SOLUTION FOR FINANCE & INSURANCE

macmon
nac smartly simple

macmon Network Access Control: Network security as an important part of banking IT

Financial institutes are one of the sectors with the highest requirements for information security. On the one hand, this is because almost all the business processes are IT-based and therefore there is a great dependency on the availability of systems that are becoming increasingly complex. On the other hand, the threat posed by cyber crime is increasing significantly. This growing vulnerability and risk of economic losses as a result of IT risks increases the pressure on having an active IT security management in banks and other financial institutes.

macmon benefits for protecting networks in the financial sector

- ✓ Comprehensive monitoring of the banking network
- ✓ Monitoring and control of all the devices present in the network (live asset management) and documentation of all access to the bank's network
- ✓ Defining specific data routes and transfer interfaces for better and more specific protection of sensitive data like customer information
- ✓ Ensuring the integrity of the network by only granting network access for the defined (internal and approved) devices
- ✓ Enabling flexible access (time and space) to selected areas of the network (VLANs, WLANs) and simultaneously protecting sensitive data from unauthorized access
- ✓ Supporting the implementation of the minimum requirements for risk management (MaRisk) published by BaFin
- ✓ Supporting the ISO 27001/ 27002 certification and the implementation of the BSI* standard for information security management and basic IT protection catalog

Compliance with legal stipulations and regulations

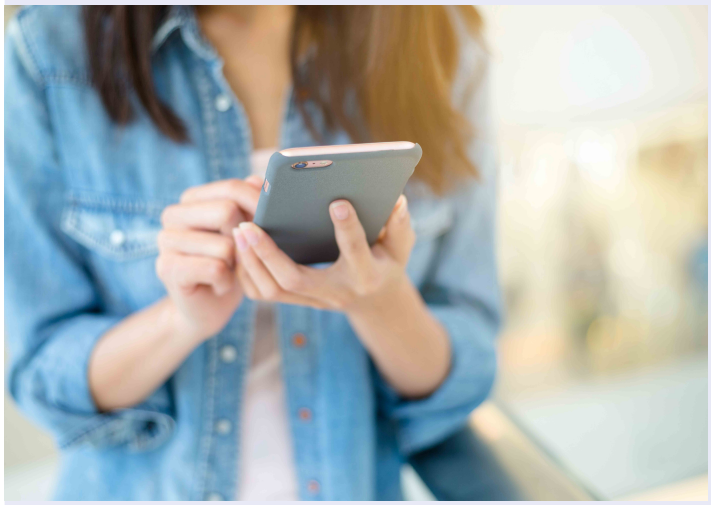
The Legislative authority now recognizes the growing threats in the field of information technology and there are a number of regulations and legal requirements for minimizing the risk. Hence banks, insurance companies, financial service providers and stock exchanges in Germany are classified under critical infrastructures. The federal government considers „the protection of critical infrastructure by the government and industry as an important national duty because the internal security is increasingly influenced by IT security."

The minimum requirements for risk management (MaRisk) published by the Federal Financial Supervisory Authority (BaFin) stipulate „the safeguarding of integrity, availability, authenticity and confidentiality of the data for IT systems and associated IT processes." While designing the security of IT systems and associated IT processes, it is advisable to refer to commonly available standards like the ISO standards 27001 and 27002.

*BSI: Bundesamt für Sicherheit in der Informationstechnik = Federal Office for Information Security

There are many recommendations on network security in these standards. Hence the installation and use of unapproved IT components should be prohibited and the compliance with this prohibition should be checked regularly. The introduction of unauthorized and unsecure devices into the network should be effectively prevented.

The network access control solution macmon developed by macmon secure ensures compliance with these security regulations. macmon detects, reports and prevents the use of external systems in the network and prevents the use of unauthorized devices.



macmon provides a flexible solution, which supports the 802.1X standard on the one hand and can also detect devices reliably on the other hand for special devices, like e.g. ATMs.

Banking confidentiality: Complete data security

Data security and handling confidential data in a responsible manner is very important in the banking environment. The customers assume that the banking confidentiality and the security of personal data is always ensured. Undesired disclosure of confidential customer and account data thus represents a significant risk. The damage to the reputation that is linked to it often outweighs the business or penal damages. This was particularly demonstrated in the data theft cases at the banks in Liechtenstein and Switzerland which have come to light in the past few years.

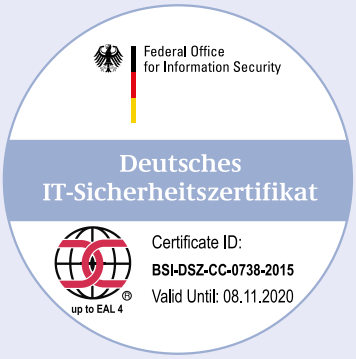
An important component of data security is the network access control. macmon ensures that only authorized, authenticated and securely configured systems are present in the network. Thus macmon helps preventing intrusion in to information systems, safeguarding sensitive data and personal information and protecting from unauthorized access.

Certified security based on the common criteria

As part of its cyber security strategy (02/2011), the federal government is taking measures in different strategic areas. This includes promoting and stipulating the use of IT components that have „undergone a certification according to an internationally recognized certification standard".

macmon is presently going through the BSI* certification process for certified security services according to the international Common Criteria (CC) standard. The certification of an IT security product according to this standard demonstrates that criteria for secure and trust-worthy systems have been met even during the development and that the product was objectively evaluated by a neutral and competent authority.

*BSI: Bundesamt für Sicherheit in der Informationstechnik = Federal Office for Information Security



Contact

macmon secure GmbH
Alte Jakobstrasse 79-80 | 10179 Berlin | Germany
Phone: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu