity-audits-and-assessments/

The importance of regular security audits and assessments in IT. (2024, May 14). Computer Business Consultants | Orlando, Clermont, Winter Garden. https://computerbusiness.com/news/the-importance-of-regular-security-audits-and-assessments-in-it/

What is a Cyber Security Audit and Why is it Important? (n.d.). https://www.dataguard.co.uk/cyber-security/audit/