The MEARIE Group
TheReciprocal
Managing risk together

Further Cybersecurity Precautions Recommended While Managing Coronavirus Logistics

Preparations for managing your workforce to limit the spread and impact of the COVID-19 epidemic at your organization may be top of mind this week. Another aspect of this matter is to ensure cybersecurity threats are managed in tandem with this development. A disruption to business, particularly related to higher than typical employee absenteeism, may leave your company more vulnerable. Your company may be considering the activation of contingency and business continuity plans which may include more employees working from home to limit the spread of the virus. In this scenario, secure networks are more critical than ever. To remain operational and secure, the following steps should be considered:

Defense against the Phishing Wave

Malicious actors may leverage the intense focus placed on the personal fears the epidemic is creating. According to Jamil Jaffer, Vice President for Strategy and Partnerships at IronNet Cybersecurity, "Bad actors are already using COVID-19 and people's desire for information as a phishing and malware distribution opportunity."[i] Security best practices might be forgotten in this environment.

It's a good time to remind staff of the need for vigilance and the dangers of opening attachments and links from untrusted sources. Up-to-date antivirus and monitoring tools can limit the effectiveness of successful spear phishing attacks, particularly if staff are using their own devices while working from home.

Elevated System Testing

With increased network traffic, based on additional remote workers, more vigilance is required. Cybersecurity resources are recommended to increase monitoring for unusual activities deriving from work-from-home users, particularly as employees' personal computers can create a more vulnerable endpoint on the network.

There is a risk that the increased volume of network traffic will place a strain on IT systems and personnel and that employees will be accessing sensitive data and systems via unsecure networks or devices.

Your company's ability to maintain network integrity while allowing remote working and Bring-Your-Own-Device (BYOD) practices is important. The secure use of virtual private networks (VPNs) and the implementation of multi-factor authentication are key. Patching protocols should apply to VPNs in addition to other enterprise software and hardware.

Brace for Disruption

In an office environment, if a cyber threat is detected, IT resources can immediately quarantine the device, disconnecting the compromised computer from the corporate network and conduct investigations. Where users are working remotely, organizations should ensure that, to the extent possible, IT and Security colleagues are available and ideally able to physically address a compromise at its source.

Sophisticated endpoint detection and response (EDR) software can also be used to quarantine workstations remotely, limiting the potential for malware to move through the network.

In the event of a network security or privacy breach incident, ensure to notify MEARIE as early as possible in the issue identification process, particularly if you require additional resources:

Regular Business Hours:
MEARIE: 1-800-668-9979 ext. 5324
claims@mearie.ca
After Hours:
MEARIE: 647-223-9243
Cyber incident-specific - 24/7 After Hours with Crawford: 1-844-660-4903

The COVID-19 situation has raised several concerns for businesses and the public. A bit of extra risk management planning can help to reduce the threat of a cyber incident while also managing your workforce through this epidemic.

[i] Walton, Robert. "Utilities on high alert as phishing attempts, cyber probing spike related to Coronavirus." *Utility Dive*, . https://www.utilitydive.com/news/utilities-on-high-alert-as-phishing-attempts-cyber-probing-spike-related-t/573698/. Accessed 9 Mar 2020.

The MEARIE Group
3700 Steeles Avenue West, Suite 1100
Vaughan, Ontario L4L 8K8
905.265.5300 | 1.800.668.9979
mearie.ca

Managing risk together