Project 8 - Cyber Best Practices

By Evelyn Wolfe

Table of Contents

Executive Summary

As cyber threats continue to evolve, ensuring the confidentiality, integrity, and availability (CIA) of our company's data and systems remains our top priority.After reviewing our current security posture, we have identified key areas of improvement focusing on secure authentication through strong password policies, encrypted email communication, VPN security, and storage encryption. These enhancements align with NIST and Microsoft best practices to strengthen our defenses against phishing, data breaches, and unauthorized access. WIth the revamp of our Cyber Security Policies and Best Practices

To prevent unauthorized access, we will implement a strong password policy that aligns with NIST 800-63B, enforcing a minimum of 10-16 characters with a mix of uppercase/lowercase letters, numbers, and special characters. Additionally, we will prohibit commonly used or compromised passwords and integrate Multi-Factor Authentication (MFA) across privileged accounts, remote and hybrid users.

To further protect against email spoofing and phishing threats, we will implement Secure/Multipurpose Internet Mail Extensions (S/MIME) within Microsoft Exchange Online to enable email encryption and digital signatures. This ensures message authenticity and integrity, reducing the risk of business email compromise. Employee training will also be introduced to help recognize signed vs unsigned emails, further strengthening security awareness.

As a part of our remote access security strategy, we will enhance our VPN infrastructure with two options:

- SSL VPN - Encrypting a web session for employees accessing corporate resources via a secure browser
- IPSec VPN - a full encrypted connection for remote users with company-issued devices, ensuring a seamless and secure connection to internal systems

Furthering the security, MFA will be mandatory for all VPN access, adding extra layers of identity verification to prevent unauthorized remote logins.

Finally, to safeguard sensitive company data, we will enforce full-disk encryption on laptops and desktops using Microsoft Bitlocker. Encryption keys will be securely stored in Azure Active Directory or a new resource Azure Key Vault. For removable storage, only FIPS-certified encrypted drives (e.g. Kingston IronKey) will be approved for use, with policies restricting unauthorized flash drives. Mobile Device Management (MDM) via Microsoft Intune will be implemented to enforce work profile encryption, biometric authentication, and remote wipe capabilities, ensuring corporate data remains protected even if a device is lost or compromised.

Implementing these security measures will significantly reduce risk exposure, ensure compliance with industry standards, and protect critical business assets from cyber threat. The next phase involves finalizing policy enforcement, employee training, and a full-scale deployment across the organization.

Security Policy, Techniques, and Approach Review

Password Policies

Implementing a strong password policy is essential to preventing attackers from exploiting weak credentials to gain unauthorized access to our systems. After reviewing our current policies, we have identified areas for improvement that align with National Institute of Standards and Technology (NIST 800-63B, 2023) recommendations. While in the NIST Special Publication 800-63B does suggest a minimum password length of 8 characters, our goal is to enforce a minimum of 10 characters, with an optimal range of 12 to 16 characters. These passwords must include a combination of uppercase and lowercase characters, numbers and special characters to enhance security.

To further strengthen enforcement, we encourage the use of passphrases rather than simple passwords. For example, a weak passphrase like “Chicken123” would not meet our requirements. However, a stronger version that incorporates complexity, such as “cH!cK!n_123”, aligns with our updated standards. Additionally, we will move forward with restricting the use of common dictionary words and preventing passwords that are easily guessed or susceptible to brute-force attacks, including newer AI-driven password cracking algorithms.

Furthermore, we will blacklist known compromised passwords, ensuring that our users cannot select credentials that have already been exposed in data breaches. Lastly, we will implement password expiration policies while preventing users from reusing previous passwords. While NIST does not strictly require password expiration, implementing this measure as a best practice further protects our assets by reducing the risk of long-term credential exposure.

Multi-Factor Authentication

While there is no exact publication outlining a policy framework specifically for Multi-Factor Authentication (MFA) under NIST, guidance on its implementation can be found in NIST Special Publication 800-63-3, 800-63B, and the NIST MFA Small Business Cybersecurity Corner bulletin. Based on these resources, the following recommendations are proposed for the company cyber security policy moving forward.

All Privileged Access Accounts must use MFA, ensuring an additional layer of security for sensitive accounts. Similarly, remote and hybrid users logging in from a non-company site will also be required to authenticate using MFA. To Strengthen this security measure, MFA should be application-based, utilizing software such as Google Authenticator, Microsoft Authenticator, or Duo Authenticator rather than relying on SMS-based authentication. This approach mitigates the risk of SIM swapping or phone service hijacking, which can compromise text message based authentication codes. Additionally adaptive MFA should be implemented to detect and prevent login attempts from authorized locations. For example, if a user is typically based in North America but an authentication attempt is made in Brazil, the system should flag or block the login attempt to prevent potential account compromise.

Secure Email With Personal Certificate - S/MIME

After reviewing our company's current email security posture, we have identified the need to incorporate Secure/Multipurpose Internet Mail Extension (S/MIME) to enhance protection against cyber threats. S/MIME will enable email encryption and digital signature, ensuring the Confidentiality, Integrity, and Availability (CIA) of our communications. By integrating S/MIME into Microsoft Exchange Online, we can bolster security against phishing and email spoofing through the use of internal communication certificates. Additionally, suers training will be critical in helping employees recognize the difference between signed and unsigned email to help reduce the risk of falling victim to malicious email attacks. Proper implementation and education on S/MIME will strengthen our company's defenses against evolving cyber threats.

Encryption of VPN

After reviewing our current VPN tunnel system, the next phase of our policy overhaul will focus on implementing a more robust, encrypted secure Virtual Private Network (VPN.) There is a value of utilizing two different types of VPN solutions, each caters a distinct use case.

A Secure Sockets Layer (SSL) VPN encrypts a web session, making it an ideal solution for remote employees who only require access to company resources via a secure browser. This method ensures that users can securely interact with internal systems without exposing sensitive data over an unprotected network.

On the other hand, Internet Protocol Security (IPSec) VPN is designed for the employee working remotely on a company-issued device who requires direct access to the internal network. By encrypting the entire network tunnel between the remote device and the company portal, IPSec VPN ensures that all security measures function as if they user was physically onsite. This approach is not only an amazing solution for individuals who are remote, it also can serve as a scalable solution for securely connecting branch offices to main corporate networks.

Finally, tying this back to Multi-factor Authentication (MFA,) establishing a secure VPN connection must also require MFA authentication as an added layer of security to protect against unauthorized access.

Encryption of Storage

The final topic to address is encryption of storage devices, including laptops, desktops, flash drives and mobile devices. While we cannot entirely prevent a device from being lost or stolen, implementing encryption with a key stored on company assets ensures that sensitive data remains protected and inaccessible to unauthorized individuals.

For laptops and desktops, Microsoft provides a built-in module called Bitlocker, which enables full-disk encryption and allows recovery keys to be sorted with in Azure Active Directory (AAD.) This setup enforces pre-boot authentication adding an additional layer of security for high-risk environments. For enhanced confidentiality, instead of storing encryption keys in AAD, the company can opt for Azure Key Vault which offers a centralized and secure solution for managing encryption keys.

Regarding flash drives, usage should be restricted unless explicitly approved. When portable storage is necessary, only FIPS-certified encrypted drives, such as Kingston Ironkey, will be utilized. These devices offer multiple recovery options including Multi-Password Recovery, Passphrase Mode, and a read-only mode, making them ideal for securely sharing data with team members. While other secure storage solutions exist, Ironkey remains a top recommendation for encrypted flash drives.

Finally, encryption policies for mobile devices must also be carefully structured. Given the widespread use of smartphones and tables, monitoring non-encrypted personal devices should not be considered a viable security approach. Instead, the best practice is to enforce segregation between work and personal profiles by encrypting only the work profile. Mobile Device Management (MDM) solutions such as Microsoft Intune enables this level of security, allowing the company to enforce encryption policies on non-corporate devices. To further secure data, mobile devices must require biometric authentication and/or a PIN. Additionally in the event of a lost or compromised device, a remote wipe can be initiated, ensuring that work-related data is erased while leaving persona data intact.

Citations

NIST Special Publication 800-63B. (n.d.).
https://pages.nist.gov/800-63-3/sp800-63b.html
NIST Special Publication 800-63-3. (n.d.).
https://pages.nist.gov/800-63-3/sp800-63-3.html
Multi-Factor Authentication | NIST. (2024, March 12). NIST.
https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication

SMIME:
Ashalyengar, Chrisda, PriyaRakshith, KCCross (2024, February 22). *S/MIME in exchange online.* Microsoft Learn.
https://learn.microsoft.com/en-us/exchange/security-and-compliance/smime-exo/smime-exo
Chernick, C. M. & National Institute of Standards and Technology. (2002). *Federal S/MIME V3 Client Profile.* National Institute of Standards and Technology.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-49.pdf

VPN:
IPSEC VPNs vs SSL VPNs. (n.d.). Cloudflare. Retrieved February 4, 2025, from
https://www.cloudflare.com/learning/network-layer/ipsec-vs-ssl-vpn/

Azure Key Vault:
Msmbaldwin, Jackrichins, Wharvex, Batamig, Jlichwa, Sebansal, V-kents, JamesTran-MSFT, Rolyon, Manishk2018. (2024, September 11). *Azure Key Vault Overview - Azure Key Vault.* Microsoft Learn.
https://learn.microsoft.com/en-us/azure/key-vault/general/overview

Kingston Ironkey
Kingston IronKey Vault Privacy 50 Series. (n.d.-b). Kingston Technology Company.
https://www.kingston.com/en/usb-flash-drives/ironkey-vp50-encrypted

Intune:
MandiOhlinger. (2024, May 21). *What is Microsoft Intune.* Microsoft Learn.
https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune