America's energy infrastructure sector is increasingly vulnerable to cyberattacks that could take down electric power to millions of Americans, disrupt the U.S. economy, lead to death and illness, and leave behind billions of dollars in costs for energy companies. Meanwhile, documented cyber attacks on energy infrastructure in the U.S. and its allies and partners are on the rise, as the U.S.'s adversaries develop their offensive cyber capabilities, probe for weaknesses, and seek a strategic advantage.

Among the factors aggravating the threat are increasing automation in the power grid, distributed generation, the rise of electric vehicles, digitalization and interconnection in energy transmission and distribution, behind-the-meter energy storage, and other advances, all of which expand electricity systems' external attack surface and make them more vulnerable to intrusion and sabotage.[1]

Billions in Potential Losses

In addition to the deleterious effects on households and businesses, a cyberattack that causes power losses could result in billions of dollars in damages for electric utilities, including the cost of the investigation, containment and recovery, as well as disruption to its business, loss of information, and revenue loss. A major attack taking out power to tens of millions of Americans, insurance giant Lloyd's of London has warned, is "technologically possible."[2]

Since as far back as 2013, the U.S. government has warned of the threat of cyber attacks on energy systems, with the Obama administration naming energy systems "uniquely critical due to the enabling functions they provide across all critical infrastructure sectors."[3]

The first documented case of a cyber attack taking down an electricity network with sustained impact on customers came in December 2015, when Russian state hackers using the BlackEnergy malware toolkit caused a six-hour blackout for hundreds of thousands of customers in Ukraine's capital Kyiv. "The attack methodology, tactics, techniques and procedures that were successfully deployed in Ukraine could be deployed against infrastructure here and around the world," researchers have noted.[4]

Among subsequent incidents, in 2020 German officials discovered that Russian hackers had penetrated networks of power companies in Germany by compromising their supply chains. In 2022, cybersecurity officials thwarted an attack by Russian military intelligence on Ukrainian electrical substations. And in 2023, Russian hackers exploited a critical command injection flaw

[1] https://www.iea.org/reports/power-systems-in-transition/cyber-resilience

[2] https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf

[3] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[4] https://www.sciencedirect.com/science/article/abs/pii/S1040619017300507?via%3Dihub

to strike 22 Danish power companies, while Chinese hackers struck the national power grid of an unspecified Asian country by exploiting a corrupted Windows application.[5]

In the U.S., a 2021 ransomware attack on the Colonial gasoline and diesel pipeline led to a six-day shutdown and spurred a run on gasoline along parts of the East Coast. The episode only ended when the pipeline company paid a $4.4 million ransom.[6] Jen Easterly, director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), later called the incident "a watershed moment in the short but turbulent history of cybersecurity," and said, "this was the moment when the vulnerability of our highly connected society became a nationwide reality and a kitchen table issue."[7]

U.S. Under Threat

The U.S. has yet to suffer a major attack that caused a power outage, but numerous studies have indicated that the danger is growing fast. Across federal, state and local governments, officials warn that the U.S.'s electrical grid is extremely vulnerable to ransomware and other attacks, and urge local power authorities to take action to manage risks to their operations and assets.

In the Biden administration's National Cybersecurity Strategy, released last year, officials warned that ransomware attacks had disrupted critical services and businesses across the U.S. and the world, causing billions of U.S. dollars in total economic losses annually.[8]

A unit of Russian military intelligence, GRU Unit 29155, has conducted scanning and offensive operations against critical infrastructure components, including energy, in North America and NATO countries, according to a CISA report.[9]

In February, CISA, the National Security Agency and the Federal Bureau of Investigation warned that the People's Republic of China's state-sponsored Volt Typhoon hacking group "are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United

---

5 https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-08/240806_Significant_Cyber_Events.pdf?VersionId=K8TmKaKAnABvt0tYFNxofnqbL7Tq5wVB

6 https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

7 https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

8 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

9 https://www.cisa.gov/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.pdf

States."[10] In what's known as the Living Off the Land strategy, Volt Typhoon hackers penetrate a target network's external attack surface and wait inside, moving laterally through holes in the internal attack surface to gain access and cover their tracks, until receiving orders to strike, the federal officials warned.

Meanwhile, the number of virtual and physical weak spots in U.S. power grids that are vulnerable to cyber attack grew to 23,000 to 24,000 in 2023 from 21,000 to 22,000 the year before, according to a report from the North American Electric Reliability Corporation.[11] In 2023, the FBI's Internet Crime Complaint Center received 30 reports of energy sector companies being the victim of ransomware attacks, double the previous year.[12]

What Can Power Authorities Do?

R-MOR has provided its artificial-intelligence based cyber- and open-source intelligence security solutions to state, local and foreign government agencies, manufacturers, and utilities in the U.S. and across the world, and its executives and analysts have decades of experience in military and civilian cybersecurity and intelligence. Our team recommends that electrical systems:

1. Identify and assess cyber risks and continuously monitor and evaluate external, internal and human vulnerabilities
2. Implement a risk management strategy that will prioritize risks and remediation actions
3. Reduce the likelihood of an intrusion by mandating that all remote access to the organization's network and privileged or administrative access require multi-factor authentication; ensuring software is up to date; confirming all ports and protocols that are not essential for business purposes have been disabled
4. Continuously monitor the organization's external attack surface and the vulnerabilities in its third-party vendors' and service providers' networks
5. Secure the organization's internal attack surface by making sure systems are appropriately segmented to prevent hackers who have gain unauthorized access from moving laterally within the system
6. Instill a culture of cyber-awareness in your workforce, including providing anti-phishing training with simulations
7. Install robust anti-phishing protections
8. Mandate use of secure passwords, urge employees and contractors to use password managers

[10] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[11] https://reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04

[12] https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

How Can We Help?

R-MOR's agentless External Attack Surface Management platform, RECONIZER™, scans an organization's cyber perimeter, simulating complex attack scenarios and probing for vulnerabilities. Using predictive analytics, RECONIZER™'s AI algorithm tracks and gathers data on potential attackers across the digital landscape, including hacker forums, social media and all layers of the web. It uncovers hidden attack vectors such as leaked data and stolen passwords and Personally Identifiable Information while reducing false positives to less than 5%.

In addition, RECONIZER™'s AI-driven Insight module navigates your network's topography and organizational policies to identify, monitor and patch potential vulnerabilities in the internal attack surface before they are exploited. It offers visibility and monitoring of a company's shared files and folders to uncover and eliminate malicious content, and maintains vigilance over role and permission configurations to prevent unauthorized access.

Armed with those insights, RECONIZER™'s AI algorithm predicts and detects cyber vulnerabilities and prioritizes them by criticality and severity, then offers strategies and recommendations to remediate them.

The AI algorithm prioritizes uncovered vulnerabilities by criticality and severity, and offers strategies and recommendations to remediate them.

Get in Touch

Contact us for more information at info@r-mor.com

September 2024