Project
Week 7 day 5
Submitted by Navneet kaur

Report on Basic Security Approaches to Protect Company Employees and Information
Executive Summary:

Executive Summary: In today's digital landscape, ensuring the security of company employees and information is paramount to maintaining a robust technological infrastructure and safeguarding sensitive data. As the Cyber Security Analyst, I have reviewed the company's current security policy and identified several key techniques and approaches that can significantly enhance the protection of employees and information against potential cyber threats. This report outlines the importance and benefits of implementing strong passwords, a password expiration policy, Multi-Factor Authentication (MFA), secure email with personal certificates, VPN IPSec on laptops, and encrypted hard and flash disks for portable/mobile devices. These strategies serve as essential building blocks to fortify our cyber defense and ensure the integrity, confidentiality, and availability of company assets.

1. **Strong Password**:

A strong password is the first line of defense against unauthorized access to company systems and accounts. It is crucial to educate employees about creating complex passwords that combine a mix of uppercase and lowercase letters, numbers, and special characters. Utilizing passphrase techniques can also enhance password strength. By enforcing strong password requirements, we reduce the risk of brute-force attacks and unauthorized access.

2. Password Expiration Policy:

Regularly changing passwords is an essential practice to minimize the potential impact of compromised credentials. Implementing a password expiration policy ensures that passwords are regularly updated, reducing the window of opportunity for attackers. By setting a reasonable password expiration interval, such as every 60 to 90 days, we reduce the risk of unauthorized access through the exploitation of stale passwords.

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

MFA is a highly effective technique that adds an extra layer of security to the authentication process. By requiring employees to provide multiple forms of verification (e.g., password and a unique code from a mobile app), we significantly reduce the risk of unauthorized access, even if a password is compromised. MFA enhances security by confirming the legitimacy of users attempting to access company resources.

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

Email is a common vector for cyberattacks, including phishing and malware distribution. Implementing secure email with personal certificates helps ensure the authenticity and confidentiality of email communications. Personal certificates digitally sign emails, verifying the sender's identity, and can encrypt the content to prevent unauthorized interception. This approach reduces the risk of email-based attacks and enhances the overall security of sensitive information.

5. **VPN IPSec on Laptops:**

Virtual Private Networks (VPNs) with IPSec encryption provide a secure channel for remote employees to access the company's network. By requiring employees to connect through a VPN, we encrypt data transmitted between remote devices and our internal network, safeguarding against eavesdropping and unauthorized access. This approach is especially critical for protecting sensitive data when accessing company resources over public networks.

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

Company-owned portable and mobile devices are susceptible to loss or theft, potentially exposing sensitive information. Encrypting hard and flash disks on these devices ensures that even if they fall into the wrong hands, the data remains unreadable without the decryption key. This approach safeguards company information from unauthorized access and data breaches resulting from physical device compromise.

Here are some cryptographic tools

AES (Advanced Encryption Standard): AES is a symmetric encryption algorithm that has become the de facto standard for encrypting sensitive data. It offers strong security and efficiency and is used in various applications, including secure communication and data encryption.

RSA (Rivest-Shamir-Adleman): RSA is a widely used asymmetric encryption algorithm that enables secure data transmission and digital signatures. It's a cornerstone of public-key cryptography.

SHA-256 (Secure Hash Algorithm 256-bit): Part of the SHA-2 family of hash functions, SHA-256 is extensively used for data integrity verification and cryptographic applications.

Diffie-Hellman Key Exchange: This key exchange protocol enables two parties to securely establish a shared secret key over an insecure channel. It played a pivotal role in the development of public-key cryptography.

Elliptic Curve Cryptography (ECC): ECC offers strong security with smaller key sizes compared to other asymmetric algorithms, making it well-suited for resource-constrained devices and applications.

OpenSSL: OpenSSL is an open-source cryptographic library that provides various tools and libraries for implementing secure communications and applications.

TLS/SSL (Transport Layer Security/Secure Sockets Layer): These cryptographic protocols provide secure communication over networks like the internet. They are essential for securing online transactions, communication, and data exchange.

HMAC (Hash-based Message Authentication Code): HMAC is widely used for message authentication and integrity verification. It combines a hash function with a secret key to produce a unique code that authenticates the message.

These are just a few examples of the most famous and widely used cryptographic tools and algorithms. Cryptography is a rapidly evolving field, and new tools and algorithms continue to emerge as technology advances and security needs evolve.

Conclusion:

These fundamental security techniques and approaches into our Cyber Security policy will significantly enhance the protection of company's employees, information, and resources. By promoting the use of strong passwords, enforcing a password expiration policy, implementing MFA, securing email communications with personal certificates, utilizing VPN IPSec for remote access, and encrypting portable/mobile devices, we establish a robust defense against potential cyber threats. As the company's Cyber Security Analyst, I am committed to fostering a culture of security awareness and vigilance among our employees, ensuring the ongoing integrity and confidentiality of our digital assets.

References:

https://cybercoastal.com/cryptography-cheat-sheet-for-beginners/
https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html
https://venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role/
https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111