ISEC 675: Information Systems Auditing

Summer Term 2023

Eric Webb

Professor Ling Wang

Assignment 3: Written Essays

**Written Essay 2-2:**

The Remote Access Domain is a critical component of IT infrastructure and its purpose is to allow authorized users to remotely connect to a network. The Remote Access Domain is prone to various risks, threats, and vulnerabilities that can compromise the security of the network. It is essential to implement proper security controls at the Internet ingress/egress point to mitigate these risks. Organizations should identify common risks, threats, and vulnerabilities associated with the Remote Access Domain and identify network and security policies necessary for proper security.

Some common risks, threats, and vulnerabilities in the Remote Access Domain are unauthorized access, weak authentication, network eavesdropping, malware, phishing, and insider threats. Unauthorized access can cause significant risk because without proper authentication controls, malicious users can exploit and compromise systems. Weak password policies and lack of multi-factor authentication can increase the risk of brute-force attacks and other password cracking techniques. Network eavesdropping can be caused by un-encrypted traffic being intercepted or Man-In-The-Middle attacks. This risk is significantly increased when accessing systems through unsecured networks. Remote access endpoints are susceptible to phishing attacks, where users may unknowingly download malicious software or divulge private information through deception. Such attacks can compromise the integrity of the remote access domain. Insider threats happen when authorized users have malicious intent and gain access to unauthorized data or the ability to make unauthorized changes.

Network and security policies for remote access domain hardening should include strong authentication mechanisms, encryption, secure protocols, Intrusion Detection Prevention Systems (IDPS), network segmentation, audits, and patching. A strong authentication policy should implement multi-factor authentication, have strong password policies, and regularly update authentication protocols to help mitigate unauthorized access. All encryption should happen when data is in motion and at rest. The encryption should operate over a secure medium such Secure Shell (SSH) or a Virtual Private Network(VPN). Encrypting over secure protocols protects against eavesdropping. Implementing IDPS at the internet inguress/egress point all for real-time monitoring of suspicious activities and anomalies. IDPS can mitigate potential attacks on the remote access domain. Having networks segmented through firewalls or Virtual Local Area Networks (VLAN) can help contain potential threats. By isolating networks, it prevents adversaries from making lateral movements. Regular security audits are crucial for organizations to perform on a periodic bases. By reviewing the security audits, vulnerabilities assessments, and penetration testing results, organizations can address the security gaps within their remote access domains. Prompt patching and updating of remote access software and hardware mitigate the risk of exploitation of known vulnerabilities.

In conclusion, the Remote Access Domain is an integral part of IT infrastructure, but it is also susceptible to various risks, threats, and vulnerabilities. By implementing proper security controls at the Internet ingress/egress points, organizations are able to harden the Remote Access Domain and mitigate potential security breaches. By adopting strong authentication mechanisms, encryption protocols, IDPS, network segmentation, conducting regular security audits, and patching, organizations can enhance the security posture of their Remote Access Domain and protect the integrity of their network infrastructure.

**Written Essay 2-3:**

The System/Application Domain is a critical component of IT infrastructure and encompasses servers, applications, and data. This data can stored personal information such as credit card information or health care records. This domain is susceptible to various risks, threats, and vulnerabilities that can compromise the security of the data. It is crucial to implement proper security controls at the internet ingress/egress point to mitigate these risks. Organizations should identify common risks, threats, and vulnerabilities associated with the System/Application Domain and review the relevant elements of the Payment Card Industry Data Security Standard (PCI DSS) that pertain to servers, applications, and stored personal privacy data.

Some common risks, threats, and vulnerabilities in the System/Application Domain are unauthorized access, malware, ransomware, weak configurations, insider threats, and lack of data encryption. Unauthorized access to servers or applications can post significant risk to organizations. Lack of proper authentication controls can allow malicious actors to gain access to systems or data. Malware can compromise servers and applications. While also manifesting its self as ransomware demanding a ransom payment. This can lead to data loss, service disruption, financial loss, and reputation damage to an organization. Weak configuration among servers, applications, and unpatched software, can create security vulnerabilities. Attackers can exploit these weaknesses to gain unauthorized access, execute arbitrary code, or launch other attacks in the Systems/Application Domain. Insider threats come from authorized users with malicious intent. They abuse their privileges within the System/Application Domain nefariously. This includes unauthorized data access, data modification, or data exfiltration. Lack of a strong data encryption policy can result in eavesdropping on the network. Data should be encrypted in motion and at rest and used over secure means of communication.

The Payment Card Industry Data Security Standard (PCI DSS) outlines specific requirements and controls for securing servers, applications, and private data in the System/Application Domain. Organizations should review the following requirments that are particularly relevant. Requirement one, being to to install a firewall configuration to protect cardholder data. Firewalls should be configured to allow only necessary network traffic and restrict access to sensitive data. Requirement two, do not use vendor-supplied defaults for system passwords and other security parameters: This requirement focuses on the need to change default passwords to prevent unauthorized access. Strong password policies, multi-factor authentication, and regular password updates can be used to mitigate these risks. Requirement five states to protect all systems against malware and regularly update antivirus software. This requirement focuses on the importance of implementing a robust antivirus solution. Requirement six mentions to develop and maintain secure systems and applications. This requirement highlights the need for secure coding practices, vulnerability management, and regular patching to mitigate vulnerabilities in servers and applications within the System/Application Domain. Requirement ten mentions to monitor all access to network resources and cardholder data. This requirement focuses on implementing logging mechanisms and conducting regular monitoring to detect and respond to any unauthorized access or suspicious activities within the System/Application Domain.

In conclusion, securing the System/Application Domain within IT infrastructure is crucial to protect data and mitigate risks, threats, and vulnerabilities. Implementing proper security controls at the Internet ingress/egress point is beneficial in preventing unauthorized access, malware attacks, weak configurations, insider threats, and data breaches. By adhering to the requirements of the PCI DSS, organizations can establish a strong security posture for their servers, applications, and stored personal privacy data. This includes implementing firewalls, not using default passwords, protecting against malware, secure development, and logging access to data. By following these requirements organizations can stay vigilant in maintaining a secure System/Application Domain.

**References:**

Chhay, A. (2021, October 21). Cybersecurity Awareness: Default Passwords. Lawrence Berkeley National Laboratory. Retrieved from https://it.lbl.gov/cybersecurity-awareness-default-passwords/

Fortinet. (n.d.). Data Egress. Fortinet Cyber Glossary. Retrieved from https://www.fortinet.com/resources/cyberglossary/data-egress

PCI Security Standards Council. (2018). PCI DSS Quick Reference Guide, Version 3.2.1. Retrieved from https://listings.pcisecuritystandards.org/documents/PCI\_DSS-QRG-v3\_2\_1.pdf

Muhammad, H. (2023, June 16). SSH vs. VPN: What's the Difference and Which One Should You Use? PureVPN Blog. Retrieved from https://www.purevpn.com/blog/ssh-vs-vpn/

Whitman, M. E., Mattord, H. J., Weiss, M., & Solomon, M. G. (2016). Principles of Information Security (2nd ed.). Jones and Bartlett Learning. ISBN 978-1284090703.