Mitigation Plan for Stolen Credentials

When our scanning process identifies stolen credentials associated with your organization in leaked databases, it's crucial to act quickly and implement a comprehensive mitigation strategy. Here's a detailed plan to address this security risk:

Immediate Actions

1. **Password Resets**
   - Force immediate password changes for all affected accounts.
   - Ensure new passwords meet strong complexity requirements.
2. **Account Lockdowns**
   - Temporarily lock affected accounts until the user verifies their identity.
   - Implement additional authentication steps for these accounts.
3. **Multi-Factor Authentication (MFA)**
   - Enable MFA for all affected accounts immediately.
   - Prioritize rolling out MFA across the entire organization if not already implemented.
4. **Access Review**
   - Conduct an immediate review of access logs for affected accounts.
   - Look for any suspicious activities or unauthorized access attempts.
5. **Notification and Education**
   - Notify affected users about the credential leak.
   - Provide clear instructions on how to secure their accounts.
   - Educate users on the risks of password reuse across multiple sites.

Short-term Strategies

6. **Credential Screening**
   - Implement a system to screen new passwords against lists of known compromised passwords.
   - Prevent users from setting passwords that have been previously exposed in leaks.
7. **Enhanced Monitoring**
   - Increase monitoring of affected accounts for a set period (e.g., 30-60 days).

- Set up alerts for unusual login patterns or access attempts.

8. **Phishing Awareness**
   - Conduct a phishing awareness campaign, as leaked email addresses may be targeted.
   - Provide training on how to identify and report suspicious emails.
9. **VPN and Remote Access Review**
   - Review and tighten security for VPN and remote access systems.
   - Implement or enhance network segmentation to limit potential damage from compromised accounts.

Long-term Strategies

10. **Password Policy Enhancement**
    - Review and strengthen organizational password policies.
    - Consider implementing passphrases instead of complex passwords.
    - Enforce regular password changes, but balance this with usability to prevent password fatigue.
11. **Single Sign-On (SSO) Implementation**
    - Consider implementing SSO to reduce the number of credentials users need to manage.
    - Ensure the SSO solution itself is highly secure and supports strong authentication methods.
12. **Passwordless Authentication**
    - Explore and implement passwordless authentication methods where possible (e.g., biometrics, security keys).
13. **Continuous Monitoring for Credential Leaks**
    - Implement a continuous monitoring solution for detecting newly leaked credentials.
    - Set up automated alerts and response procedures for future credential leaks.

By implementing these mitigation strategies, organizations can significantly reduce the risks associated with stolen credentials, enhance overall security posture, and better protect sensitive information from unauthorized access. Regular review and updating of these practices will help maintain robust security in the face of evolving threats.

Revision #1
Created 19 September 2024 11:08:08 by Admin
Updated 19 September 2024 11:08:41 by Admin