CAPCO

SECURING ENERGY'S INFRASTRUCTURE:

THE GROWING PROLIFERATION OF CYBERSECURITY THREATS IN A SMART GRID ENVIRONMENT

a **wipro** company

Never has the danger of a changing climate been as pressing as it is today. The United Nations declared in their 2021 climate report that all countries must be net zero emissions by 2050 or "limiting warming to 1.5°C will be impossible, with catastrophic consequences for people and the planet on which we depend."[1] Alongside the expansion in global energy demand, a drive toward renewable and clean energies is gaining momentum. These advanced generation sources are affecting a traditional grid system that has insufficient capability of handling these new technologies and is replacing it with a smarter grid. The shift away from a legacy grid comes with both widespread adoption of new devices and incorporation of variable, bi-directional power flow. All this restructuring of the energy landscape offers an interconnected network of communication that not only opens new ways of operating, but also introduces new avenues for cyber threats.

TECHNOLOGIES, DEVICES, AND LANDSCAPE

Each new device entering the electrical grid is a potential access point for bad actors. In comparison to a consistent way of managing the grid in the past, the rapid expansion in the operations of our modern utilities requires steadfast diligence regarding security. It remains imperative that a highly critical piece of infrastructure, such as the electrical grid, stays available, maintains the integrity of its communications, and safeguards the confidentiality of the user's data. However, when legacy power generators that have been regulated for decades are being complemented with widespread inclusion of renewable energies, such as wind and solar, there are many issues to consider.

One of the key additions to energy consumption in the 21st century is the introduction of distributed energy resources (DERs). DERs are small, modular, energy generation and storage technologies that can be installed near the consumer and includes wind turbines, rooftop solar photovoltaics (PV), fuel cells, microturbines, cogeneration, and battery storage systems . According to the WoodMac Q2 2021 US energy storage report, annual energy expense is expected to grow from under $2 billion in 2020 to nearly $8 billion by 2025.[2]

Previously, physical meters were read manually until power companies had a communication line of information flowing back to them. Smart meters, which are electronic devices that record energy consumption, have been introduced and relay information back to utilities for monitoring and billing. Now that bi-directional power and data flow exist on the grid, the industry need be cognizant of how these communications can affect their cybersecurity posture.

The U.S. National Institute of Standards and Technology (NIST) offers an evolving framework for the smart grid architecture. Their conceptual model "supports a collective understanding of the actors, roles, and responsibilities needed to ensure effective day-to-day grid operations and control."[3] Further, the expansion of distributed energy resources complicates the exchange of information and creates new challenges for the industry. "To realize the benefits of an interoperable smart grid, security practices will have to evolve beyond strategies of physical isolation or other overly restrictive access regimes," claims NIST.

As an example of a vulnerable device, during the 2014 Black Hat USA conference, a team of white hat hackers were able to hack into a Google Nest within 15 seconds and have it display the message "I know that you and Frank were planning to disconnect me, and I am afraid that is something I cannot allow to happen."

Although Google has since fixed this vulnerability, and the attack was harmless, a Nest device is able to read usage patterns, communication with the electrical grid, and has a direct line of communication with the energy supplier. There's no saying what the damage could be from more serious hackers.

SECURITY AND THREATS

It may seem that security over the grid can no longer be maintained by a single organization now that an increasing number of devices are connected and can be owned by non-utility stakeholders. However, organizations can mitigate this risk with structured system security; minimizing exposure to threats and prioritizing actions that provide the strongest defence against risks.

The North American Electric Reliability Corporation (NERC) identifies the following top tactics confronting utilities:[4]

- **Cyber Hygiene** – Known and unremedied vulnerabilities in popular software, inappropriate device configurations, and reusing exposed credentials are easy targets for attackers.
- **Social Engineering** – Phishing and other forms of targeted exploiting of human trust is widely used to get a foothold in targeted systems.
- **Insider Threat** – Existing access and knowledge from employees, subcontractors, and other affiliates can be coerced or recruited to get into sensitive areas.
- **Supply Chain Compromise** – One of the most relevant topics to the growth of the smart grid. An adversary abuses an organization using equipment with unknown exploitable features.

Additional threats to the smart grid include:

- **Denial of Service (DoS**) – An attack against the availability of the network. If this were to happen to our smart grid, we would lose the connection to countless devices disrupting services on a large scale. Prolonged loss of control can lead to a halt in operations and massive damage to the reliability of the grid.
- **Malware Propagation** – Attackers develop and inject malware to manipulate functionality of the system, thereby providing access to sensitive information.
- **Eavesdropping and Traffic analysis** – An attacker can gain access to sensitive information by monitoring network traffic. The expanding smart grid creates a larger attack surface where data could be stolen from network nodes.
- **Ransomware** – The notorious hack that shut down Colonial, the largest pipeline in the U.S. in April 2021, is increasingly common.[5] Attackers abused a VPN account that lacked multifactor authentication (MFA) to take down the Colonial networks, then demanded payment in cryptocurrencies to restore functionality in the costliest attack to date. According to Cybersecurity ventures, global ransomware damage costs are predicted to reach $10 billion by 2027 from just $325 million in 2015.[6]

Deciding the best response when facing uncertainties can be daunting. Questions can include tracking where and how devices are sourced, who will enforce new security processes and to what degree, or ultimately who should be liable and in charge of remediating incidents of these new devices. As the standards and regulations of this growing industry mature, we recommend checking out Real-Responses-To-Repel-Cyberattacks-On-Utilities for the three best-practice initiatives to mitigate risks of cyberattacks in operational technology (OT) infrastructure.

CONCLUSION

Many current cyber practices can be applied to the challenges of a smart grid when having various devices connected over vast geographical networks, including threat / risk assessments, control implementation, vulnerability assessments, and testing. However, even with an agnostic approach of addressing these problems, the landscape is evolving rapidly, and we can no longer rely on the maturity of an "industry standard." To leverage the benefits of interconnected resources, companies must invest in their cybersecurity program to protect from vulnerabilities of the smart grid. Ensuring security is a critical step in our fight against climate change.

REFERENCES

1. https://public.wmo.int/en/resources/united_in_science
2. https://www.woodmac.com/research/products/power-and-renewables/us-energy-storage-monitor/
3. https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-40
4. https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2020.pdf
5. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
6. https://cybersecurityventures.com/cybersecurity-market-report/

AUTHOR

Grant Auerbach, Senior Consultant, Grant.Auerbach@capco.com

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

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
a wipro company

JN_4236