How Businesses Can Securely Work From Home

As the novel coronavirus (COVID-19) continues to spread, many businesses are assessing how they can prioritize their employee safety and still maintain regular business operations.

One solution many businesses are turning to is recommending employees to work from home to avoid potential illnesses. To help ease the burden on businesses, Microsoft, Google, LogMeIn, Cisco Webex, and Zoom are providing free remote working tools.

With the likely increase in remote work, companies will have to prepare in various ways to avoid cybersecurity risks or interruptions to business. "When supporting a remote workforce, understand that security controls shift. Therefore, firewalls, DNS, and IDS/IPS could be ineffective when employees head home. Most environments that support VPNs should be able to protect the remote user, be sure to account for the bandwidth of users and remote desktop sessions," said Dan Garcia, Senior Information Security Engineer II at Datto.

CISA's VPN Guidance

The Cybersecurity and Infrastructure Security Agency (CISA) released an alert to encourage organizations to adopt a heightened state of cybersecurity. According to the CISA, remote work options require a VPN solution to connect employees to an organization's network. The CISA encourages organizations to review the following recommendations when considering alternate workplace options:

- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations. See CISA Tips Understanding Patches and Securing Network Infrastructure Devices.
- Alert employees to an expected increase in phishing attempts. See CISA Tip Avoiding Social Engineering and Phishing Attacks.
- Ensure IT security personnel are prepared to ramp up the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery. Per the National Institute of Standards and Technology (NIST) Special Publication 800-46 v.2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, these tasks should be documented in the configuration management policy.
- Implement MFA on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords. (See CISA Tips Choosing and Protecting Passwords and Supplementing Passwords for more information.)
- Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications—such as rate limiting—to prioritize users that will require higher bandwidths.
- Contact CISA to report incidents, phishing, malware, and other cybersecurity concerns.

The CDC has released some best practices for a disease outbreak plan:

- Review human resources policies to make sure that policies and practices are consistent with public health recommendations and are consistent with existing state and federal workplace laws (for more information on employer responsibilities, visit the Department of Labor's external icon and the Equal Employment Opportunity Commission's external icon websites).
- Explore whether you can establish policies and practices, such as flexible worksites (e.g., telecommuting) and flexible work hours (e.g., staggered shifts), to increase the physical distance among employees and between employees and others if state and local health authorities recommend the use of social distancing strategies. For employees who are able to telework, supervisors should encourage employees to telework instead of coming into the workplace until symptoms are completely resolved. Ensure that you have the information technology and infrastructure needed to support multiple employees who may be able to work from home.

In addition, managed service providers (MSPs) are recommending the following best practices and advice for how businesses can remain secure through potential remote work scenarios.

- **Use a Secure WiFi Network:** If possible, you should work on your secure, private home network instead of relying on public WiFi. If you send your data through an unsecured WiFi connection, you lose the power of privacy making it possible for cybercriminals to intercept your data. You may be putting personal information at risk if you are accessing your email account or sending sensitive data over a public WiFi network. It's essential to ensure your network is secure through the use of a VPN and a strong password that isn't easily cracked.
- **Secure Your Home Workstation:** Ensure you have fully patched and updated anti-virus and anti-malware software. It's important to follow the same best practices you would as if you were in the office, and report any suspicious activity or concerns to internal IT or your MSP.
- **Coordinate With Your Internal IT or MSP:** When working remotely, it's crucial to continue your typical cybersecurity best practices and reach out with any questions or concerns.

SUMNERONE

We're here to help.

SumnerOne

800.325.0985

www.sumnerone.com