Major energy company secures power with Advenica

advenica

Cybersecurity in
critical infrastructure

Cybersecurity in critical infrastructure – a matter of national interest and business value

With more frequent and increasingly viscious cyberattacks, vulnerabilities in IT architecture pose a severe threat. Particularly the energy sector is targeted, making upgraded cybersecurity a matter not only of securing production and business value but also of national interest to keep society up and running – and people safe.

Segmentation and data logging – fundamental security measures

To safeguard ICS and SCADA systems, segmentation must be applied with high assurance solutions to guard the physical isolation yet enable completely secure communication. With this in place, logging security data is the next priority. By monitoring logins, failed login attempts, transactions, USB usage etc, effective preventive measures can be mapped out and damage control can be taken without delay. However, the character of the data also makes log servers hackers' favoured target. Data logging systems thus turns into a vulnerability when insufficiently protected. To ensure integrity and security, military-graded solutions are required.

New strict legislation requires upgrade of security

In recent years, the energy sector has been scrutinised by supervising authorities regarding information security in preparation for instance the NIS Directive and stricter national security legislation. To significantly upgrade general security and to be able to present approved high-end solutions in future audits, one of the largest energy companies approached Advenica.

Rapid analysis and recommendation

After analysing audit reports and penetration tests, Advenica identified and prioritised several important measures with legislative compliance in mind. Working fast, a recommendation was presented 48 hours from receiving the reports.

> ***... a recommendation could be presented 48 hours from receiving the reports.***

Creating cybersecurity insight

With the energy company's business priorities weighed in, it was decided that security log data management and monitoring was fundamental to insight and further security efforts. A new log environment for security log data was consequently built, based on strict segmentation and with approved products to protect the various systems.

Eliminating risk of data leakage and manipulation

With national approval from armed forces, SecuriCDS Data Diodes deliver security to the highest level. They are the most effective option for classified systems. Containing an optical fibre with a transmitter on one side and a receiver on the other, only unidirectional information exchange according to information policy is allowed. Two-way transfer between the networks is impossible, and the risk of leakage and manipulation of log data is eliminated. The SecuriCDS Data Diodes deployed at the energy company have integrated proxy servers. These have been

SecuriCDS Data Diodes

SecuriCDS Data Diodes not only prevent intrusion and maintain network integrity but just as effectively prevent leakage and maintain network confidentiality. This high assurance solution safeguards assets for operators within ICS/SCADA or the defence industry. Guaranteeing unidirectional separation between network interfaces, SecuriCDS Data Diodes can safely connect two networks of the same or different security levels.

Benefits

- Creates unidirectional log data traffic from monitored systems to the log data collection system
- Eliminates data leakage from the log data system and any risk of the log data system turning into a jumping point for attacks.
- Enables strict segmentation while retaining central monitoring of systems and networks.
- Makes it possible to use one, single log data collection system without jeopardising security – this cuts costs, increases administrator insight and improves the ability to detect attacks and quickly take countermeasures.

Advenica SecuriCDS Data Diode

designed, developed and tested to meet the requirements for interacting with sensitive information in common communication formats such as data, files or network time transfers.

Mitigating threats of remote access

ZoneGuard was implemented to further reduce potential attacks vectors while providing secure and selective access to the systems from remote networks. The technology allows secure information exchange between separate systems, with access based on the energy company's defined policies and tuned for their specific systems. By using ZoneGuard with remote desktop capability, access is controlled and threats towards a remote desktop solution are effectively mitigated in the cross domain point. All information is validated and transformed, which means that sensitive information stays within the protected network and malicious code cannot spread.

Maximising support of investment

To make sure that the energy company gets the most out of their new cybersecurity solutions, a Managed Services Agreement was signed for both remote and on-site operational control and system support. This means that Advenica's experienced team is available 24/7 to answer questions. With our continuous presence potential threats can be discovered well in advance and information security can be boosted.

World-class cyber preparedness without compromising local operations

> *The energy company can also report pre-approved cybersecurity solutions to supervising authorities.*

With Advenica the energy company in question quickly achieved increased security insight. It boosted its preparedness for threats such as Industroyer, which could come at great cost not only to business, but to customers. The energy company can also report pre-approved cybersecurity solutions to supervising authorities. In addition, both technology and services enable cost-effective administration without compromising current or future reliability and integrity.

ZoneGuard

ZoneGuard offers a custom-fitted yet simple information policy-based solution for secure information exchange between varying security domains. As a gateway, it uses a whitelisting approach, only forwarding received information that complies to information policy structure, format, types, values and digital signatures. Any changes require a digitally signed information policy by either an IT security department or another appointed policy approver. ZoneGuard also provides log control and audit trails – vital evidence of compliance to policies and regulations.

Benefits

- Enables suppliers to support equipment through the remote desktop protocol (RDP)
- Prevents risky, unnecessary connections associated with RDP, such as printer, microphones and speakers
- Prevents unauthorised use
- Prevents direct network communication, thus preventing viruses and ransomware to spread from the site to the supplier, and vice versa
- Provides full traceability – who, what and when
- Can be extended with time-limited or scheduled connectivity
- Possible to design a four-eyes principle, enabling an internal gatekeeper to decide how and when connectivity is allowed

Advenica ZoneGuard

Fast track to secure production, compliance and long-term business value

Big challenges

- Desire to upgrade general security
- Compliance to increasingly stricter legislation
- Certified solutions required
- Vulnerabilities in IT architecture
- Insufficient security log environment
- Classified systems

Smart solutions

- Apply strict segmentation to networks
- Enable secure information exchange with ZoneGuard
- Create secure log environment to collect security data
- Eliminate all risk of data leakage and manipulation with SecuriCDS Data Diodes, approved to the highest level of security in several European countries
- Optimise security and operational conditions with Managed Service Agreement

General benefits

- High assurance cybersecurity
- Enforced information policy
- Reduced potential attack vectors
- Secure information exchange with no risk of data leakage or manipulation
- Products approved to the highest level of security
- Quick and simple deployment
- Cost-effective and secure administration
- Experienced teams at hand

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at: www.advenica.com

advenica

ISO 9001
CERTIFIED
ISO 14001
CERTIFIED