Adjusting to the New Reality: Cyber Threats During the COVID-19 Crisis

Working remotely during the COVID-19 pandemic has been a lifesaver, but it has also brought new threats.

Working from home allows people to minimize social interaction, which limits and slows the spread of COVID-19. But, as highlighted in a recent alert from the North American Electric Reliability Corp. (NERC), the electric power industry "is in a period of heightened cyber risk due to a large contingent of industry employees working remotely."

As remote working ramped up in response to COVID-19, there has been an increase in opportunistic actors who are testing the defenses of businesses as their workers shift to home offices, NERC said.

Cybercriminals, for instance, have targeted remote work technologies, such as video conferencing services even as many of their targets, employees working remotely, are more vulnerable by being distracted by domestic circumstances and anxiety about the threat of COVID-19.

And, in many cases, those employees and their employers are even more vulnerable because they are working on computers that had to be made secure quickly.

"We are lucky to be able to do it, but working from home comes with risks," said Scott Kaylor, manager, Member cybersecurity and networking services at National Information Solutions Cooperative (NISC).

"Overall, our workload for supporting our Members in their work-at-home transition has increased by at least three times," Kaylor said. "We are still seeing Members sending workers home and our calls are still about two times what they are under normal circumstances."

With so many employees working from home, "the threat has grown immensely because now you have all these unknowns," Kaylor said. All those devices greatly increase what IT experts call the "attack surface" available to cyber criminals.

Work-From-Home Security Challenges

In late April, the FBI's cyber division reported receiving 3,000 to 4,000 cybersecurity complaints each day. Prior to the COVID-19 pandemic, the unit received about 1,000 complaints a day.

Part of that challenge comes from trying to provide high-level information technology security in an environment that had to be put in place quickly. A utility's IT department has little control of how an employee connects to the internet when they are working from home. "A virtual employee is more of a challenge" from a security point of view, Kaylor said.

Many home users, for instance, have off-the-shelf wireless routers, which are far more liable to being hacked than more expensive business-grade routers. In addition, the personal computers people use at home tend to be old, so their operating systems might not be up to date with the latest security patches.

Tommy Higginbotham, information services manager at Colorado-based electric cooperative Mountain View Electric Association, an NISC Member, echoed Kaylor's comments about the risks of working from home.

"We have employees that are working from home and there is no way for us to understand what their environment is like or to investigate their setup," Higginbotham said. "We are relying heavily on the security that was already in place with a few minor changes to protect our environment."

Those risks are compounded by the fact that the pandemic has people on edge, making them more vulnerable to fall for a phishing scam. People are more likely to search on topics such as "pandemic" or "stimulus check" and that creates opportunities for criminals, Kaylor said.

In the first three weeks of March, security firm Barracuda Networks detected 467,825 spear-phishing email attacks, of which 9,116 were related to COVID-19. In February, the firm detected just 1,188 coronavirus-related spear-phishing attacks and only 137 in January.

Increasing Vigilance

With so many people working from home, training is more important than ever. “There is a lot of need for educating employees from a social engineering perspective,” Kaylor said. Cybercriminals are always looking to exploit weaknesses. The COVID-19 crisis has made people more anxious, so employees need to be even more vigilant, he said.

Repeating and reinforcing lessons and training about social engineering, that is, cybercriminals’ efforts to manipulate and deceive people, is one of five recommendations NISC is making to its Members during the COVID-19 crisis.

NISC recommends employees should be reminded to look for some basic telltale signs that an email might, in fact, be a phishing campaign. Is the spelling correct? Does the sender match the email address? Am I expecting this email? Does the email want me to click on or download something? Who should I contact if I see something malicious?

Another vulnerability that has emerged and become more prevalent as more people are staying at home is an increased use of tools such as video conferencing. Increased use has made the flaws in tools such as Zoom video conferencing more visible. A simple solution, NISC recommends, is to password protect meetings and only allow the meeting host to share their screen.

With so many people working remotely, their homes essentially become a virtual branch office that must be made secure. “It is best to clearly list expectations for the staff as security comes more naturally to some than others,” Kaylor said. “Make it be known what is expected of all staff.”

He recommends having a secure, password-protected WiFi connection, locking computers when they are not in use, and properly filing papers and safely storing work files and documents.

“It should also be made clear to employees working remotely that updating is not optional,” Kaylor said. He recommends being sure that firewalls, laptops, desktops, email, mobile devices and printers all have the latest patches and updates applied. “Staying up to date effectively closes the weaknesses that cybercriminals are exploiting,” he said.

Work-from-home mandates have also opened potential vulnerabilities with payment systems. Many utilities have closed or limited customer access to offices for functions like paying bills. “When we move employees to an untrusted place, such as a home office, we must either fortify the new location or leave what would otherwise be vulnerable services within the trusted environment,” Kaylor said. “With Payment Card Industry (PCI) compliance, that is every bit the case.” He noted that NISC’s e-commerce solutions allow customers to make payments to those avenues without compromising PCI compliance or cardholder data.

Even though it may not have been widely used, the ability to work from home is a valuable tool.

Right now, it is hard to estimate the effect work-at-home mandates have had on the spread of COVID-19, but it is likely to turn out to be a contributing factor in slowing the spread of the virus. In addition, the flexibility and benefits that working remotely gives both employees and employers may become more apparent and attractive in the post-pandemic world where working-from-home arrangements become more widely used.

As the post-pandemic environment emerges, “it will be very important to get the right technology to make cybersecurity as seamless as possible,” Kaylor said.

This sponsored advertising feature was published May 4, 2020, by the American Public Power Association.

For more information, visit NISC.coop or contact us at:

cybersecurity@NISC.coop
866.999.6472

nisc™
www.NISC.coop