Project 8: Cyber Security Best Practices

Prepared by: Esther Ogunlana
November 2, 2024

Executive Summary

In the evolving landscape of cyber threats, establishing robust security measures is critical for protecting sensitive information and maintaining employee privacy. This report outlines essential practices that should be implemented by the organization, including strong password policies, regular password expiration, multifactor authentication (MFA), secure email communication with personal certificates, VPN usage, and encryption of portable devices. According to the National Institute of Standards and Technology (NIST, 2020), the adoption of MFA significantly enhances security by requiring multiple forms of verification, which mitigates risks associated with unauthorized access. Furthermore, a strong password policy, as supported by Bonneau et al. (2012), is fundamental to preventing breaches from compromised credentials.

By utilizing secure email protocols that employ S/MIME certificates, organizations can ensure the confidentiality and integrity of communications (IETF, 2021). Implementing VPNs with IPSec provides an additional layer of security for remote connections, encrypting data in transit and protecting it from interception (Global Cyber Alliance, 2020). Lastly, encrypting hard drives and flash disks ensures that sensitive information remains protected even in the event of device loss or theft (FTC, 2020). This report aims to equip the organization with the necessary strategies to enhance its cybersecurity posture and safeguard its critical assets.

Introduction

In today's digital landscape, protecting sensitive information and maintaining user privacy are paramount. Cyber attacks are becoming increasingly sophisticated, necessitating proactive measures to safeguard organizational assets.

Cybercrime can negatively impact business operations if proper precautions are not taken to prevent it (Mass.gov, 2024). Some precautions include integrating secure networks and databases, limiting access to important databases, educating employees on the threat landscapes, and creating security policies. This report aims to present practical, effective techniques that the company can employ to enhance its cyber security framework focusing on introducing strong passwords, password expiration policy, Multi-Factor Authentication (MFA), secure email with personal certificate, VPN IPSec on laptops, and encrypting hard drives/flash disks to protect portable/mobile devices.

1. Strong Password Policy

A strong password policy is the foundation of effective security practices. Strong passwords should be complex, comprising at least 12 characters, including a mix of uppercase letters, lowercase letters, numbers, and symbols, using random characters, and encouraging unique passwords for different accounts. Regular training sessions can educate employees about creating and managing secure passwords. According to the National Institute of Standards and Technology (NIST, 2020), the implementation of strong password guidelines reduces the likelihood of unauthorized access.

While the thought of using lengthy passwords can be daunting, especially because passwords can be a hassle to remember, introducing an enterprise-level password manager takes the edge off remembering passwords as they create passwords, store, and fill passwords automatically (CISA, 2024).

2. Password Expiration Policy

Implementing a password expiration policy encourages employees to change their passwords regularly, typically every 60 to 90 days. This practice minimizes the risks posed by compromised passwords. A study by Bonneau et al. (2012) emphasizes that frequently changing passwords can limit the window of opportunity for attackers who may have obtained a password through phishing or other means.

However, as recently as 2020, NIST revised their password guidelines to emphasize password length over complexity requirements, salting and hashing stored passwords, MFA, and making it easier for users to adhere to password security policies. Additionally, organizations should not require their employees to reset their passwords more than once per year and only recommend creating new passwords in cases of suspected unauthorized access or breaches that result in personal credentials being published on the dark web, where they can be used in future cyberattacks (NIST, 2020).

3. Multifactor Authentication (MFA)

MFA provides an additional layer of security by requiring users to provide two or more verification factors to gain access to resources. This could involve something they know (a password), something they have (a mobile device), or something they are (biometric data). The Cybersecurity & Infrastructure Security Agency (CISA, 2021) recommends MFA as a critical component of security protocols, significantly reducing the risk of unauthorized access even if a password is compromised.
Implementing multifactor authentication (MFA) improves security by making stolen or cracked passwords far less useful to adversaries. NIST recommends implementing MFA only when the company can use Google Authenticator or another authentication process that doesn't involve SMS (Grassi et al., 2017).
Other recommendations by NIST are ensuring that the MFA process is user-friendly, and undergoing continuous evaluation of the MFA methods to ensure that they are adapting to the threat landscape (Grassi et al., 2017).

4. Secure Email with Personal Certificates

An email certificate is a digital file installed in your email application to facilitate secure communication. These certificates are often referred to by various names, including email security certificates, email encryption certificates, and S/MIME certificates. S/MIME, or "secure/multipurpose internet mail extension," allows users to digitally sign their emails and encrypt the content and attachments. This process not only verifies the sender's identity to the recipient but also safeguards the integrity of the email data during transmission over the internet (orange_resources, 2024).

Using personal email certificates ensures that communications are secure and verifiable. Employees can encrypt emails and sign them digitally, protecting sensitive information from interception. This method enhances the confidentiality and integrity of communications, making it difficult for malicious actors to tamper with messages. The use of public key infrastructure (PKI) for email encryption is supported by various organizations, including the Internet Engineering Task Force (IETF, 2021).

5. VPN IPSec on Laptops

IPSec, which stands for Internet Protocol Security, encompasses a set of communication protocols designed to create secure connections over a network. These protocols connect devices and incorporate encryption to protect data as it moves between them.

The IPSec protocol suite can be utilized by both individuals and larger organizations, serving as a primary protocol for various types of VPNs.

Implementing a Virtual Private Network (VPN) with Internet Protocol Security (IPSec) on company laptops ensures secure remote connections. VPNs encrypt internet traffic, protecting sensitive data from eavesdropping, especially on public networks. A report by the Global Cyber

Alliance (2020) highlights that using a VPN can significantly decrease the risk of data breaches while employees work remotely.
An IPsec VPN protects data from unwanted intrusions by using the IPsec protocol to establish a connection and encrypt data packets in transit and is particularly useful for businesses and large organizations with out-of-office workers who need remote access to resources (Higgins, 2024).

6. Encrypted Hard Drives and Flash Disks

Hard-drive encryption is a technology that encrypts the data stored on a hard drive using sophisticated mathematical functions.

Data on an encrypted hard drive cannot be read by anyone who does not have access to the appropriate key or password. This can help prevent access to data by unauthorized persons and provides a layer of security against hackers and other online threats (Rouse, 2022).

Encryption of hard drives and flash disks is essential for protecting sensitive data stored on portable devices. Full-disk encryption ensures that data remains secure even if the device is lost or stolen. According to the Federal Trade Commission (FTC, 2020), encryption is a critical measure to prevent unauthorized access and data breaches. Employing solutions like BitLocker or VeraCrypt can provide robust encryption for company devices.

Conclusion

In conclusion, integrating these fundamental cybersecurity practices is essential for protecting the organization's employees and sensitive information from potential threats. By establishing a strong password policy, implementing regular password changes, utilizing multifactor authentication, securing email communications, employing VPNs with IPSec, and encrypting portable devices, the organization can significantly reduce its vulnerability to cyber-attacks.
As highlighted by NIST (2020), a comprehensive security approach protects data and builds trust among employees and stakeholders. Proactively adopting these measures will contribute to a resilient cybersecurity framework, ensuring the organization can operate securely in an increasingly complex digital environment.
While all these are important, it is paramount to note that training the employees and regularly reminding them of the advancements in the threat landscape will help them identify threats better and significantly reduce the possibility of them falling prey to cyber attackers' tricks and antics.

References

Bonneau, J., Herley, C., Oorschot, P. C., & Stajano, F. (2012). The password is dead; long live the password. Proceedings of the 2012 New Security Paradigms Workshop. https://doi.org/10.1145/2462106.2462114

Federal Trade Commission (FTC). (2020). Protecting personal information: A guide for business. https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

Global Cyber Alliance. (2020). Using a VPN: A guide for small business. https://www.globalcyberalliance.org/vpn-guide

Grassi, P. A., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Fenton, J. L., Burr, W. E., Lefkovitz, N. B., Richer , J. P., Danker, J. M., Theofanos, M. F., Greene, K. K., & Choong , Y.-Y. (2017, June). NIST SPECIAL PUBLICATION 800-63-3 IMPLEMENTATION RESOURCES. National Institute of Standards and Technology .

Higgins, M. (2024, July 1). *What is the IPsec Protocol and How Does It Work*. NordVPN. https://nordvpn.com/blog/what-is-ipsec/

Internet Engineering Task Force (IETF). (2021). RFC 8551 - The TLS Protocol Version 1.3. https://doi.org/10.17487/RFC8551

Mass.gov (n.d.). Protect Your Company from Cyber Attacks. Retrieved November 1, 2024, from https://www.mass.gov/info-details/protect-your-company-from-cyber-attacks

National Institute of Standards and Technology (NIST). (2020). NIST special publication 800-63B: Digital identity guidelines: Authentication and lifecycle management. https://doi.org/10.6028/NIST.SP.800-63b

Protect your company from cyberattacks. Mass.gov. (n.d.). https://www.mass.gov/info-details/protect-your-company-from-cyber-attacks

Require strong passwords: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/secure-our-world/require-strong-passwords

Vicente, V. (2024, May 3). NIST password guidelines 2024. AuditBoard. https://www.auditboard.com/blog/nist-password-guidelines/