Cybersecurity Best Practices

Why Cybersecurity?

Cybersecurity has become a necessity for all businesses with the current threat environment. Attackers are working hard to breach your workplace to steal your data or set you up for ransomware. Hacking, phishing, and malware incidents are the number one cause of security breaches today. We have put together some tips to assist you in securing your users and your workplace to help prevent these attacks from happening.

1) Think before you click!

Most cyberattacks are started with phishing emails sent to unwary users who click on a seemingly harmless link that gives attackers access to their systems. Always think before you click on a link in an email and if you are not sure then **don't click**! Confirm that the email in legitimate before clicking on any links within the email. You can also subscribe to security awareness training to educate your users on what to watch out for with phishing emails and other types of attacks.

2) Keep all software and firmware up to date!

Another way attackers enter networks is through unpatched software and devices. Always keep your software up to date and the firmware on your devices current.

3) Use firewalls and anti-virus!

Firewalls and anti-virus software assist in keeping your data safe. Attackers must first get past these protections during an attack, so it is imperative to have firewalls and a robust behavioral AI anti-virus software (like SentinelOne) in place on your endpoints to assist in protecting your environment.

4) Use strong passwords and a password manager

Strong, unique passwords are a must in today's threat environment. Always use long, unique passwords and do not reuse passwords for multiple logins. Do not store passwords in your browsers. A password manger like LastPass will allow you to securely store all your passwords in a single location so the only password you need to remember is the password to access your management tool.

Tips for managing passwords:

- Don’t write passwords down.
- Don’t share your password with other users.
- Don’t use the same password for multiple accounts.
- Change your passwords every 3-6 months. The more sensitive the information, the more often the password should be changed.

Creating a strong password:

- Strong passwords must be at least 8 characters long (12 characters or more are recommended unless the application does not allow 12 characters or more then use max characters allowed), and are recommended to contain characters from three of the following four groups:
    - Uppercase A-Z (unless application does not allow uppercase)
    - Lowercase A-Z (unless application does not allow lowercase)
    - Numbers 0-9 (unless application does not allow numbers)
    - Special characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ (unless application does not allow special characters)
- Avoid using single dictionary words, names, places, etc. You can use combinations of unrelated words with or without spaces, but don’t use words that relate. “Bigbluesea#” is not very secure, something like “Scubatreepurple!” is much better.
- Passwords can contain spaces and can be up to 128 characters (the longer the password is the more secure it is). For passwords that need to be changed often, use a password manager like LastPass to store all your passwords so you only need remember one – the password for your password manager.

5) Use two-factor (2FA) or multi-factor (MFA) authentication

Two-factor or multi-factor authentication is a service that adds additional layers of security to the standard password method of online identification. Without two-factor or multi-factor authentication, you would normally enter a username and password. But, with two-factor or multi-factor authentication, you would be prompted to enter an additional authentication method such as a Personal Identification Code, another password or even fingerprint.

6) Backup your data regularly

One of the most common types of cyber-attacks is ransomware where an attacker gains access to your system, encrypts the data on the system then requires a “ransom” to be paid before providing the key to unlock the data. There is no guarantee that the attacker will provide the key even after a ransom is paid so it is always beneficial to have a backup copy of all your data. Backups aid in restoring your data in the event of a machine crash too.

7) Use your mobile devices securely

We all use our cell phones for accessing email, surfing the Internet and accessing our social media applications. Your mobile device is now a target for attackers too. There are over 1.5 million new incidents of mobile malware that target your data.

Tips for using mobile devices:

- Install a good anti-virus on your mobile devices (SentinelOne Mobile).
- Create a mobile passcode to access your device – do not use your birthdate or other information that can be guessed or found out from your social media accounts.

- Avoid sending PII (personal identifiable information) through email or messaging and keep it off your social media accounts as much as possible.
- Install apps from trusted locations and sources only.
- Update the software on your mobile device regularly and keep all apps up to date.
- If possible, backup your data on your phone using iCloud or enabling backup and sync from Android.
- Do not use public wi-fi to access your bank accounts or any other system or accounts.

Conclusion

In today's threat environment it is imperative that businesses protect their networks and educate their employees on the ever-present threats of today. MuniMetriX Systems offers a state-of-the-art, next generation antivirus with SentinelOne. SentinelOne will not only stop an attack before it does any harm but also allows you to roll back the infected endpoint to a state where it was healthy minimizing any down time. MuniMetriX Systems can also train your employees to recognize threats stopping them before they happen with Security Awareness Training. We will train your employees to be your first line of defense, human firewalls!