IT SECURITY ACT 2.0

Legally prescribed intrusion detection in substations

Cyber attacks are on the rise, and their methods are becoming more deceptive. Defending critical infrastructures is a high priority, as the damage caused by an attack could be devastating. Such an attack took place in Ukraine in 2015 that left nearly a million people without power. Germany is responding to this threat and leading the way. The recently passed 'IT Security Act 2.0' defines a legal framework intended to minimize such risks. What exactly does this mean for power supply companies? Thomas Friedl, Cybersecurity Sales Manager at OMICRON, gives us the answers.

Thomas, what exactly was introduced in Germany with the IT Security Act 2.0? Who does it affect?

Thomas: Critical infrastructure operators need to provide state-of-the-art protection for their IT systems with appropriate organizational and technical precautions. A major disruption must be reported to the Federal Office for Information Security. This enables the government to respond to the increased risk of cyber attacks on the state, economy, and society at large.

In order to reliably detect such threats, a binding standard for the use of intrusion detection systems (IDS) in critical infrastructures has been adopted in Germany for the first time, which also applies to electrical energy supply equipment. This is extremely important, as hackers can still gain access to a substation through remote maintenance channels even if a firewall is in place. They may even compromise engineering PCs from external maintenance companies and use them to carry out attacks.

A breach of this law results in heavy fines. With the Regulation on the Determination of Critical Infrastructures ('KritisV'), the Department of the Interior also plans to lower the power threshold that classifies power generators as critical infrastructures. This would mean that the IT Security Act would also apply to smaller operators with maximum capacities above 36 MW in the future.

What exactly does this mean for energy suppliers?

Operators often work with an Information Security Management System (ISMS). As such, they may already fulfill some of the specifications from the IT Security Act 2.0. They may, for example, document their network or store data securely.

But they often ask themselves what else they can do, how these things can be integrated into their infrastructure, who needs to be involved, and how to deal with alarms. They may even ask whether they need to appoint their security specialists for Operational Technology (OT).

We offer workshops that clarify these and other uncertainties. In these workshops, we help operators decide on the best way to implement systems and processes. The law stipulates that affected companies have two years to implement appropriate solutions.

The installation contains an IDS in the critical area. Doesn't this also pose operational risks? What do I need to prioritize as an operator?

In a substation, the system must not interfere with any time-critical processes. A circuit breaker, for example, must open immediately in a critical situation. The signal must not be analyzed first and then forwarded to the circuit breaker following a delay.

*«**StationGuard doesn't require a long learning phase** compared with many other solutions and it protects the installation immediately.»*

Thomas Friedel, Sales Manager Cybersecurity, OMICRON

We've designed our StationGuard IDS solution for use in substations from the ground up. It monitors the network traffic from the switchgear passively and non-reactively and notifies the operator automatically in real-time whenever a problem is detected. This ensures that there are no delays in critical processes.

It's also important that the IDS takes everyday switchgear processes into account. Personnel on-site must be able to easily understand alarms in order to respond to problems quickly. StationGuard is a user-friendly addition for day-to-day operations. It speaks the same language as control and network engineers. Therefore, the system enables faults to be remedied swiftly and reduces the coordination required with other departments.

StationGuard does not output any false alarms. This is partly because the system creates a model of the automation system based on the substation SCL file and 'knows' the installation. It's also due to StationGuard's maintenance mode. During maintenance work, special protocols are often used that are not required during regular installation operations. Under normal circumstances, an IDS would send repeated alarms while this task is being carried out due to the unrecognized activities and thereby interrupt the operation unnecessarily.

Our solution has another advantage: StationGuard compares each network packet with the model of the substation. As a result, it reliably detects cyber attacks and communication and time synchronization problems within the installation. During day-to-day operations, it helps identify faults and changes to the configuration and defective components promptly.

Many energy providers operate multiple installations. How complicated is it for them to operate all their stations in accordance with the regulations?
StationGuard doesn't require a long learning phase compared with many other solutions and it protects the installation immediately. This keeps the effort involved in its implementation to a minimum: the system can be configured, set up, and installed within a day. If the assets and configurations are already known through ADMO or StationScout, StationGuard simply builds on that information, simplifying migration.

The effort required for energy providers is reduced significantly if the same intrusion detection solution can be used for their switchgear. It's not uncommon for some stations to have adapted to the newer IEC 61850 standard, while some continue to operate with protocols such as IEC 60870-5-104. StationGuard supports all common communication protocols, which is a major advantage.

Does the IDS offer full protection?
Yes, because attacks within the installation can be detected quickly. However, comprehensive protection against cyber attacks also requires other security measures for preventing access to the installation. These include network segmentation, clearly controlled network transitions with firewalls, hardened maintenance computers, role-based access authorizations, remote access with secure tunnel connections, and of course, secure and device-specific user/password combinations. We're always happy to discuss specific requirements with our customers.

Thank you for talking to us.

Resolved quickly: StationGuard reliably records suspicious activities and displays clear alarms in an automatic substation overview.

Find out more about StationGuard:
omicronenergy.com/stationguard