Case Study with Supporting Media and Simulation Exercise

Title: Assessing Vulnerabilities in Wind Energy and Future Policy Through a 2022 German Cyberattack.

Real World Inspiration

The world of power generation is ever-changing. While the idea of harnessing wind to power machinery had been around since antiquity, and the first wind turbine to be connected to the power grid was brought online in the early 1950s, the prominence of fossil fuels as an electric power source was so strong that wind turbines were considered more supplementary rather than critical to the operation of the power grid, as seen in Figure 1. Given the shift towards renewable energy has only materialized in the last 40 years or so, there are relatively few large-scale real-world attacks upon which inspiration can be drawn. It is apparent that in the future wind energy will play a crucial role in satisfying the needs of a green power grid. This outlook means that now is the critical time to research and mitigate potential vulnerabilities before wind turbines become integral to our power grid [1]. Another reason that wind turbines represent a major attack target is inherent in their nature; Since they need plenty of wind to operate, a typical installation is in a remote area. Because of this, even if an intrusion is detected, which is itself a major challenge, the response time of security personnel will be much lower than that of many other critical infrastructure installations, therefore the need to design secure system architectures informed by CIE principles is crucial [2].

On February 24, 2022, a Russian hacker group attacked a German company named ‘ENERCON’. These attackers were specifically targeting Ukrainian military communications but affected the wind farms owned by ENERCON as a byproduct of their attack [3]. Around 5800 wind turbines were affected on 1217 wind farms. These turbines were compromised due to their SATCOM architecture. Malware called ‘Acid Rain’ was able to enter the network through the SATCOM modems located inside the wind turbines and disrupted the communication between those modems and the servers. About 30,000 SATCOM terminals were affected by this malware. It infected these modems due to misconfigured VPN connections and gaining trust from within their network [4]. Then, it was able to overwrite key data in the flash memory of the modems and disconnect the turbines from the main network. Service centers and customer operation centers were unable to communicate with the wind turbines for important information. Some technicians were able to get some of the turbines’ communication systems back by using cellular LTE networks. It took around 2 months for the technicians to repair and replace the affected modems in their wind farms [5].

Figure 1: Example Wind Turbines in Southern California 2016

Media Feature for the General Audience

For a custom media clip designed by faculty and students of the University of Pittsburgh, please click on the video file found here: https://youtu.be/vSQh6bQYca0

This video adopts a narrative structure while remaining educational. It opens with a real-world scenario that illustrates the effectiveness of this use case. We focus on wind turbines and their impact on communities, using a compelling example to bring the real-world relevance of this case.

Next, we feature an interview with our group (students working on this use case), discussing the CIE principles relevant to our case. We start with Engineered Controls and Active Defense. To make this engaging, we incorporate a "man on the street" style segment. We interviewed a diverse range of people, including a professor, a student, a university store employee, and a registered nurse, to highlight the seriousness of the issue and capture different perspectives.

The video concludes with a team interview section where the students respond to questions created by the media representative of the group. We discuss our case in more detail, how we plan to use CIE principles in our case and discuss the effects of placing wind turbines in communities. This interactive segment serves as an effective learning tool and a recap of the video's keys points.

Future Policy Implications

Over the past few decades, the United States (U.S.) has made a noticeable shift towards using renewable energy. The Energy Policy Act of 1992 created the renewable electricity production tax credit (PTC), which has been renewable many times since. Most recently, the tax credit provides up to 2.75 cents/kWh for electricity generated from wind, and the credit is good for 10 years after the equipment is placed [6]. The Energy Policy Act of 2005 also established that double credit must be given if renewable energy is produced at a Federal facility, on Federal lands, or Native American Lands [7]. In 2023, the U.S. produced 425.2 terawatt-hours of energy from wind power, which was ruffly 10.18% of the electricity that year [8]. In 2019, wind power became the largest form of renewable energy. As use of wind power increases, so does the threat of cyber-attacks on wind farms, which is heightened due to their physical vulnerabilities. National and corporate policies must be developed, implemented, and enforced to protect the nation's wind power. Use of wind power has decreased in use over the past few years compared to other renewable energies, as seen in Figure 2.

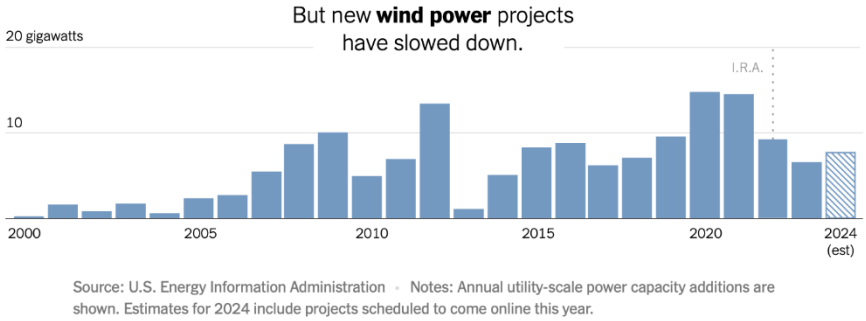

Figure 2: Use of Wind Energy Over 20 Years [9]

Across the U.S., policy is created on both the federal and state level. Tax incentives exist across both levels, with state incentives varying significantly. There are also varying ordinances and permits across the 50 states. Federally, recent policies have surrounded offshore wind energy projects. In 2023, the Biden-Harris administration began expansions on wind energy, including in deep water and setting a goal of 30 gigawatts of offshore wind by 2030. It is necessary for state

and federal entities to continue investment in both tax credits and building infrastructure for wind turbines [10]. This investment, though, should include investing in cyber security for the wind farms and wind turbines. Government entities should deploy better standards and practices for companies to follow. Additional support, like those seen for other critical infrastructures, which helps to provide assessments and incident coordination during cyber threats is needed, especially as renewable energy rapidly expands [2]. Recent recommendations for national and corporate policies were released by the INL but are not currently mandated.

On the corporate side, adopting the INL recommendations as soon as possible is necessary to protect the induvial wind farms. Managing inventory, access to networks, analysis of software on the network, and device security are all needed steps by each corporation to help strengthen their cyber security.

Part 1: Expand Your Understanding with the Following Exercise

(a) Consider the hypothetical scenario: A wind turbine farm was attacked due to physical access to their systems. The farm, known as Whispering Pines Energy, was attacked by an outsider threat who gained access to one of the turbines. The attacker was able to infect one of the turbines and plant a worm, a type of malware, through the use of a personal laptop which was connected directly to the fiber optic cable network inside the turbine. The worm virus subsequently spread throughout their network, impacting most of the other turbines in the SCADA architecture of the wind farm. The worm spread from one turbine to the others through the internal network and spread into the server which spread the worm packets to other devices. The devices on the network, called fiber to ethernet converts, whose purpose is to convert the fiber optic signals to ethernet ones were vulnerable as they featured outdated hardware. The effect of this attack was disabling the communications between the turbines and the servers. This meant that operators couldn't see or communicate with the turbines to ensure proper function.

1) Based on the reading, what are some CIE Principles that can be applied here to help prevent and reinforce the overall setup of the scenario?
2) Are there any ways that this attack can be mitigated physically? For example, locks on doors or other physical methods that don't involve software.
3) Are there any software mitigations that this scenario could use to prevent an attack like this from happening again?

Further Reading and Useful Public Video Links

For further reading, the following references would be suitable to explore at your convenience.

[1] Protecting wind energy systems from cyberattacks | Department of Energy, https://www.energy.gov/eere/wind/articles/protecting-wind-energy-systems-cyberattacks.
[2] "Roadmap for Wind Cybersecurity ," Department of Energy, https://www.energy.gov/eere/wind/articles/roadmap-wind-cybersecurity.
[3] M. Egan, "A Retrospective on 2022 Cyber Incidents in the Wind Energy Sector and Building Future Cyber Resilience," ScholarWorks, https://scholarworks.boisestate.edu/cgi/viewcontent.cgi?article=1002&context=cyber_gradproj.

[4] “Attack Surface of Wind Energy Technologies in the United States,” Idaho National Laboratory, https://inl.gov/content/uploads/2024/02/INL-Wind-Threat-Assessment-v5.0.pdf.
[5] J. Staggs, “Wind farm security: Attack surface, targets, scenarios and mitigation,” Research Gate2, https://www.researchgate.net/publication/315590797_Wind_farm_security_Attack_surface_targets_scenarios_and_mitigation.
[6] “Renewable Electricity Production Tax Credit Information,” EPA, https://www.epa.gov/lmop/renewable-electricity-production-tax-credit-information#:~:text=For%20facilities%20placed%20in%20service,kWh%20for%20electricity%20generated%20from.
[7] “H.R.6 - 109th Congress (2005-2006): Energy policy act of 2005 ,” Library of Congress, https://www.congress.gov/bill/109th-congress/house-bill/6.
[8] “Electric Power Monthly,” U.S. Energy Information Administration (EIA), https://www.eia.gov/electricity/monthly/.
[9] B. Plumer and N. Popovich, “As solar power surges, U.S. wind is in trouble,” The New York Times, https://www.nytimes.com/interactive/2024/06/04/climate/us-wind-energy-solar-power.html.
[10] “Fact sheet: Biden-Harris Administration announces new actions to expand U.S. Offshore Wind Energy,” The White House, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/15/fact-sheet-biden-harris-administration-announces-new-actions-to-expand-u-s-offshore-wind-energy/.

Authors

Ethan Crosby is a rising junior majoring in Computer Science. His background also includes work in electrical engineering.

Michael Estocin is majoring in Film and Communications with a certificate in Television and broadcast arts.

Katie Fitzpatrick is a rising senior pursuing a degree in Political Science and Psychology. She has a background in human interaction and behavior in the political landscape and application to policy.

Aidan Gresko is a rising senior majoring in computer engineering pursuing a Bachelor's degree. He thrives on gaining knowledge about technology and has a background in coding, circuits, and digital design work.