Passive VA Risk Mitigation

Risk Mitigation Strategies

Addressing the vulnerabilities identified through passive vulnerability assessment is crucial for improving an organization's security posture. Here are specific mitigation strategies for each of the key risk areas:

1. Mitigating CVEs and Outdated Software/Services Risks

- Implement a robust patch management process to ensure timely updates of all software and services.
- Establish a regular vulnerability scanning routine to identify new CVEs quickly.
- Create and maintain an up-to-date inventory of all software and their versions used in the organization.
- Implement a software end-of-life policy to plan for replacement of outdated or unsupported software.
- Use virtual patching or web application firewalls (WAF) as temporary measures while planning updates.
- Conduct regular security assessments to identify and prioritize vulnerabilities for remediation.

2. Mitigating Risks from Open Ports and Exposed Services

- Implement the principle of least privilege by closing all unnecessary ports and services.
- Use firewalls and access control lists (ACLs) to restrict access to necessary ports and services.
- Regularly audit open ports and exposed services to ensure they are still required and secure.
- Implement network segmentation to isolate critical services from public-facing networks.
- Use strong authentication mechanisms, such as multi-factor authentication, for accessing exposed services.

- Employ intrusion detection and prevention systems (IDS/IPS) to monitor and protect exposed services.
- Implement proper logging and monitoring for all exposed services to detect potential security incidents quickly.

3. Mitigating Shadow IT and Rogue Asset Risks

- Develop and enforce clear policies on the use of unauthorized software, services, and devices.
- Implement network access control (NAC) solutions to detect and manage unknown devices connecting to the network.
- Conduct regular network scans and asset discovery to identify unknown or unauthorized assets.
- Use cloud access security brokers (CASBs) to discover and control the use of shadow IT in cloud services.
- Implement data loss prevention (DLP) solutions to monitor and control data flow to unauthorized services.
- Provide approved alternatives to common shadow IT solutions to meet employee needs securely.
- Conduct regular security awareness training to educate employees about the risks of shadow IT and the importance of following security policies.
- Establish a process for employees to request and rapidly receive approval for new software or services they need.

By implementing these mitigation strategies, organizations can significantly reduce the risks identified through passive vulnerability assessment. It's important to note that security is an ongoing process, and these strategies should be regularly reviewed and updated to address new and evolving threats.

Revision #2
Created 19 September 2024 09:15:14 by Admin
Updated 19 September 2024 09:19:02 by Admin