Wind farms next target group for cyber-attacks

21 December 2022, 10:55

Tatiana Galibus
Pieter Jan Jordaens

The continuous growth of wind energy is highly dependent on energy infrastructure becoming more digitally connected. Yet the more connected energy infrastructure becomes, the more vulnerable. This is what cyber criminals are anticipating on when they strike, too often successfully. High time to turn the tables.

According to a recent article on Offshore WIND, in 2022 (at the time of writing), there were three high-profile cyber-attacks on wind farms across Europe, with OT (the computer systems that manage, monitor, automate, and control industrial systems) at risk of being exploited and compromised.

According to the article, one of the most urgent tasks companies in the energy sector are facing, is to identify where their projects and operations are exposed to threats before cyber criminals can find them. Companies need a clear, complete and up-to-date overview of their information and control systems – including the connected supplier and third-party systems. It is not enough for companies to sporadically go through the process of discovering where they are vulnerable. It has to be done on a regular basis, to ensure that they are resilient to new attack vectors.

From breaking in to hacking

There are, at least, three different methods of attack (vectors) when it comes to wind farms:

- physically breaking into the turbine and connecting to the internal cabinet, due to lax on-site security
- compromising and remote controlling an engineering mobile or laptop to access and take advantage of a missing endpoint connection or through a VPN
- hacking into internet facing endpoints such as CCTV located at the substation.

Ultimately, all vectors allow access to the supervisory control and data acquisition (SCADA) industrial control system architecture. Once in there, cyber-criminals can take control of the entire windfarm.

Tested and found wanting

Researchers from the University of Tulsa (Oklahoma, US) demonstrated how easily a wind farm can be hacked, going from lock-picking an unsupervised turbine door in less than one minute to gaining direct access to the unsecured server behind it. More elaborate criminals could create grid instability by altering the power and frequency regulation towards the grid transmission. The worst-case scenario is loss of life, e.g., when a hacker increases the voltage within the turbine while an engineer is working on the structure or the turbine catching fire as a result of such an increase in voltage.

Staying ahead of cyber-crime

The cyber-security landscape is changing every day. Wind operators are facing potentially huge losses as a result of cyber-attacks. Still, it is not yet too late for operators to act. What to do? Be prepared. Be ahead of hackers. Keeping your finger on the pulse is essential: with attacks getting more and more organized, security should be more collaborative and agile, which means ensuring the security of the whole supply chain.

In the next months, Sirris will organise two trajectories (masterclasses), dedicated to cybersecurity for digital services as well as manufacturing. Both trajectories are designed as learning journeys, with in-depth theory modules and tailor-made practice sessions. We work with other cyber-security partners to deliver the best lessons learnt and give you networking experience. On top you will get several micro-coaching sessions for your specific concerns.

Check out our collective and individual offerings here!

Further reading: OffshoreWIND

Authors

Tatiana Galibus

Pieter Jan Jordaens