Secure electric networks without interruptions
Alperia has adopted Kaspersky's KICS for Nodes solution to protect the remote-control systems dedicated to power stations and the distribution network responsible for supplying electricity to 280,000 customers in South Tyrol. The choice was motivated by the need to have a dedicated solution for the OT environment offering maximum protection without the risk of disrupting machinery operations that are essential for the supply of services.

"The idea of having a task force with the Kaspersky engineers available in the company allowed us to customize the product by tailoring it to our situation,“

Sandro Moretti
Division Manager Teleconduction & Telecommunication

The increase in connected devices and the growing digitalization of infrastructures for public utilities networks bring with it many opportunities, but also an exponential increase in the risks.

According to the Global Risks Report 2020, produced by the World Economic Forum, the combination of large-scale cyberattacks and the possible interruption of critical infrastructures and information networks ranks second among the most feared risks.

This is also an issue highlighted by the Allianz Risk Barometer 2020, according to which computer incidents are the number one perceived corporate risk at a global level; while business interruptions are in second place.

It is therefore no surprise that the companies that provide essential services (from water to energy, from transport to telecommunications) are paying increasing attention to the protection of the infrastructure they are called upon to manage. This is also the case for companies operating in the generation and distribution sectors of the electrical power industry.

Energy and gas for 280,000 South Tyrolean

Alperia is the south Tyrolean company that provides electrical energy and gas to 280,000 users, by running 34 hydroelectric power stations, six district heating plants, over 8,600 kilometers of electrical grid and 700 electric charging points.

The company was founded in 2016 from the merger between the two most important local energy companies: AEW, which has roots dating back to the end of the 19th century, when its predecessor Etschwerke built the first power stations to harness water power in order to provide the area with electricity; and SEL – South Tyrol’s energy company, which in the last decade has taken over the management of the large hydroelectric power plants and the grid.

Head of the Telecommunications and Teleconduction function of Alperia Group is the engineer Sandro Moretti, an expert reporting directly to the general manager of the group. He is in charge of a team of 13 people tasked with managing the systems production data transmission and telecommunications. The team is responsible for remote terminal units (RTUs), the data centers, control room operations and the connection network towards the two realities of the group that deal with production (Alperia Greenpower) and distribution (Edyna) of electricity.

The specifics of the OT world

Moretti is convinced that securing industrial systems using conventional solutions would be a mistake. In the IT context, the basic principles of cybersecurity define data as being safe when confidentiality, integrity and availability – in that order – are respected. In the operational technology (OT) environment, however, the order of these three is reversed. This paradigm is particularly valid in the case of critical infrastructures, where systems must always be active (and that is why all systems are managed by redundant machinery).

A logical consequence of these principles is that in the industrial context, the solutions used are explicitly designed for this environment: the ports, protocols and rules are very different and typical of the devices connected to the plant’s network and control and remote control systems. In addition, machines are often equipped with operating systems that, in order to always be available, are not always updated in real time with the latest security patches.
“From the very beginning, management realized that the same paradigms that work in the IT world could not be used in the OT world,” Moretti explains. “That’s why Alperia separated the perimeter of the OT network from that of the IT network, and set diversified management strategies.”

The team headed by Moretti then started to look for a solution that would allow for the insertion – within the perimeter managed by the remote control systems – of a security system that is more advanced than the standard endpoints used in the IT department and, above all, dedicated to the OT area.

After a careful analysis of the (few) solutions available on the market specifically dedicated to industrial environments, Moretti decided to focus on KICS – Kaspersky Industrial CyberSecurity.

However, installing a security solution on systems that must be active all the time is not that simple. Alperia and Kaspersky therefore decided to create a joint working group, in order to create the best setup possible for the solution.

Collaboration has proven to be the right path to follow, not least because a test environment was unavailable at Alperia, and it was necessary to work directly on functioning machines.

Custom implementation

We started at the end of 2018 with a proof of concept: the KICS for Nodes solution was put into operation on certain machines for several weeks.

“It was essential for us to refine the solution in the field, check the effects on the machines’ operability, which exclusions to set up and which optimizations to make,” says Moretti.

“In Alperia all the systems are redundant. We therefore installed the solution on just one of the two redundant machines – the main one – to be able to have a solid backup in case of problems, and to avoid the risk of impacting on production. We were thus able to carry out various stress tests that were all passed successfully.”

Initially, KICS was configured in monitoring mode. “We wanted to check whether the new system would detect any false positives and interactions which could slow down running applications, with the risk of blocking specific fundamental services. Once we were sure the system was perfectly in place, we went ahead with full operability, allowing KICS to automatically block any suspicious services,” explains Moretti.

“During this phase, our engineers enabled a further in-depth logging of the agent, in order to understand its behavior and the interactions it had with the SCADA system.
After careful analysis of the logs, we offered additional information to Alperia for the configuration,” explains Diego Magni, Pre-Sales Manager at Kaspersky.

After the first experiment, the task force gradually extended the coverage of the system to other machines and environments (physical and virtual). “Today we have about 40 servers that are protected by the Kaspersky solution,” says Moretti. “In less than six months we were working at full speed, and we did so gradually and in complete safety.”

**Beyond the customer-supplier relationship**

Moretti is visibly satisfied with the results achieved and the support received. “I am convinced that in cases like this we need to go beyond the traditional customer-supplier relationship and aim for a broader partnership. This is why we are taking into consideration the idea of a service agreement with Kaspersky that goes beyond product assistance and extends to the provision of consultancy on the whole network perimeter,” Moretti concludes.