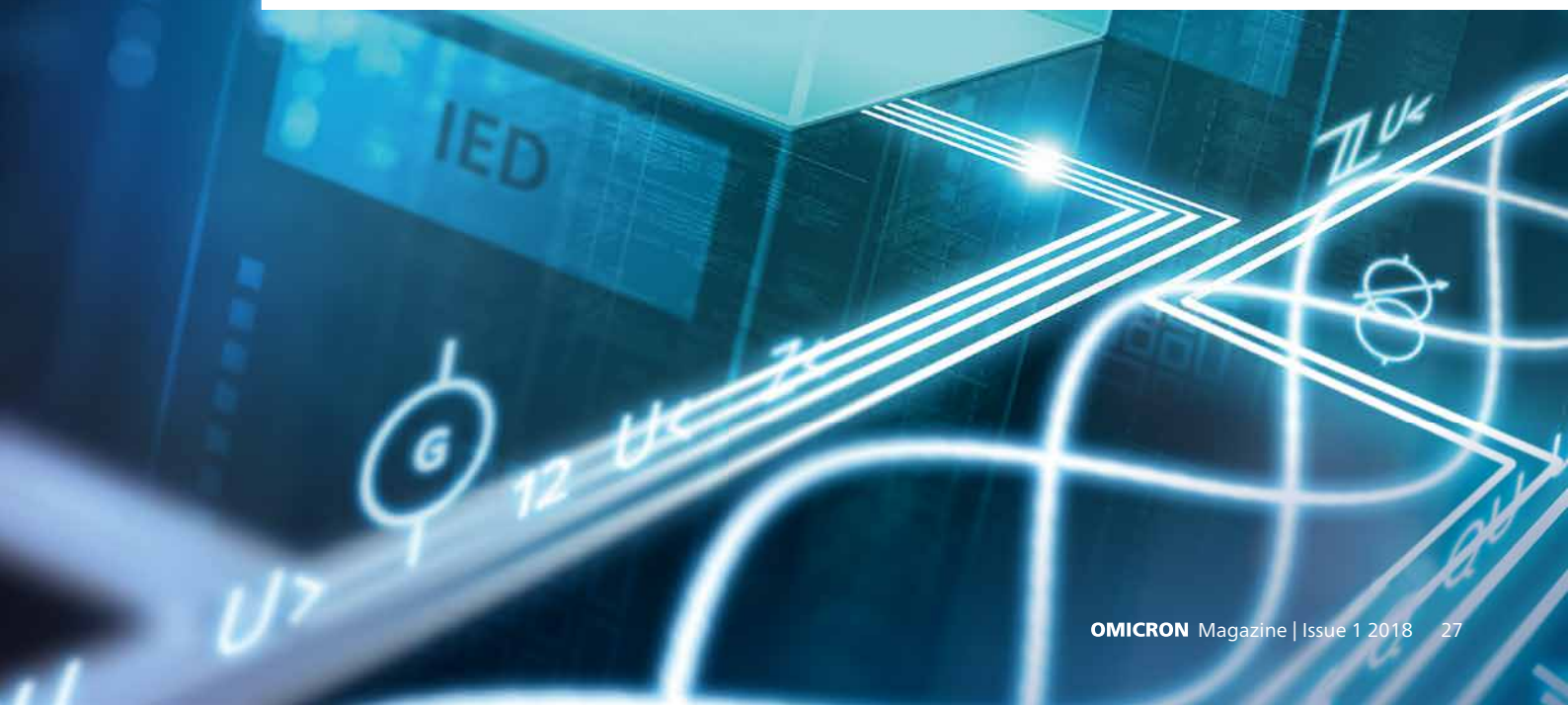
THE CYBER DILEMMA

How to include security in networked protection engineering

Protection engineering and IT – do they really belong together at all? Although their interaction is based on the same technology, there are vast differences between them when you actually look at the details. This poses great challenges to companies, especially when it comes to the topic of cyber security.

This situation has been exacerbated around the world by the introduction of new guidelines and statutory regulations, as IT is now responsible for all information systems used in the business environment. This also includes the information systems supporting the protection system as well as the rest of the entire energy supply.

Until now, the IT of the protection system had been an area where the IT department had deliberately handed over administrative responsibilities to the protection engineering department. Not least because it involves data and protocols that do not fall within the normal scope of activities of IT and are therefore difficult to control and monitor with the means available. Therefore, managing all technical equipment and software continued to be the responsibility of the protection engineering department alone. This does not merely include the relevant assets and their firmware and software, but also the test sets and their operating system and application software.



«An attack is less likely to be successful if employees within the company are aware of the individual steps of a potential attack.»

The expertise of the protection technicians is now mostly focused on the secure operation of the substation and less on the administration of IT systems and their complex infrastructure and functionality – not to mention the associated security aspects that are anything but trivial.

And let's not forget the public and political attention, which is moving the issue of IT security for critical infrastructures into the limelight, not least through incidents from recent history. Stuxnet, for instance: not something anyone will forget in a hurry. But there have also been two other successful attacks: in 2015 and 2016 on Ukraine's power supply, where around 230,000 people were suddenly left without power.

This motivated politicians to act as quickly as possible and draw up guidelines or statutory regulations for operators of critical infrastructures – including energy provision.

Regulations and guidelines

What form do the abovementioned changes or tightening take? Up until now, every region has done its own thing. In Germany, the legislator has amended the special provisions in the German Energy Act [Energiewirtschaftsgesetz]. Therefore, operators of energy supply networks have until January 31, 2018 to implement and certify an Information Security Management System (ISMS) pursuant to ISO/IEC 27001. An integrated approach is required here, which should be continuously reviewed with regards to its performance and effectiveness, and which should be modified as necessary. As a minimum requirement, the ISMS must include EDP and telecommunication systems used for controlling the network and those that are required for secure network operation – as per the IT Cybersecurity Act (ITSiG).

Since August 2016, a guideline (NIS Directive) has been in force throughout the rest of the EU for network and information security. EU member states have 21 months in which to incorporate this directive into appropriate national legislation, which presumably won't be too different from the ITSiG. It's the same story in Switzerland, which has dedicated itself to this issue with the "National Strategy to Protect Switzerland Against Cyber Risks" (NCS).

North America too has its agenda to safeguard energy provision against unauthorized attacks and the resulting problems from it. There is a whole range of guidelines for this purpose, covered by NERC CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection).

Ultimately the implementation of the guidelines remains the responsibility of the operators and their partners. The problem here is that the networking of infrastructures of various power supply companies as part of the smart grid is based largely on existing components and protocols from the IT sector.

Turning your back on communication media such as Ethernet is however not very advisable, as has been demonstrated by analyses of attacks and faults. Underlying data connections that are not even considered to be vulnerable are also often affected.

Awareness

The first step to be taken towards security is the permanent and ongoing training of personnel with regard to the awareness of threats. An attack is less likely to be successful if employees within the company are aware of the individual steps of a potential attack. Employees are usually always involved, but are largely unaware. Malware gets into the network through the careless opening of e-mail attachments, links in e-mails, external media such as USB thumb drives, insecure WiFi connections, unprotected installation of routers (connecting USB sticks or laptops, etc.).

When prompted to open an attachment or to click on a link, it is always better to first confer with the person sending the request. Removable storage devices belonging to protection engineers must never leave the assigned area of activity. This ensures that malware from less protected computers cannot accidentally be installed. Removable storage devices that have been given as a gift or have been found must be tested by the IT security department prior to use, preferably in a sandbox. In case of the latter, it would even be best to destroy them straight away. Since the malware is under supervision here, it can go wild without posing a risk to the company.

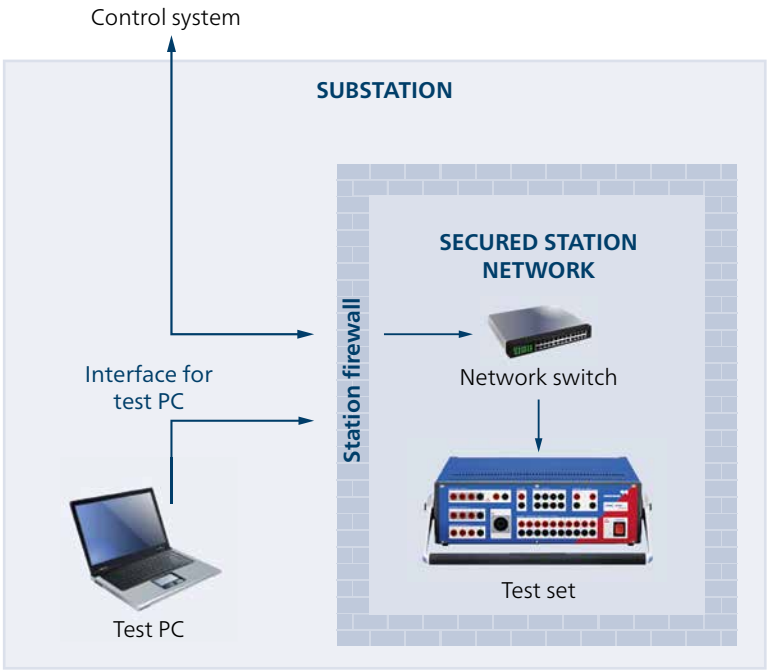
Secure test PC

Contrary to some of the rumors within the sector, let's be clear about one thing: every computer that can be accessed on a public network is usually vulnerable, no matter how "hardened" it is. The likelihood of an external attack can nevertheless be significantly minimized by deactivating any unnecessary Windows functions that are not needed for work in the protection engineering sector. Much could surely be gained by the constructive cooperation between the IT and protection engineering department to draw on the in-depth knowledge of the IT experts.

Security can be increased even further if computers that are used to parameterize the testing and maintenance of the protection engineering are strictly limited to this use and have no contact whatsoever with office IT or the Internet. This could be a test ▸

PC that is installed in the respective system, or a laptop that is exclusively used for protection engineering. Alternatively, it could be possible to have virtual machines on the computers that basically function in the same way as separate computers and strictly separate the individual areas.

A station firewall can be set up as an additional security level that monitors communication between the PC and the protection devices or the test sets, thereby preventing unauthorized access in extreme cases. This is very possible with the OMICRON test sets in particular. Meanwhile, there are firewall systems that can handle the protocols used in engineering substations. A tool like this also allows the logs to be used to determine if unauthorized access was attempted.



A station firewall monitors communication between the PC and the protection devices or the test sets, thereby preventing unauthorized access in extreme cases.

Cyber security with OMICRON

For some years, OMICRON has been actively addressing the issue of cyber security and its impact on the day-to-day work of performing tests in energy installations. These initiatives were expanded in 2016. The activities include technical aspects in product development projects and also a company-wide initiative on the issue of cyber security by OMICRON's executive management.

OMICRON test sets already provide a high level of security. Connecting to the test computer via USB disconnects it completely from the data communication network of the substation, thus making the transmission of malware virtually impossible. The same security is also offered by both Ethernet interfaces in the CMC, which are not interconnected. Therefore, the substation network connected to it is on a different network from the test computer

and the CMC does not transmit any packages from the "insecure" computer to the substation network.

An even bigger step towards security is to set up a so-called demilitarized zone. This means fully separating the protection engineering IT from the usual office IT. The standalone data management system ADMO allows such an infrastructure zone to be set up in the station network. ADMO is specifically tailored to meet these requirements in the protection engineering sector, thereby avoiding unnecessary functions that would make the system unclear and slow. This not only simplifies the daily processes, but also administration. All necessary data is collected and compiled here and then securely transferred to the relevant test or engineering computers. Now none of the documents are in an un-trusted zone like the office IT zone. Data received externally for the protection devices must nevertheless continue to be checked to ensure it is safe. No matter if it's new firmware, security updates, data transmission or the like – all of this can bring about undesirable effects.