Becker Becker & Poliakoff

Cybersecurity During COVID-19

March 24, 2020

By: Jack S. Kallus

By now many of your employees are working remotely. As an employer, this poses an increased risk for a cyber incident to occur. Cyber threat actors are preying on the concerns associated with COVID-19 and using the hysteria as a launching pad for cyber-attacks. These attacks can have significant consequences.

Many federal agencies along with local law enforcement have issued alerts addressing cyber vulnerabilities. Some of these alerts focus on risks associated with virtual private networks (VPNs), which organizations use to allow employees remote access to their servers and workspaces, others focus on current scams being attempted worldwide by criminals. Organizations need to be extra vigilant during this time period and may need to adopt a heightened state of cybersecurity to prevent against these attacks. Some of these measures may include updating VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches, and security configurations. Enabling multi-factor authentication as a requirement for all employees utilizing a VPN is also an essential tool in preventing attacks. Organizations should also pay close attention to their incident response and recovery plan.

Phishing attacks using “social engineering” have been on the rise since the COVID-19 outbreak. Threat actors have taken advantage of the COVID-19 outbreak and have utilized phishing emails from entities posing as the World Health Organization or the Centers for Disease Control and Prevention to entice users to provide sensitive information. Other methods used by these criminals have been creating malicious websites and apps that appear to share virus-related information to gain and lock access to devices until payment is received. These criminals have also circulated an email, which purported to contain attachments with useful information on how to protect against the spread of coronavirus, how to detect it, and news updates. However, the attachments contained malware capable of destroying, blocking, modifying, or copying and exfiltrating personal data, as well as interfering with victims’ servers and networks.

Organizations should ensure that their employees are up to date on security awareness training and consider requiring employees to undergo additional training measures in the context of COVID-19 amid increased remote access (or at least issue periodic alerts to their employees identifying common scams). The DOJ issued a COVID-19 Fraud Alert which can be found at: https://www.justice.gov/coronavirus. If you think your organization is a victim of a scam or attempted fraud involving COVID-19, this website provides contact information to report the incident.

Protecting your organization and its servers from, and against, any cyber threats and/or attacks from the risks posed by the COVID-19 outbreak should be a focus during this time period.

Should you have any questions or concerns, Becker’s Data Privacy, Protection, & Cybersecurity team can assist your business during this time.