MSP's Blueprint for Passkey Security

WHY PASSKEYS AREN'T THE "SILVER BULLET"

Passkeys are being marketed as the ultimate solution to replace passwords, offering better security and convenience. But here's what no one is telling you—if passkeys aren't properly secured, they can be just as vulnerable as passwords, if not worse. A single misconfiguration can expose authentication tokens, allowing hackers to bypass security controls and gain full, undetected access to critical systems. We've seen it happen in real-world attacks, and we've proven it in every analysis we conduct. Passkeys aren't a security silver bullet. If you don't lock them down before deployment, they could be your biggest security risk.

STEP-BY-STEP GUIDE TO HARDENING PASSKEYS

STEP 1: IMPLEMENT ROBUST MFA CONFIGURATION

Many assume passkeys eliminate the need for multi-factor authentication (MFA). That's a dangerous mistake. Without strong MFA policies, a compromised passkey could give a hacker unrestricted access.

Action Items:

- Enforce hardware-bound passkeys (YubiKeys, biometric-secured TPM storage) instead of software-only passkeys.
- Require additional MFA only for cloud-synced passkeys stored in iCloud, Google, or Microsoft environments.
- Disable fallback authentication methods like email-based account recovery, which attackers exploit to bypass MFA.

Outcome:

Even if a hacker gains access to a passkey, they'll still be blocked without the second authentication factor.

STEP 2: VALIDATE IDENTITY PROVIDER (IDP) CONFIGURATIONS

Your passkey security is only as strong as your identity provider (IdP). Weak configurations in Azure AD, Okta, or other IdPs can expose tokens to theft.

Action Items:

- Disable browser-stored passkeys unless secured by enterprise policies
- Restrict token lifetime to minimize the risk of long-lived session abuse.
- Ensure tokens are stored securely, preventing extraction from memory or disk.
- Block token replay attacks by enforcing anti-replay measures.

Outcome:

Hardened authentication settings that reduce the risk of passkey-based exploits.

GALACTIC ADVISORS

MSP's Blueprint for Passkey Security (Continued)

STEP 3: ENABLE DEVICE-BASED SECURITY

If an attacker gains access to a device storing passkeys, they own the keys to the kingdom. Secure every device that interacts with passkeys.

Action Items:

- Require full-disk encryption to prevent unauthorized access to locally stored passkeys.
- Deploy endpoint detection and response (EDR) solutions to monitor suspicious activity.
- Enforce secure boot and hardware-based storage (e.g., TPM 2.0) for key storage.
- Implement Zero Trust security principles to restrict access based on identity, device health, and behavior, ensuring only verified users and devices can interact with passkeys.
- Enable application allowlisting to prevent unauthorized applications and scripts from running, blocking malware that could attempt to steal passkey tokens.
- Use privilege management tools to restrict administrative rights, reducing the risk of token theft through malicious code execution.

Outcome:

Passkeys remain protected, even if a device is compromised.

STEP 4: TURN OFF LEGACY AUTHENTICATION METHODS

If passwords are still enabled as a backup authentication method, passkeys lose their value. Hackers will simply bypass them using stolen credentials.

Action Items:

- Disable NTLM authentication to eliminate outdated and insecure authentication protocols.
- Turn off password-based authentication entirely, ensuring passkeys are the sole method of access.
- Block legacy authentication protocols which don't support modern security standards.
- POP3, IMAP, and SMTP – Email authentication methods that don't support modern security controls like MFA.
- SMBv1 & SMBv2 – Outdated file-sharing protocols vulnerable to exploits like EternalBlue.
- TLS 1.0 and TLS 1.1 – Deprecated encryption standards with known vulnerabilities; enforce TLS 1.2+ instead.
- LDAP (Unencrypted) – Upgrade to LDAPS (LDAP over TLS) to prevent credential interception.

Outcome:

A truly passwordless environment where attackers can't bypass security measures.

STEP 5: AUDIT ACCESS LOGS REGULARLY

Attackers don't always strike immediately. Many will test stolen passkeys and tokens over time, looking for weaknesses. If you're not watching, you won't know until it's too late.

Action Items:

- Monitor for repeated token refresh requests, a red flag that an attacker is testing stolen credentials.
- Look for logins from new or unexpected devices, especially in high-risk geographies.
- Set up automated alerts for unusual authentication patterns.

Outcome:

Proactive threat detection that catches attackers before they can cause damage.

MSP's Blueprint for Passkey Security (Continued)

STEP 6: EDUCATE CLIENTS ABOUT TOKEN SAFETY

Passkeys eliminate phishing attacks—unless users fall for new tricks. If they don't understand how token theft works, they'll make mistakes that put your security at risk.

Action Items:

- Teach users that tokens can still be stolen through device compromise or man-in-the-middle attacks.
- Train employees to never share authentication tokens, just like they wouldn't share a password.
- Establish a policy for reporting lost or stolen devices immediately.

Outcome:

A security-aware workforce that actively protects passkeys from compromise.

STEP 7: LOCK DOWN TPM CONFIGURATIONS

Trusted Platform Module (TPM) is often used to store passkeys, but default configurations can leave them vulnerable.

Action Items:

- Ensure TPM 2.0 is enabled and properly configured on all devices.
- Disable weak cryptographic algorithms that could allow brute-force attacks.
- Restrict access to TPM-stored credentials to prevent unauthorized key extraction.
- Disable local TPM key export to prevent attackers from moving passkeys off-device.

Outcome:

Secure key storage that prevents attackers from stealing passkeys directly from hardware.

FINAL THOUGHTS

Passkeys aren't a plug-and-play security solution. If you don't secure them properly, they become an open door for attackers—one that's harder to detect than a compromised password.

MSPs must take the lead in securing passkeys before deployment. Lock down device security, enforce strong authentication policies, eliminate legacy authentication, and continuously monitor for threats.

If you're not securing passkeys properly, you're not securing anything at all. The question is: **will you get ahead of the threats, or will hackers get there first?**