The Significance of securing your Data in this Digital Age

Executive Summary:
With so many new innovations in our world, it is a blessing for all of us to have access to new forms of technology that help to assist us in our daily lives and in many cases, make our work a bit easier. Unfortunately with everything, there are negatives that come with the positives and that is exactly the case here with tech. Anyone in the world can become a victim of a cyber attack and have their personal information/data stolen by a malicious actor (cybercriminal). As the Cyber Security manager, it is my duty to implement strategies to safeguard the organization from cyber threats and ensure that we are taking the relevant measures to protect our private data. The following techniques and approaches should be utilized by all of the employees to maximize the company's cyber security. This report will not only outline techniques and approaches but also explain how they will help in protecting the company's employees and information.

Use of Strong passwords:
It is recommended that all of the employees should secure all of their accounts with strong passwords. Cyber attacks are becoming more sophisticated everyday and with the use of weaker passwords, it is relatively simple for criminals to gain access to your personal accounts and steal your data. An example of these attacks is a brute-force attack; which involves trying different combinations of characters until the correct password is found. There are now automated systems where attackers can use various techniques to breach your accounts within hours due to the weak nature of many passwords. Strong passwords are essential for protecting personal information and preventing unauthorized access to online accounts. Follow the guidelines below for strong passwords:

1. Use a mix of upper and lower case letters, numbers, and symbols
2. Avoid easily guessable information such as identifiable information (name, birthdate)
3. Aim for a password of at least 12 characters long
4. Try not to reuse passwords because if a hacker breaches one account, they could potentially gain access to any account that uses the same password

Implement Password Expiration Policies:

Password expiration policies regulate how frequently users must replace old passwords with new ones. Organization administrators use tools to set timeframes for passwords for password expiration; in which individuals would have to then change their password.

The benefit of these policies is that an attacker has a limited amount of time to compromise a user's password and gain access to your data. However, in 2019, Microsoft stated that they believed password expiration policies were no longer making organizations safer due to employees creating simpler passwords as a result of frequent changes. This is where we must educate our employees so that they fully understand the importance of using strong passwords as stated above. There are even methods in which admins can reward the use of more complex passwords by giving users a longer amount of time before having to reset their credentials.

Use of Multi-Factor Authentication (MFA):

This is a process in which a user is required to present at least two 'factors' that prove their identity. The factors involved typically include your login credentials as one and the other could be something such as a cell phone verification or biometric scan. The purpose of MFA is not to replace passwords but to back them up as another layer of protection against attackers trying to breach your accounts. The following are some of the benefits:

- MFA enables stronger authentication
- MFA adapts to the changing workplace
    - As more and more employees continue to work outside the office, this can allow for added safety if users are working from untrusted locations
- MFA offers security without compromising user experience

Secure your email with a personal certificate:

It can be beneficial to use forms of encryption to secure emails so that sender and receiver are the only ones that can access the contents of the email. This can be done with the use of personal certificates and I will outline some of the benefits below:

- Email security can help you avoid business risk
- You can reduce compliance risks by securing your emails
- Email encryption helps you protect confidential information
- Signing your emails can detract identity thieves

Implement VPN IPSec on laptops:

In the case of company employees that work remotely, we should implement IPsec VPNs to secure their remote network connection. IPsec is a group of protocols for securing connections between devices. It works by encrypting router traffic and authenticating where incoming traffic comes from. VPN stands for virtual private network and it is an encrypted connection between two or more computers. The addition of IPsec VPN connections to the company network can enhance the security of the organization in case of some remote employees that access important data from unsecure locations.

Cryptografied hard and flash disks to protect portable/mobile devices:

Disk encryption software prevents a disk drive from booting up unless the user inputs the correct authentication data. This kind of software is particularly practical in securing data when it is stored on a portable device. Below are some benefits of using disk encryption:

- Securing data from hackers
- Eliminating the risk of human error
- Eliminating the risk of data leaks
- Mitigating the likelihood of liability issues arising
- Achieves high-level security with minimal effort

Conclusion:

As we continue to navigate this digital age in which data breaches and cyber attacks are now a common occurrence, we continue to dedicate time and effort to improve the safety of our personal information and data. The techniques outlined in this report are only one aspect of how we can protect the security and integrity of this company. I will persist in fulfilling my responsibility to thoroughly research and inform users about methods to enhance the security of their accounts.

References

Cloudflare. (n.d.). *What is IPsec?* | *How IPsec VPNs work*. Cloudflare. Retrieved August 18, 2023, from https://www.cloudflare.com/en-ca/learning/network-layer/what-is-ipsec/

Creating Strong Passwords: Importance and Best Practices. (2023, March 20). EC-Council University. Retrieved August 18, 2023, from https://www.eccu.edu/blog/technology/the-importance-of-strong-secure-passwords/

Hayes, D. (2020, April 16). *5 Reasons to Utilize S/MIME Certificates for Email Security*. GlobalSign. Retrieved August 18, 2023, from https://www.globalsign.com/en/blog/5-reasons-utilize-smime-certificates-email-security

Microsoft. (2022, October 2). *Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903*. Microsoft. Retrieved August 18, 2023, from https://learn.microsoft.com/en-us/archive/blogs/secguide/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903

N-able. (2020, August 24). *Five Key Benefits of Using Disk Encryption Software*. N-able. Retrieved August 18, 2023, from https://www.n-able.com/blog/disk-encryption-software-key-benefits

N-able. (2020, September 8). *Why Password Expiration Policies Matter in Your Managed IT Business*. N-able. Retrieved August 18, 2023, from https://www.n-able.com/blog/why-password-expiration-policies-matter

Okta. (2023, February 14). *Why Multi-Factor Authentication (MFA) Is Important*. Okta. Retrieved August 18, 2023, from https://www.okta.com/identity-101/why-mfa-is-everywhere/

Project Reading. (2022, October 2). LHL Compass. Retrieved August 18, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w07d3/activities/3022