How can enterprises #BeCyberSmart with Hexnode?

Cybersecurity attacks have become the modern-day sword of Damocles, constant and ever-looming. We've seen SMBs, enterprises, and even government institutions fall victim to varying degrees of cybersecurity attacks, in recent years. In a study by Kaspersky Labs, it was found that about 90% of security attacks happen due to human error.

#BeCyberSmart is a campaign powered by the Department of Homeland Security and is aimed at improving the cybersecurity posture of each and every American citizen. Even though the points made in this campaign are geared towards individuals or homes, there are some good takeaways for businesses too. Since the human element is the weakest link of an organization from a cybersecurity standpoint, we'll look into ways we can strengthen that with Hexnode UEM.

We'll be following along with the cyber lessons that the Department of Homeland Security has elucidated in their campaign and the add-on how Hexnode can help adapt them to a corporate space.

Maintaining a password protocol

It's the year 2021, we are in the future, and still, some of the most commonly used passwords in the world include, 123456, qwerty, and abc123. This is not okay. This is the equivalent of writing "kick me" on a post-it note and sticking it on your back. How do we enforce a protocol that would prevent the usage of such passwords in your organization? With Hexnode UEM you can set multiple criteria, through a password policy, that could follow the best practices while creating a password. These could include:

- Password History: Employees can be restricted from using old passwords on a regular basis if a policy is in place. They would be less likely to use passwords they've used before. It is best to implement a password history policy that determines an employee's number of unique passwords before they attempt to reuse an old one. At least 3 to 5 unique passwords should be entered by the employee.
- Password Age: The administrator or the IT staff can set an expiry date for the passwords that employees use on their work devices. Passwords on such devices must be updated on a regular basis, in order to strengthen your organization's security posture. Set a password age with Hexnode so that this is possible, and allow employees to renew their passwords on their own.
- Complexity Requirements: Complex passwords are difficult to guess and thus more difficult to crack. At least 6 to 12 characters should be a solid difficult password; also, no user name elements (such as the first name) and include several types of character – lower case and upper case, names, and symbols such as!*+, etc. With Hexnode you can ensure that the staff follows the complexity criteria set by you.

- Lockout: With Hexnode you can also formulate a lockout policy that defines how long the device is locked out following some invalid password submissions.

These password policies can be applied to Android, iOS, macOS, and Windows devices, remotely. So, enforce strong password protection for your devices from a single platform with Hexnode UEM.

Bypassing email phishing attempts

According to a recent study by Proofpoint 75% of organizations around the world faced phishing in some way, type or form. In the Data Breach Investigations Report by Verizon, it was found that 96% of phishing attempts were made via email. These attackers understand the weakest link and they exploit it to the maximum. When an employee is a victim of a phishing attack within your corporate network, your entire corporate data is in jeopardy.

With Hexnode's email management capabilities, you can stave off phishing attacks without breaking a sweat.

- Email domains can be configured so that the employees can only open emails received from managed domains. They can also only download attachments from managed domains.
- Hexnode can ensure that emails aren't opened in an unmanaged app. This is possible with the blacklist/whitelist function.
- Copy and paste can also be disabled for emails so that employees don't accidentally cause a data breach.

Phishing is one of the most prevalent forms of cybersecurity attacks out there. Even though most companies do provide phishing awareness training to their employees, it's always better to have a plan to face these scenarios head-on.

Keep tabs on your apps

Nowadays, every app you download asks for a million permissions. Not really bothered about it, we just accept all of them blindly. In a corporate setting, this could spell danger. Furthermore, what if the employee blindly downloads an app from an untrustworthy source, that's a recipe for a full-blown data breach.

Hexnode can mitigate these risks with its app management capabilities:

- **Custom app store**: Create a repository for the apps you think the employees would require. These custom app stores can house applications that are native to that particular platform and even in-house applications. This ensures that the employee doesn't have to leave the safe digital work environment to access the apps they require. The apps can be formed into groups or catalogs for easier deployment.

- **App lifecycle management**: Hexnode can manage everything, starting from the app's installation to its uninstallation. This includes update management, version changes, etc.
- **App permission and configuration management**: You can decide what all permission an app could get away with on the work devices you have deployed with Hexnode. You can place restrictions on certain permissions if you feel it would tamper with the organization's security. You can also place configurations on the apps present in the employee's work device that can restrict them from indulging in any malicious activity.
- **App blacklisting/ whitelisting**: Blacklist or whitelist apps that you feel could cause a security issue. This can be applied across all devices, all at once.
- **Work app and personal apps**: The risk posed by BYO devices are too big to be ignored. If data that is meant to be opened in a work app is opened in a personal app, it could lead to a data breach. Hexnode provides segregation for work and personal apps, so that managed and unmanaged data never mingle.

Protecting corporate networks

In the current cybersecurity landscape, the role of enterprise network security is quite important. Malicious entities can tap into your corporate network and launch cyber-attacks that could very well compromise the entire functioning of your organization. As Hexnode UEM has the capability to control many of the access points for such attacks, it would be paramount for enterprises of all sizes to incorporate such software. So, how exactly can Hexnode help you with network security?

Wi-Fi Configuration: Wi-Fi settings can be configured via Hexnode to connect devices to a corporate network. Over the air, an administrator can push Wi-Fi configurations to a managed device. Users can join the network without having to enter or share their Wi-Fi passwords.

Deploying VPN: A VPN improves security by allowing users to communicate and share data via a private and secure network. This keeps it safe from potential threats and from the public network. As a result, a virtual network is an effective security solution that can be remotely configured with Hexnode UEM.

SCEP: Security threats caused by accessing work emails, Wi-Fi, VPN, etc., from unauthorized devices, can be solved by authenticating them with digital certificates. Hexnode UEM allows you to configure SCEP and enforce certificate-based authentication for Wi-Fi, VPN, Email, etc., on your devices.

Global HTTP proxy settings: With Hexnode you can ensure that all HTTP data flow through proxy servers. By controlling the flow of the data, you can ensure that your network is protected from possible threats.

Web content filtering: With whitelisting and blacklisting capabilities, Hexnode can ensure that your employees don't access malicious content while on the corporate network.

Bottom line

The pressure of protecting your organization against hordes of malicious entities is ever mounting. Most organizations feel they won't be a victim of a cyber-attack until they experience it themselves. It's always better to be aware and be prepared against any contingencies and Hexnode UEM can surely help you with that.