Toni Sulankivi

Head of Cyber Security **at tiko Energy Solutions AG**

31.03.2020

Energy sector cyber attacks are on the rise

In 2019, the energy sector was the most targeted industry for cyber-attacks worldwide. There were more attacks against the energy sector, than against financial-, software-, automotive- or logistics -industry. When new business models in the energy sector are being developed and adopted, those will inevitably become a tempting target for advanced, skilled, and well-funded attackers.

New business models attract new attacks

One of the new business models, a Virtual Power Plant (VPP), is built on top of the Distributed Energy Resources (DER) to create a functionality similar to a bigger conventional power plant. The benefit of the VPP is not only that it can produce energy by combining several smaller assets. It can also quickly react to any changes in the grid frequency and act as a sink for excess energy, when the energy supply exceeds the demand in the grid. This provides much more opportunities and use cases compared to conventional power plant and enables more efficient use and adoption of green and sustainable energy sources.

When VPPs in the future will eventually have capacities comparable to the conventional power plants, they will also attract the same highly skilled adversaries as the conventional power plants and should be also considered a critical infrastructure in society. These attackers include, for example, nation-state actors, terrorists, and well-funded and motivated criminal actors. That is why it is important to start the discussion already now on how these business models should be protected against various digital threats and attackers in the future.

Manufacturer aggregations pose new risks for grid stability

There is already some interesting research regarding aggregated high energy capacity and “high wattage” devices creating an IoT (Internet of Things) Botnet that would have the ability to disrupt the electrical grid - If controlled by a malevolent actor. From one perspective, these aggregations are already creating capabilities similar to the VPP, with the exception that they could be used to destabilize the electrical grid by creating synchronized power spikes, instead of serving to stabilize the grid and act as an energy source, what VPPs are aiming to do.

These manufacturer aggregations (OEM) that are already taking place around the world (e.g. large aggregated pools of EV-chargers, home batteries and solar panels) should quickly be addressed in terms of the risks they pose to the grid stability. Nevertheless, these can also provide us valuable insight on the risks that we need to mitigate also with the VPPs in the future. Capacities behind a single aggregation for some manufacturers are already in the range of hundreds of Megawatts and will reach the scale of Gigawatts in the very near future.

The most notable manufacturer aggregation currently taking place is the connection of the electric vehicles to the grid and the EV-chargers charging them. In Europe alone, the number of registered all-electric passenger cars will most likely exceed 3 million this year, and that number does not even include hybrid plug-in vehicles.

The growth rate of EV's is currently exponential, and the combined charging power of a single manufacturer vehicles simultaneously connected to the grid via EV-charging stations (home or high-power chargers) is most likely well over a Gigawatt limit already. What would happen if this aggregated pool would start synchronously switching on or off, in the hands of the attacker, or just due to a software bug or human error?

Working towards a regulation

Currently, there is no regulation enforced for these aggregations on a European Union level, but the discussions and work has been started to address the issues presented above. Tiko has been actively participating in these discussions and the regulatory work in a consultative role and will continue to do so.

Watch the latest Interconnect webinar:

"New business models with household assets - Impact on Cybersecurity and data ownership" where Remi Roché and Toni Sulankivi discuss more about this topic. **https://youtu.be/AQO9qm7s9GQ**