BlackBerry. Intelligent Security. Everywhere.

The Implications of Securing Remote Work

Did You Know?

PRIOR TO COVID-19

31% of employees reported working from home at least one day per week

9% of employees were working from home full time

27% of companies had formal full-time work-at-home programs

42% had part-time work-at-home programs

More than half of the companies that had employees currently working from home were not formally prepared for this transition.

SINCE COVID-19

77% are now working from home after the stay-at-home orders

Because malicious actors are always ready to attack, there have been significant increases in attacks and a growing exploitation of COVID-related tactics.

The **U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)**, and the United Kingdom's **National Cyber Security Centre (NCSC)** issued a joint alert stating: "Both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations."

The **World Health Organization (WHO)** reported a significant increase in attacks directed at WHO employees. "Scammers impersonating WHO in emails have also increasingly targeted the general public in order to channel donations to a fictitious fund and not the authentic COVID-19 Solidarity Response Fund. The number of cybeattacks is now more than five times the number directed at the Organization in the same period last year."

What You Can Do

Here's Your Checklist for Success When Securing Remote Work

1 **Educate users on the new risks** in terms that will cause them to change their behavior. Focus on three priority actions:

Social engineering: Make sure people understand the company's technology is not the target, they are. Fear, crises, curiosity, and urgency are the attacker's greatest weapons. The more urgent the message is, or the more it's pressuring a person to ignore or bypass company policies, the more likely it is an attack.

Passwords: Reusable passwords are the Achilles' heel of security, but because of the resources required, organizations are unlikely to be able to make the move to two-factor authentication right now. Don't force staff to use long strings of forgettable computer-generated digits, and don't force them to regularly change passwords. Use of passphrases and password managers can help simplify and improve security for the workforce.

Updating: IT operations still control work laptop operating system updates for most organizations, but it's important to also tell employees to turn on auto-updates on their home PCs, work computer browsers, phones, and tablets. Using the latest version of apps or browser extensions will not only ensure the latest security features are available but invariably raise the bar against attackers.

2 **Confirm VPNs and other remote access methods** have the capacity to meet the increased demand and can enable security visibility as well as rapid detection and response to attacks.

3 **Enhance web, email, and DNS protections** and make use of these services for threat intelligence. Attackers move rapidly to modify phishing and ransomware campaigns to take advantage of confusion and crises.

4 **Improve mobile device management** of personally-owned devices and isolation/segmentation of those devices to reduce exposure. This is key to enabling business while reducing risk because bring-your-own-device policies have been a security issue for over a decade now.

5 **Optimize increased management attention** to the security issues that are getting daily press coverage. Use it to get support for stronger authentication and privilege management, faster patching and backups, and more use of persistent data encryption.

For more information about best practices for making and keeping work at home operations safe and productive, access the full **SANS report here.**