advenica

# Protecting Banks' Important Assets

Cybersecurity for banks

# Cybersecurity – Your Responsibility Towards your Clients

Cyberattacks are a constant threat to authorities as they handle a great deal of sensitive information. For banks, this is also an important threat as they manage many vital assets and sensitive information.

## Digital communication – quick, easy and risky

With digitalisation, more devices are connected to the Internet – convenient, but it also increases 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 attacks are usually targeted and well-planned.

## Attacks targeting banks

It can become very expensive not to protect information properly. The Development Bank of Seychelles experienced a ransomware attack on their network in September 2020[1]. During a ransomware attack, the attacker encrypts the victim's files and demands a ransom to make them accessible again. This means that gaining access to the files again after an attack can become far more expensive than to pay for secure protection and thereby avoid such risks.

1 CBS closely monitoring DBS' report of a ransomware attack on its network from https://www.cbs.sc/Downloads/Pressrelease/CBS%20closely%20monitoring%20DBS%E2%80%99%20report%20of%20a%20ransomware%20attack%20on%20its%20network.pdf

Hungarian banking services were also affected by a critical cyberattack during 2020 – a so called distributed-denial-of-service (DDoS) attack. This was considered to be one of the biggest DDoS attacks in Hungary[2]. During a DDoS attack, the system is flooded with data traffic by the attackers with the aim to paralyse the system. During the incident mentioned some banks' services were interrupted. This kind of attack can mean great costs in terms of the organisation not being able to run in its normal speed, meaning that employees and potential customers cannot access the system.

2 Hungarian banks, telecoms services briefly hit by cyber attack - Magyar Telekom from https://www.reuters.com/article/us-hungary-cyber/hungary-hit-by-large-cyber-attack-from-asia-magyar-telekom-idUSKBN26H0CB?il=0

## New EU Guidelines for banks

Since so much is at stake, banks cannot take the risk of not having secure protection against threats. On June 30th 2020, the new EU guidelines regarding cybersecurity for banks[3] came into force. The guidelines address financial institutions, referred to as payment service providers, credit institutions and securities companies.

The new guidelines from the European Banking Authority, EBA, are the European standard for managing security and IT risks. It describes how banks, fund managers and providers of payment services operating within the EU are to manage internal and external risks linked to IT and security. These guidelines aim to reduce the likelihood of attacks that can lead to data leaks and disruptions.

Amongst other things, the guidelines point out which security measures that must be developed and implemented to mitigate IT and security risks that financial institutions are exposed to. It is essential to understand that the guidelines have legal status and that the operators covered are therefore obliged to justify any deviations from its application.

3 EBA:s riktlinjer för hantering av IKT-risker och säkerhetsrisker from https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880828/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_SV.pdf

## What information security requirements do the new guidelines set?

The guidelines contain a lot of information, but a central requirement regards classification. This requirement states that financial institutions must make a classification of business functions, support processes and information assets, judged on how critical these are.

Another vital requirement is information security measures; the guidelines state that security measures have to be developed and implemented to mitigate IT and security risks that financial institutions face.

*Banks cannot take the risk of not having secure protection against threats*

## How do we know what information to protect?

It is vital to classify all kinds of information in order for the organisation to be able to handle it correctly. To do the classification, you must evaluate aspects such as the value and sensitivity of the information, the legal requirements and the importance of the information for the business. A good way to determine how the classification should be done is to use a risk and security analysis. It helps you to map your current information security as well as your future needs.

## You need more than a firewall

In order to protect what is most sensitive and critical to operations, a technology other than firewalls should be considered. With a firewall, it is difficult to know exactly what information is being exported or imported into the system. A firewall configuration often becomes complex, which increases the risk of misconfiguration. Firewalls also do not separate administration and data flow in a way that protects the information from insiders. Also, when firewalls are managed through cloud services, the outsourcing itself involves additional risk exposure. Firewalls work great in environments with large data flows where traffic is versatile and changeable, e.g. as external protection for the Internet and for division into DMZ

### 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 e.g. critical infrastructure, municipalities 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

and office environment. It is important to establish a deep defence with several security barriers between what is considered to be most sensitive and the threatening actors. Security products from different suppliers should be used to reduce the risk that the same vulnerability exists in all products. Configuration changes of security products should be controlled so that changes are reviewed by more than one person who understands and can approve the change.

## Network segmentation improves security for banks

An excellent method for mitigating security risks and protecting critical information and critical systems is network segmentation through a combination of physical and logical separation. Physical separation means that safety zones are defined and distributed on different physical hardware. Logical separation means that different zones or network traffic are allowed to coexist on the same hardware or in the same network cable, which makes it less apparent – and thus leads to lower confidence in the strength of the separation mechanism than that of physical separation.

***Advenica's Data Diode achieves both function and security***

Network segmentation in situations where one-way communication is imperative, i.e. where information must only go in one direction, can be solved effectively with data diodes. The most important thing about a data diode is that information only can pass in one direction. In Advenica's SecuriCDS Data Diode, the separation and diode function is based on an optical transmitter and receiver. The design guarantees that no data whatsoever passes in the opposite direction. With certified solutions such as Advenica's SecuriCDS Data Diode, which meets military standards, achieves both function and security. We also have solutions for network segmentation for situations where a two-way information flow is necessary. Here, data is effectively filtered, and in every transfer it is ensured that the organisation's information policy is followed. Advenica's ZoneGuard offers a custom-fitted yet simple solution based on allowlisting of information in an information policy. The solution ensures that organisations can exchange information between security domains at different levels in a secure and correct way.

### 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 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 ZoneGuard

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