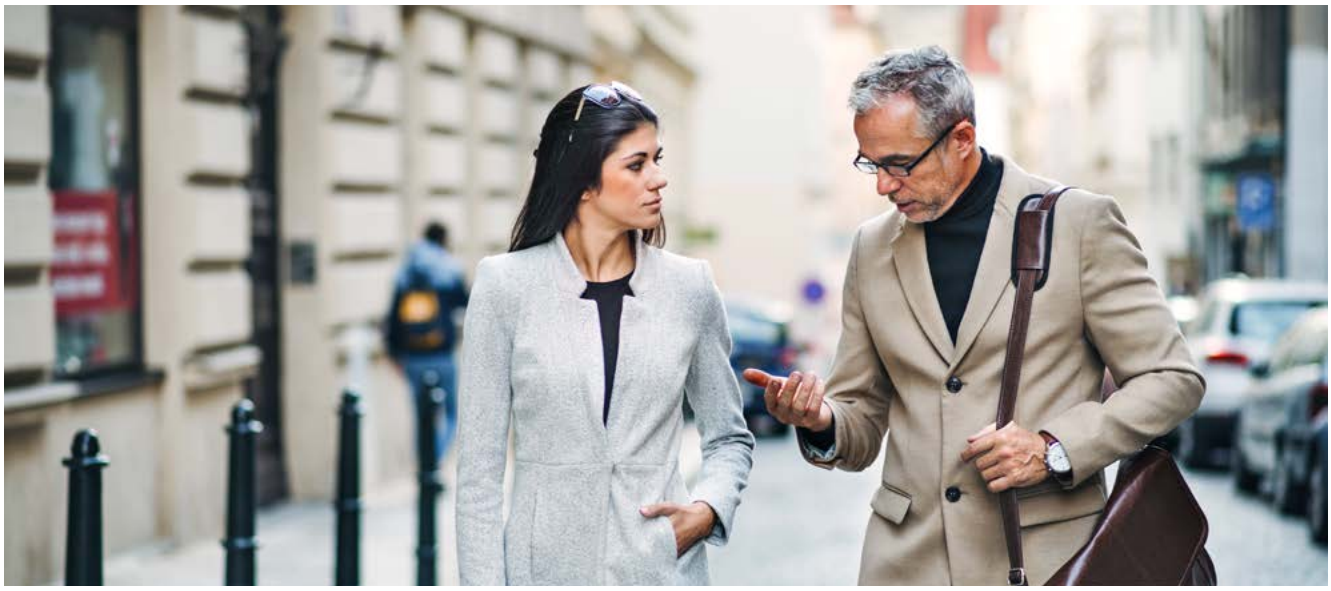
advenica

Securing municipalities' digital communication



Cybersecurity for municipalities

Cybersecurity – your responsibility towards your citizens

Ransomware attacks on municipalities and similar organisations are more frequent than ever. The attacks can block all computers, and thus all digital communication, with the attacker demanding a huge ransom to unblock them. Going without digital communication is hardly an option in today's world, and the only way to avoid falling victim to these attacks is to work with cybersecurity in a consistent and structured way.

Digital communication – quick, easy and risky

With digitisation more devices are connected to the Internet – convenient, but this also increases the possible attack routes into the IT structure. At the same time, the methods used by the attackers of today are more and more refined, and the attacks today are usually targeted and well-planned.

Millions of reasons to invest

In April 2019, around 10,000 Baltimore, Maryland (USA) city computers were infected with "file-locking" ransomware. The hackers demanded a ransom of 13 bitcoin (approx. USD 100,000), but the city refused to pay up.[1] The attack made it impossible to use municipal payment and finance systems. The effect was that

1 Baltimore government held hostage by hackers' ransomware from https://www.bbc.com/news/technology-49393479

© Advenica 2019

houses could not be sold, bills could not be paid etc. while city networks were closed down. The mayor estimated the ongoing damage to be over USD 18 million, including "USD 8 million lost because of deferred or lost revenue while the city was unable to process payments."

Lake City, a small Florida city, suffered a catastrophic malware infection in June 2019. Despite the city's IT staff disconnecting impacted systems within ten minutes of detecting the attack, a ransomware strain infected almost all the city's computer systems. The only exception were the police's and fire department's systems which are run on a separate network. A ransom demand was made a week after the infection, with hackers approaching the city's insurance provider who negotiated a ransom payment of 42 bitcoins (USD 480-500,000).

Attacks are more frequent – and very expensive

Data intrusions are constantly increasing. According to CNN at least 170 county, city or state government systems have been attacked since 2013.[2] And as Baltimore and Lake City know, a data breach can become very expensive. Another example is the Danish shipping and oil company Maersk that in 2017 was hit by an huge cyberattack, which almost made the company disappear from the market. The attack cost the company about USD 300 million in lost revenue. Also, the entire IT structure had to be reinstalled.

> ***... at least 170 county, city or state government systems have been attacked since 2013***

New legislation – higher demands on information security

The NIS directive sets a range of network and information security requirements which apply to operators of essential services and digital service providers. Since it is an EU directive, every EU member state must adopt national legislation, which follows or 'transposes' the directive. The directive aims to achieve a high common level of security in networks and information systems for critical societal and digital services within the Union. This way, the internal market will be stronger and the vulnerabilities of central social services will reduce.

2 Crippling ransomware attacks targeting US cities on the rise from https://edition.cnn.com/2019/05/10/politics/ransomware-attacks-us-cities/index.html

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

© Advenica 2019

How to keep your citizens' integrity and privacy safe

Advenica helps customers identify vulnerabilities in current hardware and network components. Based on this we advise how to take strategic and effective measures towards higher information security. Our 20 years of experience with cybersecurity solutions means we can advise the best path based on your needs regarding information security. We help government agencies, county councils and municipalities to protect classified information and keep their infrastructure running. Our solutions will also help you achieve compliance with GDPR, NIS and security protection legislations.

Obtain security insight

Advenica's risk and security analysis is a great way to start to working actively with cybersecurity. It quickly and effectively surveys your current IT security as well as your future needs. Based on the analysis, it is possible to evaluate the requirements to make sure that the right level of security is defined according to identified challenges.

Make higher demands on information security

Verify that security is built into the system ...

Complex networks and increased dependence on network-based services raises the need for higher security and quality levels. To obtain this requires robust systems and access to security solutions that protect the information and ensure that data is not lost. Unfortunately, users are usually not particularly good at security requirements when it comes to computers, applications and systems connected to the Internet. It is therefore of the utmost importance to include information security right from the start when writing requirement specifications for new technology, conducting procurement of new technology or initiating dialogue with potential suppliers. The most serious issue is often that existing, perhaps outdated, systems and networks pose the most severe threat to IT security. All older equipment exposed to connected networks should be security tested to detect security holes. To cope with potential threats to the systems, you must rethink security. Verify that security is built

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

© Advenica 2019

into the system, that the systems are secure from the ground up. This way, information security will not add complexity – instead, it will be built into the base of the network systems.

Network segmentation – fundamental for information security

Many IT architectures are based on systems designed during a politically stable era, and have often grown over the years. Getting current information on e.g. electricity use, ordering 24/7 services or teleworking have also become standard, resulting in interconnected SCADA systems, business systems and the web. To safeguard critical information, strict network segmentation must be applied with a combination of physical and logical separation. Physical separation creates security zones deployed on physically different hardware appliances. Logical separation allows different zones or network traffic to be co-allocated on the same hardware or network cable – less obvious and with less confidence in the separation mechanism strength than physical separation. Physical separation must always be applied when separating critical systems such as SCADA systems from less critical systems, e.g. office networks and the internet. Information flows between security zones must always be monitored to prevent information leakage and to protect the integrity of sensitive systems. Certified solutions that meet military standards deliver the highest level of security and functionality.

Eliminate risk of data leakage and manipulation

To protect sensitive systems and confidential data – Advenica Data diodes are the failsafe way to go. The function of a data diode is to allow all data to pass in the forward direction, while blocking all data in the reverse direction. The fibre optical connection makes it physically impossible for data to travel in the opposite direction. And as it is not software, it cannot be directly attacked by malicious code, which results in high assurance. Every organisation operating sensitive information has great use of a data diode to protect its valuable information and securely exchange data.

Mitigate threats of remote access

To further reduce potential attack vectors and at the same time provide secure and selective access to the systems from remote networks, a gateway for controlled information exchange – ZoneGuard – should be implemented. 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.

Secure file import

Importing files into secure environments is another area that poses a significant security threat unless the files are properly sanitized before transfer. By using File Security Screener, a high assurance Cross Domain Solution with malware scanning and content disarm and reconstruction capabilities, efficient and automated countermeasures for malwares is provided. At the same time, separation for the connected networks are secured. The File Security Screener provides an efficient, scalable and trusted solution for secure file import.

File Security Screener

Importing files into secure environments poses a great security threat if the files are not properly sanitized before transfer. The File Security Screener is a high assurance Cross Domain Solution with malware security scanning and content disarm and reconstruction capabilities.

Benefits

- *Malware scanning by integrating to any third-party solution such as OPSWAT MetaDefender Core and sandboxing environments*
- *High assurance protection from information leaks by using Advenica´s Data Diodes.*
- *High assurance separation between different import sources by the use of Advenica´s Data Diodes.*
- *Caching of data to be scanned, allowing service on the central equipment without data loss.*
- *Customizable import rules based on the source of the information and the file type.*
- *Scalable solution with ability to increase the number of connected source networks or increase throughput.*

© Advenica 2019

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

© Copyright 2018 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.: 18533 v1.0

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED