Project Encryption

Jasraj

Executive Summary:

As the recently appointed Cyber Security manager, I have thoroughly analyzed our organization's security practices and identified crucial areas that require immediate attention. This report presents key techniques and approaches to significantly enhance the protection of our company's employees and sensitive information. Implementing these fundamental security practices will create a robust security posture, shielding our technological infrastructure and digital assets from potential cyber threats.

1. **Strong Password:**

Password security is the combination of policies, processes, and technologies that make passwords and authentication methods more secure. It's all about knowing how to protect passwords. A password itself is a type of memorized secret authenticator. Basically, it's something that only you should know that allows you to authenticate yourself to third parties. (Crane, 2023) It acts as a critical barrier, thwarting attackers from easily guessing or cracking passwords. To ensure strong passwords:

- Encourage employees to create passwords with at least 12 characters, comprising upper and lower case letters, numbers, and special characters.
- Discourage the use of the same password across multiple accounts or services to minimize the risk of widespread breaches. (Cheatsheet OWASP, n.d.).

Implementing a strong password policy and educating employees on password hygiene will significantly reduce the likelihood of successful brute force attacks or password guessing.

2. **Password Expiration Policy:**

In addition to strong passwords, a password expiration policy is essential to minimize the impact of compromised credentials. Regularly changing passwords reduces the window of opportunity for cybercriminals to exploit stolen passwords effectively. However, the expiration period should strike a balance between security and usability to avoid causing frustration among employees. As the admin, you can make user passwords expire after a certain number of days, or set passwords to never expire. By default, passwords are set to never expire for your organization. (Kwekuako, 2023)

3. **Multi-Factor Authentication (MFA):**

Multifactor authentication (MFA) is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login

or other transaction. Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods. (Shacklett & Contributor, 2021) MFA requires employees to provide two or more forms of verification before gaining access to their accounts. Commonly used factors include:

- Something You Know: Password or PIN.
- Something You Have: A smartphone, hardware token, or smart card.
- Something You Are: Biometric features like fingerprint or facial recognition. (Cheatsheet OWASP, n.d.).

Implementing MFA can prevent unauthorized access, even if passwords are compromised, and is highly effective in thwarting phishing attempts and brute force attacks.

4. **Secure Email with Personal Certificate:**

Email is a primary communication medium, and securing email communication is crucial to prevent unauthorized access and data interception. Secure email solutions utilizing personal certificates enable end-to-end encryption of emails, ensuring that only intended recipients can read the content. Moreover, digital signatures provide authentication and integrity verification, protecting against email spoofing and phishing attacks.

Email encryption helps to protect personal information from hackers by only permitting certain users to access and read your emails. There are several methods of email encryption depending on the level of security—and convenience—you require. For example, you could download or purchase extra software that will plug in to your current email client. Or, you could install an email certificate like PGP (Pretty Good Privacy), which allows your employees to share a public key with anyone who wants to send them an email and use a private key to decrypt any emails they receive. Another simple solution is to use a third-party encrypted email service. (The Small Business Guide to Secure Email, n.d.)

5. **VPN IPSec on Laptops:**

As employees increasingly work remotely or travel, securing their network connections becomes imperative. VPN (Virtual Private Network) IPSec on laptops establishes an encrypted tunnel between the employee's device and our corporate network. This ensures that data transmitted between the laptop and the internal network remains secure, even when using public or unsecured Wi-Fi networks. (Cheatsheet OWASP, n.d.).

Enforcing the use of VPN IPSec on laptops will prevent unauthorized interception of sensitive data and maintain the confidentiality of our corporate communications.

6. **Encrypted Hard and Flash Disks for Portable/Mobile Devices:**

Mobile devices like laptops and smartphones are susceptible to loss or theft, posing significant security risks. To mitigate these risks, we must implement encryption on hard and flash disks to protect the data stored on these devices. Encrypted data remains secure even if the device falls into unauthorized hands.

You have four main options when it comes to encrypting the data on your USB peripherals. You can:

- Encrypt each document individually using document processing programs
- Encrypt the entire external hard drive using an encryption system built into your device's operating system
- Use a third-party encryption service to encrypt files or your hard drive
- Use a hardware-encrypted external hard drive

Conclusion:

In conclusion, adopting basic security approaches and practices, such as strong passwords, password expiration policy, MFA, secure email with personal certificates, VPN IPSec on laptops, and encrypted portable/mobile devices, will greatly enhance the protection of our company's employees and valuable information. Educating employees about these practices and enforcing them through well-defined policies will create a robust security culture within the organization. As the Cyber Security manager, I recommend continuous monitoring, regular security awareness training, and proactive threat hunting to stay ahead of emerging cyber threats and ensure the long-term security of our company's technological infrastructure and digital data. (Cheatsheet OWASP, n.d.)

I am confident that implementing these measures will strengthen our defenses and achieve the goal of safeguarding our employees and information from potential Cyber Security breaches. I am available to provide further explanations and collaborate with all the tech teams to implement these security practices effectively.

References:

Cryptography Cheat Sheet For Beginners - Cyber Coastal. (2021, April 8). Cyber Coastal. https://cybercoastal.com/cryptography-cheat-sheet-for-beginners/

Cryptographic Storage - OWASP Cheat Sheet Series. (n.d.). https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html

Shacklett, M. E., & Contributor, T. (2021). What is multifactor authentication and how does it work? *Security*. https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

Crane, C. (2023, March 27). *Password security: What your organization needs to know*. Hashed Out by the SSL Store™. https://www.thesslstore.com/blog/password-security-what-your-organization-needs-to-know/

Team, P. (2022). How to secure data on your external hard drives and USB peripherals. *Proton*. https://proton.me/blog/usb-encryption

The small business guide to secure email. (n.d.). https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/the-small-business-guide-to-secure-email

Kwekuako. (2023, June 28). *Set the password expiration policy for your organization - Microsoft 365 admin*. Microsoft Learn. https://learn.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide