CAPCO

STRENGTHENING IT TO HELP UTILITIES WITHSTAND CYBERATTACKS

Employees and non-employee contractors continue representing the most critical weak link in the IT chain. Too many employees, and vendors using corporate networks, are still falling for phishing attacks. Enhanced worker training on cyber risks helps, but training coupled with stronger systems offers the best protection against cyber threats.

When Colonial Pipeline was hit by a ransomware attack in early May 2021, there could not have been a clearer sign that utilities are still acutely vulnerable to cyberattack – and that it's not only their operating technology (OT) systems that are being targeted.

It didn't take long to discover it was the corporate IT network that had been breached. Colonial pre-emptively shut down its OT side to prevent the attack from spreading – sparking a momentary national crisis by temporarily stopping the supply of nearly half the gas, diesel, and jet fuel piped to the East Coast of the U.S.[1]

The attack demonstrated that no matter what security systems utilities have built around their OT, they must include IT in the cybersecurity calculus. As noted in Part 1 of this mini-series , earlier iterations of OT systems were often air-gapped – isolated and thus more difficult to attack. Today, the lines are blurring fast as OT systems become more digitized.[2] Furthermore, employers and the vendors on whom utilities depend are increasingly susceptible to ever more cunning maneuvers by cybercriminals.

Experts indicate attacks against the IT networks of energy suppliers are common. Studies show that proportionately, energy companies and utilities are targeted more often than other sectors, showing higher rates of everything from internal reconnaissance, such as file share enumeration and port scans, to lateral movement attacker behaviors and data exfiltration activities. All such attacks should be seen as precursors of attacks on ICS or SCADA systems.[3]

3 BEST PRACTICES TO PREVENT ATTACKS ON IT INFRASTRUCTURE

Our decades of experience working with the power sector point to three key areas that can do much to blunt the edge of attacks on IT infrastructure. While these are not unique to utilities, they have the benefit of a broad base of knowledge drawn from widespread application:

Endpoint security

The key here is to focus on the need to secure all IT equipment – including smartphones – and to train the users effectively. Effectively securing this vector requires IT professionals to use a variety of tools to deploy, manage, and secure the devices, applications, and data that workers require to perform their jobs. It may also leverage endpoint detection and response or application controls.

Phishing – e-mail fraud, essentially – is the most prevalent form of attack on business networks. It's likely the Colonial Pipeline breach was a phishing e-mail attack, in which case tighter endpoint security and perhaps training could have stopped it.[4]

There is no shortage of tools available to help protect IT networks from phishing.[5] Phishing campaign simulation and email inspection tools are table stakes to provide basic protections. Security orchestration, automation, and response (SOAR) technology is an evolution beyond the basic tools to coordinate, execute, and automate tasks between employees and tools.[6] Security teams can use SOAR tools from providers, such as FireEye, IBM, and Palo Alto; these tools can triage and respond to basic phishing attempts and escalate more complex occurrences to an analyst for further evaluation. The tools monitor and analyze applications and files while blocking anything deemed malicious by the security policies established by the organization's security operations center (SOC). The tools can also send alerts about potential hacks and enable the teams to take immediate action, such as isolating a hacked device.

Where utilities lack the competencies or perhaps the resources to set up and coordinate anti-phishing activities or need assistance leveraging a SOAR platform as a force multiplier, they can partner with service providers. Experienced and competent third parties can oversee all stages of the project management lifecycle, from requirements gathering and solution selection to operational handover; they work closely with the organization's SOC and with key stakeholders during deployment. They can also help gather and document all technology requirements and participate in defining scope, budget, staffing, and scheduling of the software implementation.

Endpoint security is not a trivial exercise. In fact, it's a moving target, requiring non-stop attention as user behaviors change. Many utilities have had success in accommodating employees' shifts from the desktop world to company-issued laptops and tablets; not all have fared as well with the bring-your-own-device trend, or with the proliferation of smartphones.[7]

Data classification

Another weakness in IT systems is that data exists in many different formats, systems, and storage mediums. Knowing what data is where makes it that much more difficult to determine the likelihood of data loss, let alone understand the risks. Without holistic data classification, users can inappropriately access sensitive data, risking the loss of data through accidental or malicious exfiltration.

Best practice in data classification calls for researching data classification levels and approaches used across industries and deciding on options for data classification categories appropriate to the utility's particular needs. Once key stakeholders have signed off on those categories, it's necessary to standardize, update, and provide recommendations on information classification policies, and to move quickly to interviewing key business and IT leaders while analyzing the data elements to determine their sensitivities. When those inputs have been reconciled, the utility can then build a master data classification matrix. Quite often, this exercise uncovers unknown applications and provides key updates to a firm's master list of IT systems.

As with endpoint security, data classification keeps evolving – especially as more and more data resides in the cloud. It's important to set up a plan for ongoing data classification, highlighting critical processes and roles. At one utility, the understanding of data classification is informing a robust data-loss-prevention (DLP) governance program and also a DLP tool to be used across the organization.

Utilities must, as a matter of urgency, know where they stand in terms of data classification. Many have successfully classified the data on their largest IT systems but not on others – sometimes hundreds of others – where real vulnerabilities may lie. Those who think they have adequately classified their data should look again – with an eye to an ever-changing future.

Web Isolation

This proven technique involves opening a Web browsing session or files in an isolated, typically containerized, environment. Then, even if the file or other input is malicious, it can be secured within that environment.[8] (The technique is also referred to as remote browser isolation.) A safe version of the e-mail can be streamed later to the end user's device.

In one case, the chief information security officer (CISO) of a leading U.S. energy transmission company wanted to further

protect the organization against malicious code or viruses found in suspicious emails and websites. The company brought in a third-party service provider to help with project management, delivery leadership, requirements gathering, vendor selection, design, testing, troubleshooting, and implementation of a software suite that would meet the CISO's needs. Because the software required an enterprise-wide roll-out to almost 7,000 end users, the service provider also helped create materials to educate those users, working closely with the energy company's own change management team to do so.

The energy company now has a full set of isolation policies that provide another layer of protection against suspicious sources or threats without impeding day-to-day operations.

As we noted in Part 1 of this mini-series focused on OT, the points made here are a reminder of what needs to happen now. But they are only just that: reminders. Today, the leadership teams at utilities must act promptly and forcefully to shore up the resilience and cybersecurity of their IT systems.

Crucially, though, this is not just a job for the IT teams. Cybersecurity is a pressing business issue that calls for collaborative, integrated approaches that span the entire organization and also its networks of vendors. The sooner that utilities' leadership teams break down the silos between IT and OT, the better they will be able to withstand the cyberattacks that are inevitably being planned somewhere today.

REFERENCES

1. https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html
2. https://www.power-technology.com/comment/cybersecurity-power-utilities-agenda-covid-19-globaldata/
3. https://www.securityweek.com/cyberattacks-against-energy-sector-are-higher-average-report
4. https://abnormalsecurity.com/blog/colonial-pipeline-attack-phishing-email-likely-the-culprit/
5. https://anlyz.co/blog/how-soar-cybersecurity-can-help-fight-phishing/
6. https://www.paloaltonetworks.com/cyberpedia/what-is-soar
7. https://resources.infosecinstitute.com/topic/end-user-chapter-6/
8. https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-browser-isolation.html

AUTHOR:

Robert Furr
Managing Principal
Robert.Furr@capco.com

CONTACT:

Robert Furr
Managing Principal
Robert.Furr@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO