From Assessment to Action: Defending Against Cyber Attacks

It seems like every day brings news of a new cvbersecurity threat, whether it is a sophisticated phishing attack or the latest malware developed by bad actors. No utility, large or small, is immune from cyber attack.

While they recognize the seriousness of this issue, many public power utilities are not sure how to track potential threats or put defenses in place. The path is complex and can seem daunting.

A robust option to monitor threats is the Electricity Information Sharing and Analysis Center portal run by the North American Electric Reliability Corporation. The E-ISAC portal monitors threats specific to the nation's electric grid and sends alerts to all subscribed utilities.

In terms of taking action to protect against threats, the American Public Power Association's Cybersecurity Scorecard is a good starting point. The scorecard is an online self-assessment tool to help public power utilities understand their cybersecurity strengths and weaknesses. Along with a score on their cyber posture, utilities completing the self-assessment receive personalized recommendations on systems and processes they need to put in place.

John Kuhlman, Information Systems Manager at Decatur Utilities (DU), Alabama, with 165 employees, noted that the utility's last IT audit showed that employee cybersecurity training needed to be strengthened. "Increasingly, all of our systems and staff rely on the Internet. We are constantly pushing and/or pulling electronic data to and from our customers, vendors and contractors. With that, we expose ourselves to all kinds of cyber risk," he said.

The utility took the risk of cyberattack to heart and decided to partner with National Information Solutions Cooperative (NISC) to bolster their programs. The St. Louis-based information technology organization develops, implements and supports software and hardware solutions for more than 850 primarily-US based public power, electric distribution cooperatives, independent telephone companies, and other entities.

The move was a logical outgrowth of a partnership the utility and NISC established in 2012. DU started with NISC Accounting & Business Solutions, designed to streamline and expedite business processes.

More recently, DU expanded to use NISC's enterprise-wide solution, along with two of its cybersecurity products: CyberProtect and CyberAcademy.

Before then, DU had been using off-the-shelf security software. After trying at least six different products, Kuhlman lost confidence in the ability of the commercial brands to defeat the growing cybersecurity threat. Like many organizations, DU was up-to-date in securing its basic IT operation. The wildcard was the many users on the system who might inadvertently open the door to an attack.

"We were pretty secure with hardware and software, the one thing we were lacking was the end-user education on cyber risk, things to look for in emails, safe Internet surfing, items from our end-users standpoint," Kuhlman said.

NISC's CyberProtect is designed to block hackers from using malware and other unwanted applications that attack and exploit vulnerabilities in information systems. CyberAcademy works on the human side of the security coin. Since employees are the first line of defense against cyberattacks, CyberAcademy helps them learn best practices. The program not only educates staff on security issues via interactive training, but also tests and measures their ability to recognize phishing attempts.

Attacks Become More Sophisticated

Kuhlman noted that phishing attacks are getting more sophisticated, so it is important to train employees to spot them. Malicious sites and emails increasingly mimic those that are familiar to users.

"They're just trying to grab personal information. We saw it just the other day with an email from a legitimate company that we do business with. They got attacked and 'they' sent a link out asking our users to fill out this form. The form was just asking, basically, for username and password information," he said.

That raised an immediate red flag for Kuhlman. “Why would you need to give a vendor this type of information? And why would they be asking for that?” He noted that these emails can come from a legitimate source but when you look at the link you may see it is going to a different country — evidence of a cyberattack.

“We try to train users to hover over the link and it will show you on the page where it’s going before you actually click on it,” he said.

That’s why NISC’s cyber training is so important, he said. Kuhlman also recognized that DU needed help in keeping its cybersecurity efforts up-to-date, a demanding task for a small utility, especially in light of the fact that cybersecurity programs and software are so frequently updated. NISC provides an outsourced service, managing the program on behalf of the utility.

“These are things that we don’t want to try to manage ourselves, so the NISC platform and program were just what we needed,” he said. “We don’t have to maintain or worry about upgrading the product, or make sure that it is working properly. Being such a small IT shop (six employees), we really don’t have the internal resources to dedicate to that.”

Outgrowth of NISC’s Self-Protection

Jeff Nelson, NISC General Council and Vice President of Information Security & Risk Management, said his company’s utility cybersecurity program evolved out of its own efforts to secure its home base.

“NISC initially invested heavily in cybersecurity to protect our own organization’s data and that of our members from damaging attacks. We now make these solutions available to all interested utilities and telecoms,” regardless of whether they are currently using other NISC solutions, he said.

DU liked NISC products so much that they decided to launch an enterprise-wide NISC solutions expansion. This program includes customer care and billing; SmartHub, a customer facing web portal with document management and payment channels; as well as engineering and operations IT solutions.

The products integrated seamlessly with DU’s ongoing employee training, Kuhlman said.

“Employees were used to online training for their application products. And now, as an administrator, I can actually push out which training I want each end-user to complete and when I want to complete it by,” he said.

DU also sometimes pushes out test virus emails, a scam or a phishing email to see who responds. This signals to Kuhlman which employees may need some additional training.

The Value of the One-Stop Shop

In the battle of clichés, “Don’t put all of your eggs in one basket” versus the efficiencies of “one-stop-shopping,” DU has definitely taken sides. When it comes to IT software management, one-stop-shopping wins.

Too often when there is a failure, the company found itself dealing with various product makers that each blamed the other, he said.

“Through the years, we’ve just added so many product extensions for our billing system and our customer-facing portals. And it’s just gotten to be a nightmare to manage all of these different third parties,” Kuhlman said.

While NISC has competitors, the company is further along in developing product management systems
than other vendors, Kuhlman said, so it was natural to reward them with additional responsibilities. “NISC was one of the first to get into the enterprise model from the utility standpoint,” he said. “Just one phone number to call, and we can rely on them to handle it.”

For more information about NISC enterprise software solutions, visit www.NISC.coop.

This sponsored advertising feature was published Aug. 28, 2018, by the American Public Power Association.