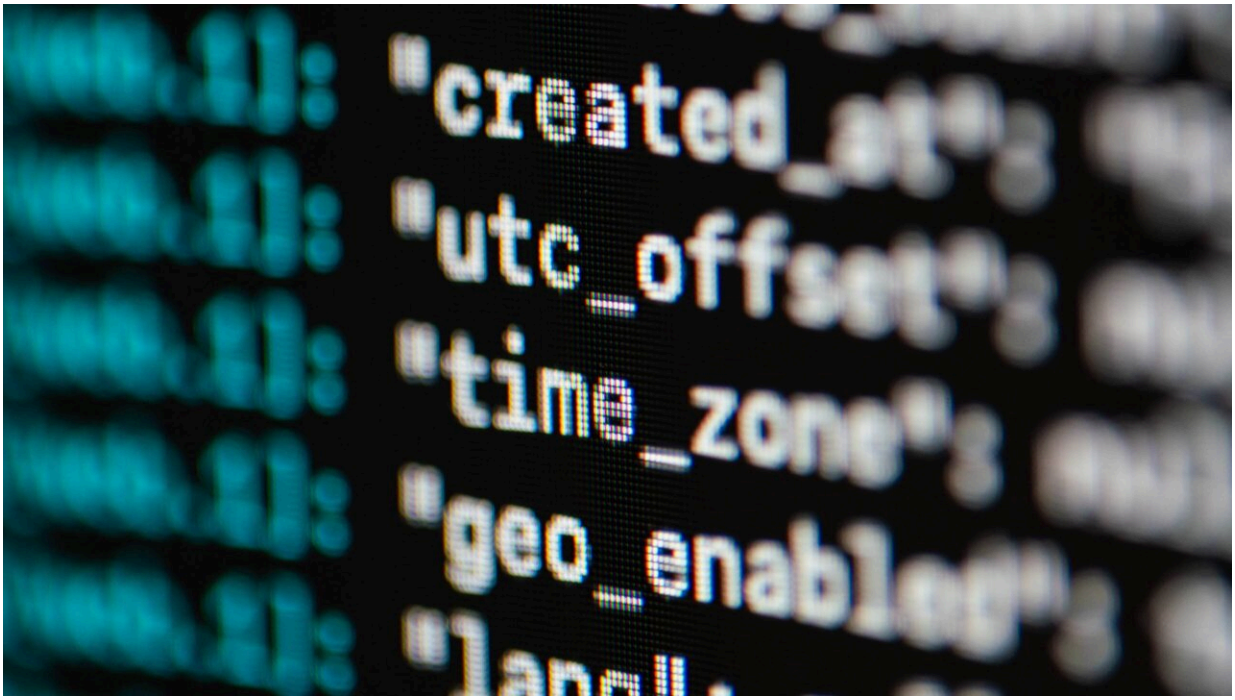
Shielding the grid to foster renewables: The cybersecurity challenge

July 18 2022, by Diego Giuliani



Fostering the energy transition requires advanced and sophisticated technology. However, such interconnected solutions are exposed to a wide range of cyber-attacks. A European project aims to tackle these growing threats by improving the security of power grids.

In the mid-1990s, when he was 9 to 12 years old, Tommy DeVoss broke

into the computer systems of global fast-food and pharmaceutical companies. He also hacked into organizations such as the U.S. government, the U.S. military, and NASA. After a few jail terms, he now works as a security engineer for a big New York-based company.

"I did it for fun," he recalls. "I enjoyed the fact that I was exposing their weaknesses. I was targeting giants who were all supposed to have the best security in the world. I was told that some of them were so secure that they couldn't be hacked. It was a further challenge for me, so I said: "OK, let's see if it's accurate. And it never was."

Almost 30 years later, in March, U.S. President Joe Biden said that "this is a critical moment to accelerate our work to improve cybersecurity" and acknowledged that "the US Federal Government can't defend against this threat alone." Furthermore, with the war raging at the doors of Europe, the United States and their allied cybersecurity authorities warned of the increased threat of "Russian cyber groups targeting critical infrastructure that could impact organizations both within and beyond the Ukraine region." "Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks, to exfiltrate sensitive data and to disrupt critical industrial control systems by deploying destructive malware," says their joint advisory, issued on 20 April.

According to Tommy DeVoss, cyber-defenders are almost always at least one step behind attackers. "Not only do the hackers have significantly more time to spend looking for new methods," he says. "The problem is also that the defensive cyber security is reactive instead of being proactive."

Anastasis Tzoumpas has been working to reverse this approach. As head of the electrical and power systems at Ubitech Energy, he leads the implementation of a "cybersecurity framework" for Tigon: a 48-month

EU-funded project, running until August 2024 and aimed at fostering the energy transition through the optimization of power grids. "While most renewable sources like photovoltaic are DC-based, the electricity grids commonly used in our cities are not," he explains. "To feed renewables into these grids, we therefore have to use transformers. The problem is that the common ones are not 100% efficient and some of the energy gets lost."

Such optimization is made possible by new and more technologically advanced transformers, which are nevertheless highly interconnected and therefore more exposed to a wide range of attacks. "The objective of our cyber-security framework is to assess the system and to provide the security information which is needed to set up the possible responses to such cyber-attacks," says Mr. Tzoumpas. "We first target the main threat models and then we try to frame the most adapted defense mechanisms."

The final step of this phase is the implementation of a cyber-security resilience plan, which is now about to be completed at two selected demonstration sites in France and in Spain. The viability of the solutions developed will then be replicated in real-life scenarios in Finland and Bulgaria. "Improvement of renewables production management and power storage systems will be tested in the Finnish residential district of Naantali. And increasing the stability and resilience of the power grid will be the objective of the replication case involving the underground network of the Bulgarian capital, Sophia."

As all other public services depend upon them, power grids are considered among the most critical infrastructure. Moreover, experts at ENISA, the European Agency for Cybersecurity, say that "the uptake of new technologies in the energy sector means there is a larger attack surface for cyber attackers. In the past, you needed physical access to a grid substation to disrupt the energy flow. Today an equivalent amount of damage can be achieved by a fingertip on a keyboard. And this

exercise can be performed from any place in the world."

As also confirmed by a study by the Institute of Electrical and Electronic Engineers, the vulnerability of critical infrastructure to cyber-attacks is today considered "a major threat to the stability and safety of our society." A clear example was the 2017 ransomware campaign "Wannacry," targeting a vulnerability in the Windows operating system. "Due to its massive distribution, it caused widespread chaos," recall ENISA's cybersecurity experts. "It infected over 230,000 systems and hit more than 150 countries. Surgery and X-rays were delayed in the hospitals, the rail sector was affected in Germany as well as the telecommunications in Spain."

Ransomware involves malicious attacks mainly encrypting an organization's data and demanding payment to restore access. In addition, a ransom is demanded for not disclosing the stolen information. ENISA warns that we're now in the "golden era" of ransomware and, in its annual report on the state of the cybersecurity landscapes, ranks it as a "prime threat" for 2021. "The number of publicly reported cases of ransomware jumped from an average of around 15 for the first few months of 2020 to around 35 for the period up to July 2021. Moreover, the average cost of such incidents more than tripled, compared to 2020."

A Europe-wide survey conducted by Ubitech, reveals that the big organizations' readiness level to tackle such threats grew recently to 3-3.5 on a scale from 0 to 5. "This outcome is encouraging," says Mr. Tzoumpas. "It means that cybersecurity is now taken more and more seriously." But a lot has still to be done and most experts agree that no defense strategy will ever be effective, as long as there is not a real and widespread awareness of cyber-threats. Chris Dickens is Solutions engineer at HackerOne, a US company with a wide portfolio of "ethical hackers" who find and fix vulnerabilities for global brands and government organizations. "Getting oversight of these vulnerabilities is

the first step to mitigating the risk," he says. "A study that we did recently has shown that one third of organizations monitor less than 75% of their total attack surface. Almost 20% also believe that over half of their attack surface is either unknown or not observable."

In such a context, says Mr. Tzoumpas, "our first step will consist in sharing the recommendations issued by our tests with the power operators. Then, depending on their policies, on their cybersecurity plans, and on the level of interconnection of their grids, we will also provide specific solutions aimed at detecting and countering such threats."

But the very challenge, warns DeVoss, will be to keep up with the cyber-criminals: "Computers and security evolve constantly," he says. "There are always new attack types and always new ways to evade whatever defenses we put in place."

More information: HackerOne report: www.hackerone.com/resources/re … ck-resistance-report

Provided by iCube Programme

Citation: Shielding the grid to foster renewables: The cybersecurity challenge (2022, July 18) retrieved 3 May 2024 from https://techxplore.com/news/2022-07-shielding-grid-foster-renewables-cybersecurity.html