Encryption Project

Protecting Our Company:
A Multi-Layered Approach to Cybersecurity

By Heather Fincati
March 22, 2024

Table of Contents

Glossary

Advanced Persistent Threat (APT): an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.

Biometric Authentication: A security method that relies on unique biological characteristics to verify a user's identity (e.g., fingerprint, facial recognition).

Cybersecurity: all about protecting our company's computers, networks, data, and information systems from cyberattacks. Imagine your company's information as a treasure chest. Cybersecurity is like building strong defenses around that chest to keep out "bad guys" (cybercriminals) who might try to steal the treasure (data) or cause damage.

Data Breach: An incident where information is accessed and disclosed without authorization.

Digital Certificate: An electronic document that verifies the identity of a website or individual.

Encryption: The process of transforming data into a scrambled form that only authorized parties can decrypt.

Endpoint Detection and Response (EDR): A system designed to detect and respond to malicious activity on endpoints (e.g., laptops, desktops).

Internet Protocol Security (IPSec): A set of protocols for securing internet protocol (IP) communications by encrypting and authenticating each packet of data.

Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to a computer system.

Multi-Factor Authentication (MFA): an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

National Institute of Standards and Technology (NIST): A U.S. government agency that develops standards and guidelines for cybersecurity.

Password Expiration Policy: A security policy that enforces users to change their passwords at regular intervals.

Phishing: A fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

Social Engineering: A psychological manipulation tactic used to trick people into clicking malicious links, revealing confidential information, or performing actions that compromise their security.

Threat Landscape: The ever-evolving range of potential threats to an organization's information systems.

Virtual Private Network (VPN): A secure tunnel that encrypts data traveling between a user's device and a network.

Executive Summary

Cybersecurity is extremely important in today's digital landscape. Ensuring our companies, employees and information is safeguarded against cyber threats is of our utmost importance.

This report outlines a multi-layered defense using key techniques and industry standard approaches, provided by the National Institute of Standards and Technology Framework (NIST) to strengthen our cyber security posture. This includes the implementation of strong passwords, password expiration policies, Multi-Factor Authentication (MFA), secure email with personal certificates, Virtual Private Network (VPN) Internet Protocol Security (IPSec) for laptops, and encrypted hard drives and flash disks. These strategies will significantly enhance our defenses against cyber attacks, protecting sensitive data and minimizing operational disruption.

Introduction

As the newly appointed Cyber Security Manager, I am evaluating and enhancing our existing cyber security policies to better protect our employees and information. To achieve this, we need a comprehensive understanding of the threat landscape. Cybercriminals employ a wide range of tactics, from social engineering scams to sophisticated malware attacks like advanced persistent threats (APTs) that can remain undetected for extended periods. These threats can lead to data breaches, financial losses, and reputational damage. By implementing robust cybersecurity measures, we can significantly reduce the risk of such incidents.

Building Strong Defenses: A Multi-Layered Approach

Strong Passwords and Password Expiration Policies

By creating a policy that enforces the creation of complex passwords (NIST, 2020) with a combination of uppercase and lowercase letters, numbers, and special characters along with regular password changes (e.g., every 90 days) we can further bolster security. And is the first line of defense against unauthorized access.

Multi-Factor Authentication (MFA)

MFA (NIST, 2020) adds an extra layer of security beyond passwords by requiring users to provide multiple forms of verification before gaining access. This could include something the user knows (password), something they have (security token or mobile device), or something they are (biometric authentication). Implementing MFA significantly reduces the risk of unauthorized access, even if passwords are compromised.

Secure Email with Personal Certificates

Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory (NIST, 2013). Implementing digital certificates for email encryption ensures only authorized parties can read email content. It would be like sending a sealed, locked package – only the recipient with the key can open it and see what's inside. This safeguards sensitive information during transmission from bad actors eavesdropping and potentially tampering.

VPN IPSec for Laptops - Enhancing Remote Access Security

To address the security risks associated with public Wi-Fi networks, we recommend deploying a Virtual Private Network (VPN) with Internet Protocol Security (IPSec) for remote access. This technology establishes a secure tunnel, encrypting data in transit using the Internet Key Exchange (IKE) protocol (NIST, 2020). This encryption safeguards sensitive information from potential interception by malicious actors, ensuring a more secure remote work environment.

Encrypted Hard Drives and Flash Disks

Many threats against removable media, could cause information stored on the devices to be accessed by unauthorized parties (NIST, 2007). Encrypting hard and flash disks on portable/mobile devices adds an additional layer of security to data, especially in case of loss or theft. Encryption renders data unreadable without a decryption key, protecting sensitive information even if the device falls into the wrong hands.

Benefits and Considerations

These security measures offer several advantages:

Enhanced Data Protection

Stronger passwords, encryption, and secure email significantly reduce the risk of unauthorized access to sensitive data and identity theft and financial loss.

Reduced Risk of Cyber Attacks

Implementing these measures makes it more challenging for cybercriminals to infiltrate our systems, making working remotely a more secure environment for accessing company data.

Improved User Education

Enforcing password policies and Multi-Factor Authentication encourages a culture of cybersecurity awareness among employees.

Next Steps

- Develop a comprehensive cybersecurity policy outlining these measures and user responsibilities.
- Conduct employee training sessions on best practices for password management, email security, and identifying phishing attempts.
- Regularly evaluate and update security measures to stay ahead of evolving threats.

Conclusion

By implementing this multi-layered cybersecurity strategy, we will significantly strengthen our defenses against cyberattacks. The measures outlined in this report – strong passwords, password expiration policies, Multi-Factor Authentication (MFA), secure email with personal certificates, VPN with Internet Protocol Security (IPSec) for laptops, and encrypted hard drives and flash disks – will create a more secure environment for our employees and safeguard sensitive company information.

This proactive approach goes beyond simply mitigating risk. Industry benchmarks suggest cybersecurity investments can provide a significant return. Additionally, studies like the IBM Cost of a Data Breach Report 2023 (IBM, 2023) highlight the potential financial losses from a cyberattack, reaching an average global cost of $4.35 million USD in 2023 as an example. By implementing these measures, we can significantly reduce the likelihood and impact of such an event.

In turn, this robust cybersecurity posture will not only protect our critical operations and financial well-being, but most importantly, maintain the trust of our stakeholders. By demonstrating our commitment to data security, we can foster a culture of confidence and ensure the continued success of our business.

References

1. NIST, Cybersecurity Framework | NIST, National Institute of Standards and Technology: https://www.nist.gov/cyberframework
2. NIST, (2020, March 2) NIST SP 800-63B Digital Identity Guidelines, NIST Pages: https://pages.nist.gov/800-63-3/sp800-63b.html
3. NIST, (2020, December 10) NIST SP 800-53B Rev. 5 Security and Privacy Controls for Information Systems and Organizations, NIST Computer Security Resource Centre: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
4. NIST, (2013, July 19) NIST Digital Signature Standard (DDS) | NIST, National Institute of Standards and Technology: https://www.nist.gov/publications/digital-signature-standard-dss-2
5. NIST, (2020, June 17) NIST SP 800-77 Rev.1, Guide to IPsec VPNs, NIST Pubs: https://www.nist.gov/publications/guide-ipsec-vpns
6. NIST, (2007, November 15) NIST SP 800-111 Guide to storage Encryption Technologies for End User Devices, National Institute of Standards and Technology: https://www.nist.gov/publications/guide-storage-encryption-technologies-end-user-devices
7. IBM, (2023) Cost of a data breach 2023, IBM: https://www.ibm.com/reports/data-breach