Cybersecurity - Shared Responsibility for Telecommuters and Organizations.

By: Omair M. - omair@iosentrix.com

Omair is a Cybersecurity Executive with over 15 years of experience in security consulting, operations, research & development. Omair has experience improving the security posture of a number of Fortune 500 companies, including Microsoft, Amazon, London Underground Subway System, Bank of America, VISA, Electronic Arts (EA), Prometric (ETS), Symantec, Sony, Nintendo, and MicroStrategy.

His current endeavors include founding a Cybersecurity Consulting firm in the Washington DC Metro area that specializes in the cybersecurity needs for the startups.

Due to Covid-19, organizations are forced to allow telecommuters/work from home. That brings a new wave of challenges. For e.g., how to allow remote access securely? Which type of security controls must be implemented by the organization to keep its infrastructure, data, and employees secure? There has been an increase in cyber attacks since the Covid-19 lockdown started. Last month, phishing attacks increased by 667%. Cybercriminals want to target remote employees to gain access to the organization's data and resources.

On the other hand, the employees who are telecommuting or working from home are also worried about maintaining their cyber hygiene. Fake websites claiming to track pandemic are spreading malware and ransomware. These employees are confused as to what should be their responsibility toward cybersecurity while working from home and what falls under their responsibility.

The truth is that it has to be a shared responsibility. The organization must do its part, such as auditing, monitoring, security assessment, and providing training to the employees. The employee must also practice due diligence, such as complying with the security policies, standards, and be vigilant about cyberattacks. Below are smart tips for maintaining good cybersecurity for both the organizations the telecommuters/working from home employees.

Organization's responsibilities:

1. Enhanced Security Monitoring

Businesses are facing one of the scariest online threats currently. If recent reports are anything to go by, the global cybersecurity spend by 2020 will be over $150 billion for major businesses.

With the Covid-19 pandemic, these figures could even double when employees are allowed to work from home. As an enterprise, you could avoid getting into too many losses due to online attacks by enforcing an enhanced security monitoring of all your devices and servers including employees' endpoints.

If you don't have a Security Operation Center (SOC)/Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) in place, it would be best if you got a reliable security partner that will work with your IT team to tighten the monitoring for the enterprise and business community.

2. Make Your Employees Aware of Covid-19 Phishing Attacks

A bit of awareness and basic online security knowledge is also essential during these times. The European Union Agency for Cyber Security (ENISA) warns about Covid-19 phishing emails and fake websites.

Perhaps, the best way of protecting your employees is by creating some awareness on the same. Be sure to schedule for cybersecurity awareness training if the employees haven’t had one in the past six months. Either way, you could also run a phishing campaign to simulate a phishing attack and see how your employees perform on this test. Use this data to target the weakest departments for further training.

Most importantly, remind your employees always not to click links or download email attachments from unknown senders or senders referencing to the Coronavirus crisis.

3. Ensure All VPN Structures are working well to avoid any anomalies

Your VPN structures should be able to handle outages and possible scalability issues. Importantly, you should test VPN for outages such as high availability in various regions as well as test scalability for e.g. 90% of the workforce using VPN and see if that brings any problem or not. Additionally, mandate employees to use VPN to access the corporate network and by default connections should be re-authenticated maximum after 24 hours.

4. Update All Your Endpoint Security Tools

Cyber threats evolve pretty quickly. According to this report, over 350, 000 malicious programs are created every day. Much more could be created now that employees are switching to working from home to manage Covid-19 spread.

It’s therefore important that all employees use updated software stack including BYOD. They should have the latest OS patches, AV/EDR signatures, and updates installed to catch the latest threats as they evolve.

5. Ensure the Employees Use Cloud-Based Backups Only

Make sure that no employee uses any local backups for important files. Most importantly, you may also need to encourage them not to use any USB drives on the devices because of the threats these tools pose.

Always remind them only to use secure and approved cloud-based backups for all the essential files.

6. Enforce Full Disk Encryption

Full disk encryption is almost mandatory if your employees work from home. It works by encrypting the entire hard drive and taking care of the OS, data files and all active software programs.

It's necessary that if these devices get lost with sensitive data in them, no unverified user can access the confidential information in them.

You can use commercial tools or third-party service providers if you use low-tiered window versions. Finally, all devices, including the BYODs, should also be enrolled in MDM/EMM solutions to make it simpler provisioning and managing multiple devices while also keeping personal data separate from corporate data.

7. Run a Password Audit

As you shift to working remotely, employee passcode audits must also be in your to-do list. These should include all the passwords that employees use when accessing enterprise services.

All passwords should be redefined to meet the stringent security policy in your company. Enforce the use of MFA and strong passwords such as alphanumeric and special characters with 15 characters or more.

As an added measure, you may also consider using enterprise-level password managers to store your passwords securely.

8. Develop Strong Contingency Plan

In developing your contingency plan, you will need to triage all your teams. Make sure different groups share management responsibilities, and contingency plans should be put in place if crucial personnel may not be available.

Be sure to also assign and duplicate critical responsibilities like access to important resources, security code management, and tech support, etc., to ensure continuity just in case one key personnel may not be available for some time.

Employees' responsibilities:

1. Secure Your WiFi Connection

First, ensure that the Wi-Fi router has the latest security patches or updates installed and turn off UPnP to make your router ignore all access requests from devices in your local network to block any malicious access attempts.

Second, make sure that you have WPA2/WPA3 turned on. This will be vital in helping you lockout malicious unauthorized devices from accessing the network. Insecure Wi-Fi connections do not use any form of encryption for data that moves across their airwaves and makes it very easy for eavesdroppers to sniff on your traffic and steal your private information.

Lastly, ensure that your devices connect to a trusted Wi-Fi network only. Anyone can spin up a Wi-Fi within your proximity with the well-known SSID, e.g., name of a common internet provider, and your device may automatically connect to such a network. This would be equivalent to using a public Wi-Fi network, which is used to compromise user's credentials, systems, to spread malware, or for DDOS attacks.

If you work from home, therefore, you must secure your Wi-Fi connection.

2. Strong VPN Connections

Virtual Private Network (VPN) connections are must-have if you wish to secure your traffic from insecure Wi-Fi or would like to gain access to the internal corporate networks securely. They will help you create a secure connection with the company devices and ensure that man-in-the-middle attackers cannot interfere with the data you receive or share.

You must use a corporate VPN with a full tunnel because it provides you with a secure and encrypted tunnel for transmitting data between your home computer and the company's network.

Even if you work for yourself, it’s still advisable that you get a reliable VPN connection to protect your privacy. Remember to choose a provider that offers privacy protection.

3. Update all your Systems to Latest Versions and Security Configurations

It’s prudent that you don’t put off software updates for too long. If you use, for example, Mac or Windows laptop, make sure that you have all the latest updates installed.

For your information, these updates usually come with repairs and patches that repair security holes in the programs and remove bugs in them. The updates also improve the performances of these devices.

As an extra measure, be sure to install reputed AntiVirus/AntiMalware and ensure that all of them are up to date. This will help you defend against new threats as they emerge.

4. Avoid the Use of External Peripherals

The inexpensive nature and portability of external peripherals like USB sticks/USB drives make them a desirable option for attackers to spread viruses and malware. Some of these viruses are so sophisticated that they will ‘know’ immediately when you insert the USB sticks to your computer and initiate malware download.

Your best bet, therefore, is not to use any untrusted storage devices that you find anywhere. If you have to use them, only use company authorized devices that are protected with enterprise-level encryptions.

5. Keep Your Personal and Corporate Emails Access Separate

It's never a good idea to mix your personal emails with corporate emails because your personal emails may not have DLP and anti-spam/anti-phishing protections on the mailboxes as you would have on corporate emails. Because of this, you could be exploited via personal email, and then attacks could be launched on the corporate assets and network.

6. Always Use MFA

Multifactor authentication is a security system designed to help in verifying the user details through multiple credentials. When you use it to authenticate the VPNs, Emails, and other vital resources, it won't ask for the username and password alone.

Instead, it will also request for extra credentials like "secret security code that's sent to your smartphone, facial recognition, fingerprint detection, security token or answer to security questions," etc.

This is critical in that if any of your credentials are leaked, the threat actor won't be able to access your accounts and gain authorized access to the data or resources.

7. Do Not Click Links or Download Email Attachments from Unknown Senders

Did you know that over 90 percent of malware is usually delivered via email? Well, it involves a social engineering attack mechanism–phishing, which is also responsible for over 80 percent of reported cases.

The attacker's goal is always to convince you to click malicious links or download malicious attachments in your devices. If you wish to be safe; therefore, don't click any links in emails from unknown senders or download attachments.

Also, during this period, be wary of emails referencing to Covid-19 and those pressing you to download attachments or click links in them. Usually, these links will lead you to malicious websites where malware is installed on your computer/laptop in seconds.

Wrapping Up:

The Covid-19 pandemic has caused a bit of panic, but we all need to stay cool at this moment if we wish to keep safe both health-wise and security-wise. Maintain the isolation to avoid the spread but also ensure all the online-security best practices are followed to prevent any cyber-attacks.

Remember that cybersecurity is everyone's responsibility. Understand your part and follow the tips to stay secure.