



Major Insurance Company Secures Personal Information in Data Centers with Advenica



Cybersecurity for
insurance companies

Cybersecurity for insurance companies – Protecting critical and personal information

Ransomware attacks on companies with personal information are more frequent than ever. The attacks can block all computers, and thus all digital communication, with the attacker demanding a ransom to unblock them. The only way to avoid falling victim to these attacks is to work with cybersecurity in a consistent and structured way.

Personal information must be protected from leakage

Insurance companies are typical examples of businesses that handle a lot of critical and personal information on a daily basis in their internal networks. It is of course highly important to make sure that leakage of such information is not possible, as this could have devastating effects both businesswise and on a personal level.

Attacks on insurance companies happen all the time

An example of an insurance company that has been attacked is Chubb. Chubb is a leading provider of cyber insurance products, dealing with forensics, incident response and investigation costs, data loss and restoration, crisis communications and public relations among other things. Chubb¹ was targeted by the Maze ransomware group in March 2020, who claimed to have encrypted the firm's systems and threatened to release stolen data if a ransom was not paid.

¹ Insurance firm Chubb allegedly hit by Maze Ransomware from <https://www.teiss.co.uk/chubb-ransomware-attack/>

Filtering information can be the solution

To upgrade security and avoid leakage of information, a major European insurance company approached Advenica. To secure their internal data centers, where the critical and personal information is handled, a filtering solution was installed.

Advenica ZoneGuard technology allows secure information exchange between separate systems, with access based on the insurance company's defined policies and tuned for their specific systems. By using Advenica ZoneGuard, all information is validated and transformed, which means that sensitive information stays within the protected network and malicious code cannot spread.

The insurance company now sends syslog information from the secure network, via Advenica ZoneGuard, to the SOC (Security Operation Center) system. Advenica ZoneGuard is a perfect extension to the customer's SOC/SOCaaS implementation to assure that only defined allowlisted data, which complies to their tailored policies, is allowed to enter or leave a network domain. This shows how Advenica ZoneGuard can be customised for special requirements in customer networks.

Advenica ZoneGuard

Advenica ZoneGuard offers a custom-fitted yet simple information policy-based solution for secure information exchange between varying security domains. As a gateway, it uses an allowlisting 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



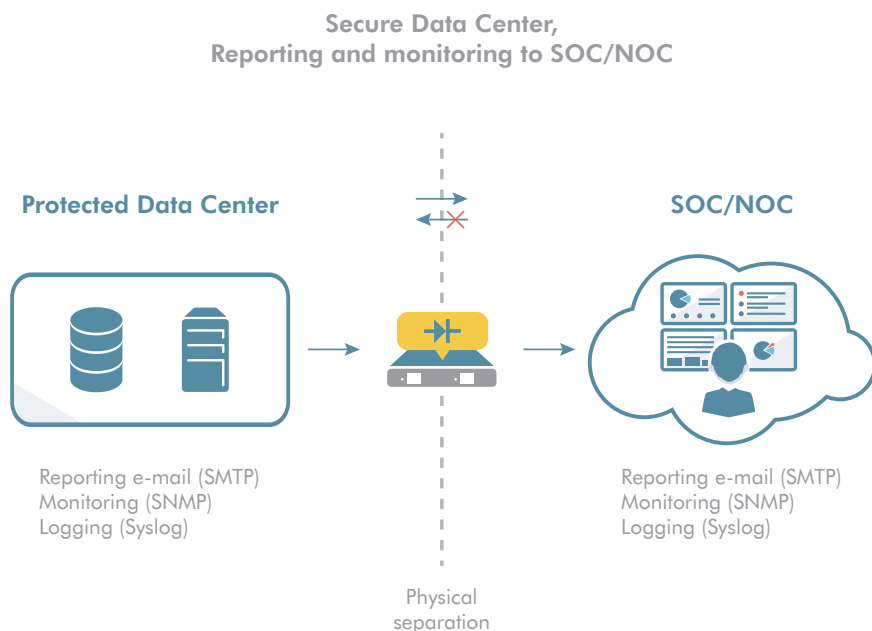
Advenica's Data Diodes ensure both operational functionality and security

Secure extracting of performance and reporting data

Another way of providing a secure way to export performance values, monitoring and network management data without opening any channel that could compromise the servers in the data center, is to let it be handled by SecuriCDS Data Diode DD1000i, including SMTP, SNMP and SYSLOG services.

The benefits of this solution are:

- Secure one-way data transfer without sacrificing domain integrity
- No malicious reverse traffic or access physically possible
- Allows more flexible role-based operation



Advenica Data Diodes

Advenica 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, Advenica 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 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 advenica.com



© Copyright 2021 Advenica AB. All rights reserved. Advenica and the Advenica logo are trademarks of Advenica AB. All registered and unregistered trademarks included in this publication are the sole property of their respective owner. Our policy of continuous development may cause the information and specifications contained herein to change without notice. Doc. no.: 19288 v1.0

ISO 9001
CERTIFIED
ISO 14001
CERTIFIED