Topic 6 Discussion 1

There is no such thing as a secure information technology system. Many information systems have design flaws or vulnerabilities that a threat actor can exploit. Therefore, organizations need to have an incident response policy. Review the NIST computer security incident handling guide and discuss the different phases of the incident response process, as well as the tools and technology used by the incident response team during the different phases.

Hello Class,

No IT system is perfectly secure. This necessitates robust incident response policies. The NIST Computer Security Incident Handling Guide provides a structured approach to managing these inevitable security incidents. It breaks the process down into four key phases, each crucial for an effective response.

The first phase, Preparation, is about proactive readiness. It involves establishing an incident response team, defining roles and responsibilities, and developing a comprehensive incident response plan. This includes identifying potential threats and vulnerabilities through risk assessments and vulnerability scanning(Grance, 2024). Organizations also need to implement security awareness training to educate staff on recognizing and reporting incidents. Tools like security information and event management (SIEM) systems, vulnerability scanners (Nessus, OpenVAS), and collaborative platforms (Slack, Microsoft Teams) are essential for this phase.

Next comes Detection and Analysis. This phase focuses on identifying and understanding security incidents. It involves continuous monitoring of systems for suspicious activity, analyzing logs and alerts generated by security tools, and correlating events to determine the scope and impact of the incident(NIST, 2024). Tools such as SIEM systems, intrusion detection systems (IDS), intrusion prevention systems (IPS), and network traffic analyzers (Wireshark) are crucial for this phase. The goal is to determine the nature of the incident, its source, and the affected systems.

The third phase, Containment, Eradication, and Recovery, is where action is taken to limit damage and restore systems. Containment involves isolating infected systems or limiting the impact of the incident(Cichonski, 2012). Eradication focuses on removing the threat, such as malware or malicious code. Recovery involves restoring systems and data from backups. Tools used during this phase include endpoint detection and response (EDR) solutions, malware analysis tools, disk imaging tools, and data recovery software.

Finally, Post-Incident Activity involves learning from the incident. This includes conducting a post-incident analysis to identify lessons learned, documenting the incident, and creating reports for management and stakeholders. This phase also involves implementing corrective actions to prevent similar incidents from occurring in the future(NIST, 2024). Tools utilized here include documentation software, project management tools, and potentially specialized incident reporting software. The aim is to improve security posture and prevent future incidents.

By following the NIST guidelines and utilizing the appropriate tools and technologies, organizations can significantly improve their ability to detect, respond to, and recover from security incidents, mitigating the inevitable risks associated with IT systems.

References:

Cichonski, Paul, et al. “Computer Security Incident Handling Guide.” *Csrc.nist.gov*, 6 Aug. 2012, csrc.nist.gov/pubs/sp/800/61/r2/final.

Grance, T. “Computer Security Incident Handling Guide.” *Govinfo.gov*, 2024, www.govinfo.gov/app/details/GOVPUB-C13-680c78d954997f970d751190be3e717b.

NIST. “Incident Response | CSRC | CSRC.” *CSRC | NIST*, 29 Feb. 2024, csrc.nist.gov/Projects/incident-response.