Working Remotely & Securely

As of the second week of March 2020, a survey of 500 U.S. companies found that only 62 percent of the businesses had any type of business continuity plans in place, and roughly 20 percent said though they had "some plans" in place, but they were not comprehensive. Half of the organizations said their plans accounted for emergency operations for two to three weeks, while an astonishing 5 percent confessed theirs would only carry them for a day or two.

Of these 500 businesses, less than 40 percent felt they had the right technology in place to allow their total workforce to transition to a remote environment, and nearly 20 percent said none of their employees had the right technology to allow remote work.

This lack of planning has caused an unprecedented surge in usage for both/teleconferencing solutions as well as collaboration/communication/cloud services as companies scramble to get solutions in place that enable their employees to work and communicate from home. Moreover, the realization that an alarming number of organizations were far less prepared to react to any type of emergency, became widely apparent early-on.

Telecom providers indicate they've seen usage soar over 2,000 percent in the U.S. alone since the pandemic started, and internet traffic attributed to video conferencing has increased roughly 200 percent in Asia and North America.

Similarly, with the sudden influx of remote employees, Microsoft reports a 775 percent jump in demand for cloud services such as Windows Virtual Desktop, Power BI, and Teams, which has forced the company to prioritize demand for their customers most in need.

As organizations rushed to address the immediate needs of their newly remote workforce, these same organizations now need to ensure that all of the new solutions they've been implementing are secure and, perhaps even more importantly, that their employees are following best practices for cybersecurity while working remotely.

Ensuring the proper protocols are in place to allow employees—especially those that haven't previously worked remotely—to access business-critical applications and documents without opening the network to vulnerabilities may not have previously been on the radar. Additionally, knowing how to maintain security when employees are working remotely looks a little different from when an entire workforce works from a single location.

First and foremost, every business needs to have a work from home security policy that ensures sensitive information receives the same level of protection on a remote network as it would on the company network—and make sure there is a mechanism in place to ensure this policy is being adhered to. Businesses using Microsoft, for example, can leverage Group Policy Settings to help prevent data breaches and make the organizational network safer by configuring the security and operational behavior of company devices through Group Policy (a group of settings in the computer's registry).

Together with Active Directory, which organizes a complete hierarchy including which computers belong on which network and which users have access to the storage room, Group Policy Settings can prevent users from actions such as accessing specific resources or running scripts.

Mandating that remote users connect to the organization's network using a VPN (virtual private network) and placing them behind the company firewall with the corporate security policy in place is an absolute necessity. A VPN routes a device's internet connection through the VPN's private server instead of the internet service provider (ISP) so that when data is transmitted to the internet, it originates from the VPN rather than personal computers.

In addition to ensuring employees' connections to the internet and internal networks are secure, the security of cloud-native applications and environments is also critical.

While a Fort Knox-level security environment does not need to be constructed, particularly when attempting to build up defenses on short notice, organizations need to ensure all cloud applications are encrypted at the application layer, and, when available, a WAF (web application firewall) is also a great layer of protection to add to your public cloud environment. A WAF helps protect web applications by filtering and monitoring HTTP traffic between a web application and the internet.

The cloud is typically one of the most secure methods of storage for the simple reason that the data centers are housed in facilities with strong physical protections, redundant power, and tested disaster recovery procedures. In addition, reliable cloud service providers can provide evidence of verification and frequent validation by independent auditors.

Lastly, one of the top security risks with a remote workforce is simply the potential vulnerabilities of employees' home networks. With the volume of IoT devices in the average American household—from Alexa and Google Home to security systems and appliances—no shortage of risks exist to a remote worker. Something as simple as an infected file unwittingly downloaded by a family member living dormant on the network can potentially affect the organization if employees are connecting their own devices to the corporate network.

Similar to a work from home security policy, organizations should ensure that they have both a BYOD (bring your own device) policy as well as an acceptable use policy in place is a critical factor in keeping your network free from infections or attacks through an unintentional security breach via an employee's home network.

While the world right now is offering many uncertainties for businesses and individuals alike, some of the most important things we can do to help ease the fear of the unknown. Be prepared by making plans and contingencies, maintaining clear, direct communication, and, more than anything else, demonstrating an abundance of patience and empathy toward other businesses, departments and, of course, each other.

Storyline by Amanda Johnson