Remote Access and Best Practices

Cybercriminals are now leveraging our national crisis to target businesses of all sizes by launching cyberattacks and phishing campaigns in order to exploit us at a potential time of weakness. There have been warnings issued by government agencies related to cybercriminals targeting businesses that are turning on remote access to their systems in order to help with business continuity. Remote access is a very powerful tool but, if not implemented correctly, may result in a cyber or ransomware attack against the business. As businesses rush to close their physical operations and move to a remote workforce, the improper configuration of these remote access systems can be an easy way for cybercriminals to attack. Please follow these best practices for remote access:

1. Unless your IT resources clearly understand the risks associated with using Remote Desktop Protocol (RDP), do not allow them to install it. RDP is a highly exploitable technology that is a primary target of cybercriminals.

2. Utilize a remote control software that allows you to "log in" to a computer at your office.

3. Make sure the remote control software utilizes Multi Factor Authentication (MFA) so it makes it more difficult for a cybercriminal to hack into your system. MFA sends a text message to your cell phone or an App on your phone to authenticate your log in.

4. Utilize strong passwords that incorporate multiple words, numbers and special characters for the authentication for the remote control software.

5. If you are using a VPN, make sure your IT vendor has updated all the VPN software. As of just a few months ago, many VPNs had vulnerabilities that could allow a breach to occur.

6. Make sure all remote computers are running the latest versions of Windows 10 or MAC.

7. Make sure all remote computers have anti-virus software installed and the virus definitions are up-to-date.

8. Use strong passwords on all remote and host computers that incorporate multiple words, numbers and special characters.

9. For Wi-Fi enabled devices, use the strongest encryption protocol available. WPA3 is the newest. At a minimum, you should be using WPA2.

10. Do not allow family members to access any device that is used to remote into a work computer.

11. Make sure you lock the computer before you walk away from it. On a Windows computer, this can be done by pressing the "Windows" key and the letter "L" at the same time.

Data Backup

1. Confirm that 100% of your data is in fact being backed up.

2. Before you leave the office, make a backup of ALL your data. This includes imaging, patient databases, attachments, financial systems, images, etc. This backup should be saved to an encrypted external hard drive that is stored offsite.

3. Confirm that all your cloud data backup is up- to- date and all your systems are being backed up.

Phishing Attacks/Social Engineering

Cybercriminals are now leveraging the current COVID-19 crisis as a methodology to attack systems. Be extremely careful when receiving any emails related to the COVID-19 infection. These phishing emails are designed to lure you into clicking on links or attachments that may seem relevant to the current situation. In addition, "heat maps" that show the infection rates may direct you to a fake website that will download malicious code onto your device.

Signs of a COVID-19 Phishing email may include:

- A link to a “heat map” showing the infection areas/rates
- A link to a fake government or state agency designed to look real
- A link to a government or state agency with a legitimate name, but a fake hyperlink
- A warning to download a document related to COVID-19
- A link to a hospital or other healthcare institution

Please be extremely careful regarding these types of emails and always use the link hovering technique to verify the final destination. Place your mouse over the link or image, look at the bottom left corner of your screen and validate the URL (web address).

For additional information, please contact Black Talon Security at 800-683-3797 or visit us at blacktalonsecurity.com