How to deal with increased cyber threats during the Covid-19 pandemic

Cyber threats are on the rise and enterprises are looking for the cyber equivalent of masks and sanitizers to help them secure their assets.

Have you ever imagined what would have happened if the Corona outbreak happened 10 or 15 years ago? The thought of being stuck with books and board games for a year or two would have driven most of us crazy. Thankfully we don't have to think about it, all we need is a mobile phone, wi-fi connection, and a charger to keep it fresh.

The development in technology has allowed us to turn our living rooms into office rooms that can function equally if not better than a typical workplace. The rapid increase in home offices has given hackers a host of new opportunities to exploit. Cyber threats are at an all-time high and enterprises are their primary target.

Nearly tens of thousands of coronavirus-related websites are being created daily and almost 90% of them are fishy. They are focused on selling fake cures, collecting user data, installing malware, and spreading false information.

Covid-themed spam and phishing campaigns are aimed at exploiting personal data. Employees tend to use a load of websites and applications to help with their work, it is a common practice especially among senior staffers to use the same login credentials for most of their accounts. The attempts at stealing passwords have gone up exponentially through social media. Fake login pages and data capture forms are being extensively used.

Most users don't realize that their data has been compromised until it's too late. The lack of information about trending cyber threats and phishing methods leaves users as prey.

Remote work has affected the quality of information that is passed to employees from IT admins. Failure in communications leaves your company open to attacks that are targeted specifically at you. It's easier for misinformation to spread and timely corporate intervention is always missing.

Another key concern is the lack of supervision of the devices used by employees. The employee might be well trained in the dos and don'ts regarding their work devices but when they are not at the office, there is a chance that someone like their children, spouses, friends, etc. might use their device. These unauthorized usages can increase the chances of cyber-attacks on your device.

Due to the long lockdown period, a small number of workers from other countries have returned home and are working remotely. Most countries have different cybersecurity laws and governmental data restrictions. The usage of unauthorized and unmonitored shared networks for work can leave the devices vulnerable especially if they are in a different country.

With the increase in employees working from home, the number of unsecured desktop devices being used has also risen. There has been a 40% rise in remote desktops being used for office work. Attackers can use brute force attacks where they systematically try all possible usernames and passwords till the correct one is found. There was a 400% increase in brute force attacks in the first 2 months of the lockdown alone.

Email scams have been trending since the pandemic began. Email scams are widespread and easy to propagate. They are also being created specifically to target users with critical data. After the pandemic started it has been reported that people are accepting emails that don't look as professional or formal as it used to. Several households are in financial trouble with salary cuts and layoffs the urgency for money makes it easier for attackers to manipulate vulnerable users.

Zoom scams and scams related to trending information are also becoming popular. The rise in usage of several online applications and services like zoom has increased the ways for attackers to gain user trust and exploit their data. Fake call centers are thriving owing to the pandemic.

Not all attacks necessarily come from outside, a disgruntled or compromised employee can create havoc with his access to corporate information. The monitoring of employees working remotely is hard, especially for bigger companies. Unlike outsider attacks, internal attacks can be more devastating since they know the system and its vulnerabilities well.

These are just some of the most common cyber threats that have been prevalent since the pandemic hit. These attacks on a corporation can cause financial, reputation, and legal issues but the good news for enterprises is that all this can be avoided by taking simple precautionary measures.

The first step would be to secure your organization with an MDM service. Once all the devices used for work are secured you have the benefits of:

Device Functionality: Most of the device functions and features can be restricted via an MDM. In cases of highly sensitive data, it would be wise to limit device functionality to the bare essentials. In other cases, you can block device features that might get exploited leaving most of the other features open.

Kiosk: Turning devices into kiosks is another method for management where the device can only be used to access limited applications set by the enterprise. Hexnode MDM has multiple options like the single app and multi-app kiosks. Users can also be restricted to just certain websites with the help of web apps.

Device partitioning: The partitioning of personal and work profiles on BYOD and corporate-owned devices ensures that any attacks on the personal profile don't affect the work profile. This allows users to enjoy their personal space free from corporate restrictions.

App management: App management features like app upgrades to ensure that the devices don't have any outdated or buggy applications, app configuration, app blacklisting and whitelisting, etc can be applied. These measures help to make sure that only enterprise-approved apps from verified locations can be used on corporate devices.

Remote actions: Remote actions like remote view and remote control can be used in cases where a device is lost or functioning suspiciously. Remote wipe is a feature that can be used as an SOS button for completely wiping the corporate data on a particular device if it is at risk of being or already compromised.

Password policies: The device and partition password complexity and history can be managed with MDMs. It helps in keeping the common passwords unique and fresh. It also prompts users to change their passwords at regular intervals.

Notifications: Broadcast messages and other push notifications can be used to constantly update employees on trending cyber threats, reminders to update passwords, etc. It helps IT admins reach all the devices used, unlike emails and messages which can be delayed or ignored.

Grouping: MDMs like Hexnode allow the grouping of devices. It helps admins categorize devices and assign different policies to each. Dynamic grouping is also available which can be used to automate tasks and policies based on device status.

Location: Geofencing is a feature that can be used to assign policies based on a device's geolocation. Companies can set up fences where the devices have more features available and step-up restrictions in areas with a higher risk. It can also be used for employees working from other cities and countries or for those that travel a lot. It helps to monitor the networks they connect to and the location they connect.

Regulations: Regulatory compliance can be a hassle, especially for companies with employees from several countries. It's not exactly a cyber threat but many countries have different cyber-security laws, some of which may require employees to turn over their data to the government or deem your data a breach of their laws. With the help of MDMs admins can check and keep tabs on employees working remotely to make sure that they are compliant. Most MDMs provide a preset policy configuration for the common data protection regulations and compliances around the world.

Blacklisting and whitelisting: Just like the blacklisting and whitelisting of applications, blacklisting and whitelisting websites are also possible. Blacklisting can be used to block certain potentially harmful websites that users access. Whitelisting can be used to limit the website access users have by blocking all websites other than the whitelisted ones.

Monitoring and compliance: With the use of MDM policies and functions the devices used for work can be constantly monitored. Instant notifications and reports can be set up for cases where devices fall out of compliance. Reports on device activity can be used to check device history and status. Alerts can be configured to send notifications to email, SMS, etc, of admins so that any major breaches of security or policies can be addressed immediately.

The deployment of an MDM solution in your company can help you manage, monitor, and safeguard corporate assets. Especially with the increase in cyber threats, it is important to take the necessary steps to secure your corporate data. The benefits of MDMs don't end at security, you also get better productivity by securing your devices, making it a win-win for enterprises.