Top 10 Cybersecurity Misconfigurations From CISA/NSA

The Cybersecurity and Infrastructure Agency (CISA) and the National Security Agency (NSA) have teamed up to release a comprehensive joint cybersecurity advisory, shedding light on the most prevalent cybersecurity misconfigurations that tend to plague large organizations. This article delves deeper into these common misconfigurations and provides a detailed understanding of each, along with recommended mitigation strategies for your organization to implement.

Top 10 Misconfigurations

1. **Default software configurations:** Default configurations can have vulnerabilities that hackers can exploit. Default credentials, permissions and settings can give unauthorized access. Hackers can also exploit overly permissive access controls and vulnerable configurations that are in place by default.

   To avoid security risks, modify the default configurations of apps and appliances before deploying them. Change or disable default usernames/passwords during installation, secure ADCS configurations, review permissions on templates and assess LLMNR/NetBIOS necessity.

2. **Improper user/administrator privilege separation:** Assigning multiple roles to a single account by administrators can create a situation where a single compromised account can gain access to a wide range of devices and services without being detected.

   To minimize cybersecurity risks, implement authentication, authorization and accounting systems. Audit user accounts regularly and remove any unnecessary ones. Limit privileged account use and the number of administrator users. Restrict domain users in local admin groups, run non-admin accounts for daemonized apps and configure service accounts with minimal necessary permissions.

3. **Insufficient internal network monitoring:** Inadequate configurations for host and network sensors can lead to undetected compromises. They also hamper the collection of data needed for developing baselines and detecting suspicious activity in a timely manner.

   To address this, it's vital to establish baselines of applications and services; routinely audit their access and use, especially for administrative activities; and develop a baseline representing an organization's normal traffic activity, network performance, host application activity and user behavior. Use auditing tools that can detect privilege and service abuse opportunities and implement a security information and event management system.

4. **Lack of network segmentation:** The absence of network segmentation security allows malicious actors to move laterally across various systems without any security boundaries. This poses a significant risk as businesses become more vulnerable to ransomware attacks and post-exploitation techniques.

   Mitigation strategies include implementing next-generation firewalls that perform deep packet filtering, stateful inspection and application-level packet inspection. Engineer network segments to isolate critical systems, functions and resources. Implement separate virtual private

SCS AGENCY INSURANCE

cloud instances to isolate essential cloud systems.

5. **Poor patch management:** Keeping software up to date is critical to prevent security vulnerabilities. To do this, implement an efficient patch management process that includes regular updates for operating systems, browsers and software. Automate the update process as much as possible and rely on vendor-provided updates. Segment networks to limit exposure of vulnerable systems and discontinue the use of unsupported hardware and software. Finally, patch firmware to prevent known vulnerabilities from being exploited.
6. **The bypassing of system access controls:** Malicious actors can gain unauthorized access to a system by exploiting alternate authentication methods like pass-the-hash (PtH). It is important to restrict the use of the same credentials across different systems to prevent such unauthorized access and limit the malicious actors' ability to move around and cause damage. To further mitigate the risk, enabling PtH mitigations and denying domain users from being part of the local administrator group on multiple systems can be helpful.
7. **Weak or misconfigured multifactor authentication (MFA):** Some networks require accounts to use smart cards or tokens. However, multifactor requirements can be misconfigured, which may allow the password hashes associated with these accounts to never change. This can pose a significant risk, as password hashes can be used indefinitely as long as the account remains active. In addition, certain types of MFA methods can be vulnerable to various types of attacks.

   To mitigate this risk in Windows environments, it's recommended to disable legacy authentication protocols and instead enforce phishing-resistant MFA through modern open standards. This approach can help ensure your network remains secure and protected from potential threats.
8. **Insufficient access control lists (ACLs) on network shares and services:** Data shares and repositories are often targeted by malicious actors. Improperly configured ACLs can allow unauthorized users to access sensitive or administrative data on shared drives.

   To prevent this, organizations should ensure secure configurations for all storage devices and network shares, allowing access only to authorized users. They should also apply the principle of least privilege to important information resources; set restrictive permissions on files and directories; and enable the Windows Group Policy security setting "Do Not Allow Anonymous Enumeration of Security Account Manager (SAM) Accounts and Shares" to limit users who can enumerate network shares. It is also crucial to apply restrictive permissions on files and folders containing sensitive private keys.
9. **Poor credential hygiene:** To prevent cyber-attacks, it's crucial to maintain good credential hygiene. Follow the National Institute of Standards and Technology's guidelines for password policies, use strong passwords, avoid reusing passwords across systems, and use strong passphrases for private keys and store hashed passwords. Implement a review process to look for cleartext credentials and consider group-managed service accounts or third-party software for secure password storage.
10. **Unrestricted code execution:** Unverified programs can enable malicious actors to run harmful payloads on hosts. To prevent this, organizations should restrict applications downloaded from untrusted sources, use application control tools and constrain scripting languages. Regular analysis of border and host-level protections is necessary to ensure their continued effectiveness in blocking malware.

Additional Mitigation Strategies

It is highly recommended by CISA and NSA that organizations continuously exercise, test and validate

their security programs in a production environment. Regular testing ensures that the security measures remain effective and adaptable to new threats. Additionally, organizations can learn from the vulnerabilities and shortcomings experienced by others and swiftly implement necessary mitigation measures to safeguard their networks, sensitive information and critical missions.

Conclusion

The joint advisory from CISA and NSA provides invaluable insights into the most common cybersecurity misconfigurations and offers detailed strategies for mitigating these risks. By diligently addressing these issues and following the recommended best practices, organizations can significantly enhance their cybersecurity posture and protect against a wide range of threats.

For more risk management guidance, contact us today.