Title: Strengthening Cybersecurity Strategy for our Company to Protect Employees and Information

Prepared by: Victor Onukwu, Chief Information Security Officer (CISO)

Date: 3 November, 2023

Table Of Content

Strengthening Cybersecurity Strategy for our Company to Protect Employees and Information

Executive Summary

In an era marked by increasing cyber threats, the protection of our company's employees and sensitive information is of paramount importance. As your Chief Information Security Officer, I present a comprehensive cybersecurity strategy that embraces industry best practices and recognized standards. Our approach encompasses the following salient points:

I. Strong Passwords
The implementation of strong passwords, in accordance with NIST guidelines, significantly reduces the risk of unauthorized access.
Our approach aligns with NIST NVD recommendations.

II. Password Expiration Policy
Regular password changes, every 90 days, will be enforced to mitigate the risk of prolonged exposure.
This practice is in line with NIST NVD guidance, which highlights the importance of periodic password changes.

III. Multi-Factor Authentication (MFA)
The introduction of MFA across all company accounts adds an additional layer of security.
MFA has proven to be a strong deterrent against unauthorized access, aligning with MITRE ATT&CK recommendations.

IV. Secure Email with Personal Certificates
Implementing secure email with personal certificates safeguards our email communications and information.
The use of personal certificates for email encryption adheres to industry standards and practices.

V. VPN IPSec on Laptops
To accommodate our mobile workforce, we will deploy VPNs with IPSec on laptops.
VPNs secure data transmitted over the internet, and IPSec ensures confidentiality and integrity, following MITRE ATT&CK best practices.

VI. Encrypted Hard and Flash Disks
Encryption of hard and flash disks on portable and mobile devices prevents unauthorized access.
This strategy aligns with MITRE ATT&CK guidance and is considered an industry-standard mitigation.

Strengthening Cybersecurity Strategy for our Company to Protect Employees and Information

By implementing these cybersecurity measures, we strengthen our defences against potential cyber threats. Furthermore, our commitment extends to ongoing cybersecurity education for our employees and close collaboration with technical teams to ensure successful implementation.

This strategy positions us to protect our employees and information effectively. It adheres to industry standards and best practices and ensures we are well-prepared to safeguard our digital assets. I stand ready to provide any additional information or clarification needed

Introduction

Background

The introduction section offers essential context for understanding the cybersecurity strategy presented in this report. It is essential to grasp the background information that has led to the development of these security measures. Our company has undergone a significant evolution in its approach to cybersecurity. Initially, I joined the company as a Junior Cyber Security Analyst, and over the years, I have worked diligently, earning certifications and accumulating experience, to ultimately assume the role of the Senior Cyber Security Analyst. Subsequently, I transitioned to the position of Supervisor in the Security Operations Center (SOC). My continued dedication and expertise have now led me to the position of Cyber Security Manager. As the newly appointed Chief Information Security Officer (CISO), my primary responsibility is to define the encryption level and the optimal allocation of resources to safeguard our employees and the company's sensitive information.

Purpose of the Report

The purpose of this report is to provide an overview of the cybersecurity strategy that will be implemented to fortify our organization's defense against potential cyber threats. The strategies and approaches outlined here will offer a strong foundation for safeguarding our employees and the sensitive data entrusted to us. As the new CISO, my focus is on addressing prevalent cybersecurity challenges. This report serves as a starting point for the comprehensive review of our company's cybersecurity policy and the initiation of discussions regarding the implementation of fundamental security concepts to protect our users.

The strategies encompass various aspects of cybersecurity, including strong password policies, password expiration, multi-factor authentication, secure email communication with personal certificates, VPN with IPSec deployment on laptops, and the encryption of hard drives and flash disks for portable and mobile devices. Each of these measures is designed to mitigate potential vulnerabilities and aligns with industry standards and best practices.

In the subsequent sections, I will delve into the details of each strategy, explaining their significance, providing implementation plans, and ensuring alignment with industry recommendations, such as those from NIST NVD and MITRE ATT&CK. Furthermore, I will emphasize the importance of employee training and collaboration with technical teams to ensure the successful execution of these security measures.

Strengthening Cybersecurity Strategy for our Company to Protect Employees and Information

Through this report, I aim to convey our commitment to cybersecurity, and unwavering dedication to protect our employees and company information from potential cyber threats.

Strong Passwords

A. Importance of Strong Passwords

Strong passwords are a fundamental component of our cybersecurity strategy. They serve as the first line of defense against unauthorized access and play a pivotal role in protecting our digital assets and sensitive information. Weak or easily guessable passwords represent a significant vulnerability that malicious actors often exploit to breach our systems.
https://attack.mitre.org/versions/v14/mitigations/M0927/

By enforcing the use of strong passwords, we can significantly reduce the risk of unauthorized access, which, in turn, helps safeguard our employees and critical data. Strong passwords are designed to be complex and challenging to guess, making it extremely difficult for cybercriminals to compromise accounts.

B. Implementation Plan

To ensure that our organization benefits from strong password protection, we will enact and enforce a robust password policy. This policy will mandate the use of passwords that meet the National Institute of Standards and Technology (NIST SP 800-63B) guidelines. Key components of the policy include:

1. **Password Complexity:** Passwords must be at least 12 characters in length and contain a combination of uppercase and lowercase letters, numbers, and special characters.
2. **Password Uniqueness:** Passwords should be unique and not reused across multiple accounts. This reduces the risk of attackers gaining unauthorized access through credential reuse.
3. **Regular Password Changes:** Passwords should be changed at regular intervals, ideally every 90 days. Regular changes mitigate the risk of long-term exposure, especially in the event of a breach.

C. Alignment with NIST NVD Guidelines

Our password policy is aligned with the recommendations provided by the National Institute of Standards and Technology (NIST), as outlined in the National Vulnerability Database (NVD). NIST's guidelines serve as a recognized and authoritative source for cybersecurity best practices. By following these

guidelines, we ensure that our organization adheres to industry-standard measures for password security, significantly reducing the risk of unauthorized access and data breaches.

Password Expiration Policy

A. Rationale for Expiration Policy

The implementation of a password expiration policy is a critical component of our cybersecurity strategy. Passwords are one of the most common targets for attackers attempting to gain unauthorized access to our systems. The rationale behind enforcing password expiration is twofold:

1. **Reducing Exposure to Credential-Related Threats:** Over time, the security of passwords can diminish due to factors such as evolving attack techniques like brute force and the potential for password leaks. Regular password changes help mitigate the risk of long-term exposure.
2. **Adherence to NIST NVD Guidelines:** Our approach to password expiration aligns with the guidelines provided by the National Institute of Standards and Technology (NIST) as recommended by the National Vulnerability Database (NVD). NIST's recommendations emphasize the importance of changing passwords periodically to enhance security.

B. Proposed Frequency

We propose a password expiration frequency of every 90 days. This timeline strikes a balance between security and user convenience. More frequent changes would reduce exposure further but could lead to increased user frustration and potentially weaker passwords. Less frequent changes could increase the risk of long-term exposure. The 90-day interval is a well-established industry practice for password expiration and offers a reasonable compromise.

C. Compliance with NIST NVD Recommendations

Our password expiration policy is in compliance with the recommendations outlined by NIST through the National Vulnerability Database (NVD). NIST provides comprehensive guidance on password management to enhance

cybersecurity. By adhering to these guidelines, we demonstrate our commitment to implementing best practices and reducing the risk of credential-related threats.

Multi-Factor Authentication (MFA)

A. Significance of MFA

Multi-Factor Authentication (MFA) plays a pivotal role in fortifying our cybersecurity defenses. In an era of evolving cyber threats, relying solely on passwords is inadequate to protect our valuable assets. MFA enhances our authentication process by requiring users to provide two or more different forms of identification before granting access to their accounts.

The significance of MFA lies in its ability to substantially reduce the risk of unauthorized access and protect against various threat vectors, including stolen or weak passwords, phishing attacks, and credential breaches. By implementing MFA, we add a critical layer of security, making it significantly more challenging for malicious actors to compromise our systems and data.

B. Scope of MFA Implementation

Our approach to implementing MFA will encompass all critical systems and accounts, with a particular emphasis on those handling sensitive information, financial transactions, and administrative functions. We will prioritize the following areas for MFA implementation:

1. **User Accounts:** MFA will be mandatory for all user accounts, ensuring that each employee, contractor, and authorized personnel uses multi-factor authentication when accessing our systems and data.
2. **Remote Access:** Employees accessing our systems remotely, especially through virtual private networks (VPNs), will be required to use MFA to authenticate themselves.
3. **Cloud Services:** MFA will be enforced for accounts associated with cloud services, including email, file sharing, and collaborative platforms.

C. Mitigation of Unauthorized Access

MFA significantly reduces the risk of unauthorized access by requiring the user to provide multiple proofs of identity. These factors typically include something the user knows (e.g., a password), something the user has (e.g., a smartphone or hardware token), and something the user is (e.g., biometrics like fingerprint or facial recognition). This multi-layered approach ensures that even if one factor is compromised, access remains protected by the other factors.

MFA serves as a powerful deterrent against common attacks, such as brute-force attacks and phishing attempts, which rely on the weakness of single-factor authentication. By requiring at least two forms of authentication, we significantly elevate our security posture, making it substantially more challenging for cybercriminals to gain access to our systems.

D. Alignment with MITRE ATT&CK Recommendations

Our adoption of MFA aligns with the recommendations provided by the MITRE ATT&CK framework, a widely recognized industry standard for cyber threat mitigation. MITRE ATT&CK emphasizes the importance of MFA as an effective measure to defend against various attack techniques, including those related to credential theft and account compromise. By implementing MFA, we are proactively addressing security concerns highlighted in the MITRE ATT&CK framework and ensuring that our cybersecurity strategy adheres to industry best practices. https://attack.mitre.org/versions/v14/mitigations/M1032/

Secure Email with Personal Certificates

A. Benefits of Secure Email

Secure email communication is a critical component of our cybersecurity strategy. It offers several benefits that enhance the confidentiality and integrity of our email correspondence:

1. **Confidentiality:** Secure email ensures that our email content remains private and inaccessible to unauthorized parties. This is especially important when sharing sensitive information, trade secrets, or confidential documents.

2. **Data Integrity:** By digitally signing our emails with personal certificates, we can guarantee the integrity of the message content. Recipients can verify that the email has not been tampered with during transmission.
3. **Authentication:** Personal certificates add a layer of authenticity to our email communications. Recipients can trust the source of the email, reducing the risk of falling victim to phishing attacks or impersonation.
4. **Protection Against Email-Based Threats:** Secure email mitigates the risks associated with email-based threats, such as man-in-the-middle attacks, eavesdropping, and email interception. This is a key defense against cyber threats that often exploit email vulnerabilities.

B. Implementation Strategy

To secure our email communications, we will implement the use of personal certificates for all employees. Here's a brief overview of the implementation strategy:

1. **Certificate Acquisition:** We will provide employees with personal certificates issued by a trusted Certificate Authority (CA). These certificates will be associated with their email accounts and used to sign and encrypt emails.
2. **Email Client Configuration:** Employees will be guided on how to configure their email clients to use the certificates. This will ensure that outgoing emails are signed, and incoming emails can be verified.
3. **User Training:** To ensure the successful adoption of this approach, we will conduct training sessions to educate our employees on how to use personal certificates and recognize the security benefits they offer.
4. **Integration with Email Servers:** Our email servers will be configured to enforce certificate-based email authentication. This will ensure that only authenticated users can send and receive secure emails.

C. Conformity with Industry Standards

Secure email with personal certificates is a recognized industry standard and best practice for email security. It aligns with recommendations from industry bodies and standards organizations, including the following:

1. **Encryption Standards:** Personal certificates use encryption protocols and algorithms that conform to international encryption standards, ensuring data protection.

Strengthening Cybersecurity Strategy for our Company to Protect Employees and Information

2. **Digital Signature Standards:** Personal certificates enable digital signatures, complying with best practices for email integrity and authenticity.
3. **Regulatory Compliance:** Many regulations and data protection laws recommend or require the use of secure email for the protection of sensitive data.

By implementing secure email with personal certificates, we will strengthen the security of our email communications, safeguard our sensitive information and reduce the risk of email-related security breaches

VPN IPSec on Laptops

A. Mobile Workforce Security

With an increasing number of our employees working remotely or on the go, it is imperative to ensure that data transmitted over the internet and remote connections remain secure. To address this, we will implement Virtual Private Network (VPN) technology with the use of Internet Protocol Security (IPSec) on laptops.

B. VPN and IPSec Implementation

1. Virtual Private Network (VPN): VPNs create a secure, encrypted tunnel for data traffic between remote devices and our internal network. This ensures that data exchanged over the internet is protected from interception and tampering.
2. Internet Protocol Security (IPSec): IPSec is a suite of protocols that provides authentication, integrity, and confidentiality for network communications. By integrating IPSec into our VPN solution, we add an extra layer of security to the data exchange, ensuring that data remains confidential and unaltered during transmission.

C. Protection of Remote Connections

The implementation of VPN IPSec on laptops offers several benefits:

1. Confidentiality: IPSec encrypts data, making it unreadable to unauthorized parties. This safeguards sensitive company information from eavesdropping and interception by cybercriminals.
2. Integrity: IPSec ensures that data remains unaltered during transit. It provides a guarantee that the data received is the same as what was sent, guarding against data manipulation or tampering.
3. Authentication: By using IPSec, we require laptops to authenticate themselves before establishing a connection. This ensures that only authorized devices can access our network, reducing the risk of unauthorized access.
4. Secure Remote Access: With VPN IPSec, our employees can securely access company resources and data from remote locations, enhancing productivity without compromising security.

Strengthening Cybersecurity Strategy for our Company to Protect Employees and Information

D. Compliance with MITRE ATT&CK Best Practices

The implementation of VPN IPSec on laptops aligns with best practices outlined by MITRE ATT&CK, an industry-standard framework for cybersecurity:

1. Data Protection: VPN IPSec safeguards data against threats such as man-in-the-middle attacks and eavesdropping, ensuring data protection.
2. Access Control: Authentication through IPSec enforces access control, allowing only authorized users to connect to our network.
3. Secure Communication: The encrypted tunnel created by IPSec ensures that communication between laptops and our network is secure and protected from external threats.

By incorporating VPN IPSec on laptops, we are taking a proactive step to secure remote connections, enhance data privacy, and protect the integrity of our communications. This is crucial in an age where remote work is prevalent and where the protection of sensitive company information is paramount.

Encrypted Hard and Flash Disks

A. Importance of Data Encryption

The security of portable and mobile devices is of paramount importance in today's digital landscape. With the increasing prevalence of remote work and the use of laptops, smartphones, and portable storage devices, there is a heightened risk of data exposure in case of loss or theft. To address this risk, it is imperative to implement data encryption on hard drives and flash disks. Data encryption is the process of converting information into an unreadable format using encryption algorithms. This ensures that even if a device falls into the wrong hands, the data remains inaccessible and confidential.

B. Measures for Device Protection

Our approach to securing portable and mobile devices includes the mandatory use of full-disk encryption. Full-disk encryption protects all data on the device, including the operating system and application files. This means that even if an attacker gains physical access to a laptop or flash disk, they will not be able to access or decipher the stored data without the encryption key. This measure

greatly reduces the risk of data breaches stemming from physical device loss or theft.

C. Preventing Unauthorized Access

In addition to full-disk encryption, we will enforce strong password or PIN requirements to unlock encrypted devices. This adds an extra layer of security, ensuring that only authorized personnel can access the data. Furthermore, in the event of repeated unsuccessful login attempts, the device can be configured to wipe the data, protecting it from unauthorized access.

D. Alignment with MITRE ATT&CK Guidance

The implementation of encrypted hard and flash disks aligns with industry-standard mitigation strategies recommended by MITRE ATT&CK. This framework emphasizes the importance of data encryption to protect against data theft and unauthorized access, making it an essential component of our cybersecurity approach.

The deployment of encrypted hard and flash disks is a critical step in safeguarding sensitive information, especially for employees who work remotely or require mobility. It ensures that our data remains confidential and protected in the face of physical device loss or theft, further enhancing our overall cybersecurity posture.

Employee Training and Collaboration

A. Ensuring Awareness and Compliance

Employee awareness and compliance are pivotal in the success of our cybersecurity strategy. In this regard, the following actions will be taken:

1. **Cybersecurity Training:** We will develop and conduct regular cybersecurity training programs for all employees. These programs will cover topics such as password management, MFA usage, secure email practices, and recognizing potential threats. Training sessions will be mandatory for all employees, with periodic refreshers to ensure sustained awareness.

2. **Awareness Campaigns:** We will launch awareness campaigns, including newsletters, posters, and email updates, to keep employees informed about the latest cybersecurity trends and best practices. This will create a culture of cybersecurity vigilance.
3. **Employee Accountability:** To enforce compliance, we will implement an accountability system. Non-compliance with our cybersecurity policies will be addressed through a clear protocol that includes warnings, retraining, and potential disciplinary actions.
4. **Phishing Simulation:** Periodic phishing simulation exercises will be conducted to assess and improve employees' ability to recognize and respond to phishing attempts, a common vector for cyberattacks.

B. Cooperation with Technical Teams

Collaboration with our technical teams is essential to ensure the seamless implementation of the proposed cybersecurity measures. This involves the following:

1. **Cross-Functional Security Committee:** We will establish a cross-functional security committee comprising members from IT, cybersecurity, and relevant business units. This committee will meet regularly to review progress, address concerns, and make necessary adjustments to our security strategy.
2. **Technical Support and Guidance:** Our technical teams will be responsible for the technical aspects of implementation, such as configuring and maintaining MFA systems, securing email systems, and managing VPN and encryption solutions. They will receive ongoing guidance and support to ensure that security measures are functioning optimally.
3. **Incident Response Coordination:** In collaboration with our technical teams, we will create and rehearse an incident response plan. This plan will detail the actions to be taken in the event of a security breach and will ensure that the response is swift and effective.
4. **Regular Security Audits:** Our technical teams will conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in our systems. These audits will align with MITRE CVE recommendations and industry standards.

By fostering employee awareness and collaboration with our technical teams, we can create a robust cybersecurity ecosystem that mitigates risks, protects our employees and information, and ensure that our organization is well-prepared to respond to potential cyber threats. This holistic approach is essential for a successful cybersecurity strategy.

Strengthening Cybersecurity Strategy for our Company to Protect Employees and Information

Conclusion

In this report, I have outlined a comprehensive cybersecurity strategy designed to protect our company's employees and sensitive information from potential breaches. I have discussed the implementation of various techniques and approaches, each of which aligns with recognized industry standards and best practices.

As your Chief Information Security Officer, I want to emphasize our unwavering commitment to the highest level of cybersecurity. Our dedication to protecting our employees and sensitive information is paramount. The measures proposed in this report are the first steps in strengthening our defenses against potential cyber threats. We will continuously assess, improve, and adapt our cybersecurity strategy to stay ahead of emerging threats.

References

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines: Authentication and lifecycle management (NIST Special Publication 800-63B). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

MITRE. (n.d.). MITRE ATT&CK®. https://attack.mitre.org/

International Electrotechnical Commission. (2018). Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components (IEC 62443-4-2:2018). https://webstore.iec.ch/preview/info_iec62443-4-2%7Bed1.0%7Db.pdf

Compass. (n.d.). Project: Encryption. https://cyber.compass.lighthouselabs.ca/p/2/projects/encryption?day_number=w07d4

OpenAI. (n.d.). ChatGPT. https://openai.com/chatgpt

National Institute of Standards and Technology. (n.d.). National Vulnerability Database. https://nvd.nist.gov/

Strengthening Cybersecurity Strategy for our Company to Protect Employees and Information