Enhancing Cyber Security to Protect Employees and Company Information

By: Mahad Mohamood

Executive Summary

As the new Cyber Security Manager, it's crucial to establish and enforce robust security practices to protect our company's data and employees. This report outlines key security measures essential for strengthening our defenses against cyber threats, ensuring both technical and non-technical stakeholders understand their importance.

1. Strong Passwords: Use complex passwords that include letters, numbers, and symbols. This makes it harder for hackers to guess or crack them.

2. Password Expiration: Regularly update passwords to limit the risk if they are compromised. Automate reminders for password changes to ensure compliance.

3. Multi-Factor Authentication (MFA): Add an extra layer of security by requiring additional verification (like a code sent to your phone) beyond just a password.

4. Secure Email: Use digital certificates to encrypt and verify emails, protecting sensitive information and reducing the risk of phishing.

5. VPN on Laptops: Use a VPN (Virtual Private Network) to encrypt internet connections, especially when working remotely, to keep data secure.

6. Encrypted Devices: Encrypt data on hard drives and flash drives to protect it if devices are lost or stolen.

Adopting these practices—strong passwords, regular password updates, MFA, encrypted email, VPNs, and encrypted devices—will significantly enhance our security measures. These steps are crucial for protecting our company's data and ensuring a secure working environment for all employees. Your active participation in implementing these practices is essential for maintaining robust cybersecurity defenses.

Introduction

In today’s digital world, safeguarding our company’s employees and sensitive information from cyber threats is of utmost importance.According to the National Institute of Standards and Technology (NIST, n.d.-a) a cyber threat is “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.” (para. 1).

As we advance in our commitment to securing our organization, it’s essential to understand and implement some fundamental security practices. This report explains basic yet crucial security measures that will significantly protect our company from potential cyber threats. The goal is to provide a clear understanding of these practices so that both technical and non-technical stakeholders can appreciate their importance and contribute to their implementation.

Strong Passwords

What Are Strong Passwords?

Strong passwords are complex combinations of letters (both uppercase and lowercase), numbers, and special characters. Unlike simple or common passwords, strong passwords are designed to be difficult for hackers to guess or crack. According to the National Institute of Standards and Technology (2017), “password length has been found to be a primary factor in characterizing password strength. Passwords that are too short yield to brute force attacks as well as to dictionary attacks.” (p.67).

Why Are They Important?

According to CISA, “Simple passwords, such as 12345, or common identifying information, like birthdays and pet names, are not safe for protecting important accounts holding personal information. Using an easy-to-guess password is like locking the door but leaving the key in the lock.” A strong password serves as the first line of defense against unauthorized access to our systems. Think of it like a lock on a door: a stronger lock makes it much harder for someone to break in.

How Do We Implement Strong Passwords?

- Set Requirements: We should ensure that passwords are at least 12 characters long and include a mix of letters, numbers, and symbols.

- Educate Employees: Provide training on how to create strong passwords and the importance of using unique passwords for different accounts.

Benefits:

- Reduces the likelihood of unauthorized access if a password is compromised.

- Enhances overall security by making it harder for cybercriminals to gain access.

Password Expiration Policy

What Is a Password Expiration Policy?

According to n-able, “password expiration policies regulate how frequently users must replace old passwords with new ones. Stakeholders use password management tools to set timeframes for password expiration, monitor the ages of passwords across organizational accounts, and streamline the process of alerting users when password expiration deadlines are approaching.” The idea is to minimize the risks if a password were to become known by an unauthorized person.

Why Is It Important?

Regularly changing passwords limits the time a compromised password can be used by a malicious actor. It’s like changing the keys to your home regularly to ensure that old keys can no longer open your door.

How Do We Implement a Password Expiration Policy?

- Automate Changes: Configure systems to automatically prompt users to update their passwords at set intervals.

- Communicate Clearly: Inform employees about why password changes are necessary and provide guidance on how to create new, secure passwords.

Benefits:

- Reduces the risk associated with compromised passwords.

- Encourages the use of up-to-date, more secure passwords.

Multi-Factor Authentication (MFA)

What Is Multi-Factor Authentication (MFA)?

According to the National Institute of Standards and Technology (NIST, n.d.-b) "Passwords alone are not effective in securing your most sensitive business assets, as they have become too easy for threat actors to access. MFA is an important security enhancement that requires a user to verify their identity by providing more than just a username and password."

MFA requires users to provide two or more forms of verification before gaining access to an account. These factors typically include something the user knows (like a password), something the user has (such as a smartphone or a security token), and something the user has (like a fingerprint or facial recognition).

Why Is MFA Important?

According to okta, "Cybercriminals have more than 15 billion stolen credentials to choose from. If they choose yours, they could take over your bank accounts, health care records, company secrets, and more. Multi-factor authentication is important, as it makes stealing your information harder for the average criminal."Even if a hacker manages to obtain a password, they would still need the additional verification factors to gain access, making it much harder for them to breach our systems.

How Do We Implement MFA?

- Deploy MFA Tools: Set up MFA for all critical systems and applications.

- Train Users: Educate employees on how to use MFA and its benefits.

Benefits:

- Provides an additional defense layer, making unauthorized access significantly more difficult.

- Protects against breaches even if passwords are compromised.

Secure Email with Personal Certificates

What Is Secure Email with Personal Certificates?

According to the University of Pittsburgh, “A digital certificate is a security tool that can be attached to an email message to verify that the sender of the message is who he or she claims to be and that the message has not been altered since it was sent. It can also be used to encrypt email messages.” Personal certificates are digital tools used to encrypt and sign emails, ensuring that only the intended recipient can read the message and verify the sender’s identity.

Why Is This Important?

According to the National Institute of Standards and Technology (2019), “the purpose of authenticating the sending domain is to guard against senders (both random and malicious actors) from spoofing another’s domain and initiating messages with bogus content, and against malicious actors from modifying message contents in transit.” (p. v). Securing email communication prevents sensitive information from being intercepted by unauthorized individuals. It also helps ensure that messages are coming from legitimate sources, reducing the risk of phishing attacks.

How Do We Implement Secure Email with Personal Certificates?

- Issue Certificates: Provide employees with personal certificates for encrypting their emails.

- Provide Training: Guide users on how to use these certificates and the benefits of encrypted email.

Benefits:

- Protects sensitive information during email transmission.

- Verifies the authenticity of email senders, reducing the risk of fraud.

VPN IPSec on Laptops

What Is a VPN IPSec?

According to the National Institute of Standards and Technology (2020), “Internet Protocol Security (IPsec) is a suite of open standards for ensuring private communications over public networks. It is the most common network layer security control, typically used to encrypt Internet Protocol (IP) traffic between hosts in a network and to create a virtual private network (VPN).”(p. v)

Why Is This Important?

A Virtual Private Network (VPN) using Internet Protocol Security (IPSec) encrypts data sent over the internet, protecting it from being accessed or tampered with by unauthorized parties.

According to Archon secure, “IPSec provides a comprehensive set of security features, including data encryption, data integrity verification, and authentication of communication endpoints. It ensures the confidentiality, integrity, and authenticity of data.” When employees work remotely or access company resources over public networks, VPN IPSec ensures that their data is secure and private. It’s like having a secure tunnel that keeps your information safe from prying eyes.

How Do We Implement VPN IPSec?

- Set Up VPNs: Install and configure VPN software on all company laptops.
- Enforce Use: Require employees to use the VPN for all remote connections to company systems.

Benefits:

- Secures data transmissions over potentially insecure networks.
- Protects against interception and unauthorized access.

Encrypted Hard Drives and Flash Disks

What Is Encryption for Hard Drives and Flash Disks?

According to the National Institute of Standards and Technology (2007), “ the primary security controls for restricting access to sensitive information stored on end user devices are encryption and authentication. Encryption can be applied granularly, such as to an individual file containing sensitive information, or broadly, such as encrypting all stored data. The appropriate encryption solution for a particular situation depends primarily upon the type of storage, the amount of information that needs to be protected, the environments where the storage will be located, and the threats that need to be mitigated.”

Furthermore, according to Cloudflare, “encryption is a way of scrambling data so that only authorized parties can understand the information.” Encryption involves converting data stored on hard drives and flash disks into a code that can only be deciphered with a specific key. This ensures that even if the device is lost or stolen, the data remains secure.

Why Is This Important?

According to IBM, “Encryption can protect data at rest, in transit and while being processed, regardless of whether the data is in a computer system on-premises or in the cloud.” Additionally, encrypted devices ensure that sensitive data remains protected, even if physical devices are compromised. It’s similar to locking your valuables in a safe so that only those with the key can access them.

How Do We Implement Encryption?

- Deploy Encryption Tools: Install encryption software on all portable devices used by employees.

- Create Policies: Develop guidelines for using encrypted devices and handling sensitive data.

Benefits:

- Safeguards data on mobile and portable devices.

- Reduces the risk of data breaches from lost or stolen hardware.

Conclusion

By implementing these essential security practices—strong passwords, password expiration policies, Multi-Factor Authentication (MFA), secure email with personal certificates, VPN IPSec, and encrypted portable devices—we can significantly enhance the protection of our employees and company information. These measures will fortify our defenses against cyber threats and ensure a secure working environment.

Your active participation in adopting and adhering to these practices is crucial. I look forward to discussing these recommendations further and answering any questions you may have.

References

1. National Institute of Standards and Technology. (n.d.-a). Cyber threat. National Institute of Standards and Technology. https://csrc.nist.gov/glossary/term/cyber_threat

2. National Institute of Standards and Technology. (2017). NIST special publication 800-63B: Digital identity guidelines - Authentication and lifecycle management. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

3. Cybersecurity & Infrastructure Security Agency. (n.d.). Use strong passwords. U.S. Department of Homeland Security. Retrieved August 19, 2024, from https://www.cisa.gov/secure-our-world/use-strong-passwords

4. N-able. (2020, September 8). Why password expiration policies matter. N-able. https://www.n-able.com/blog/why-password-expiration-policies-matter

5. National Institute of Standards and Technology. (n.d.-b). Multi-factor authentication. U.S. Department of Commerce. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication

6. Okta. (2024, June 20).Why Multi-Factor Authentication (MFA) Is Important Okta.https://www.okta.com/identity-101/why-mfa-is-everywhere/

7. University of Pittsburgh.Using Digital Certificates to Encrypt Email Messages. University of Pittsburgh. https://services.pitt.edu/TDClient/33/Portal/KB/ArticleDet?ID=150

8. National Institute of Standards and Technology. (2019). NIST special publication 800-177 Revision 1: Trustworthy email. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf

9. National Institute of Standards and Technology. (2020). NIST special publication 800-77 Revision 1: Guide to IPsec VPNs. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf

10. Archon Secure. (n.d.). What is an IPSec tunnel? An inside look. Archon Secure. https://www.archonsecure.com/blog/ipsec-tunnel-technology

11. National Institute of Standards and Technology. (2007). Guide to storage encryption technologies for end user devices. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

12. Cloudflare. (n.d.). What is encryption? Cloudflare. https://www.cloudflare.com/learning/ssl/what-is-encryption/

13. IBM. What is encryption? IBM. https://www.ibm.com/topics/encryption