SOLUTION FOR AUTHORITIES

macmon
nac smartly simple

macmon Network Access Control: as an important part of information security in public authorities and administration

There are a lot of standards and recommendations regarding security processes in all industries, but public authorities are handling some of the most sensitive data available – details about every one of us. ISO/IES 27002, Information Commissioners Office (ICO), UK Data Protection Act (DPA) and others demand a high level of data protection and integrity of the network.

In Germany, the BSI - Bundesamt für Sicherheit in der Informationstechnik = Federal Office for Information Security operates a guide for basic protection, which includes a good definition of a simple network overview requirement: "the installation and use of unapproved IT components should be prohibited and the compliance with this prohibition should be checked regularly". This guideline is similar to the Standard ISO/IEC 27001 and 27002 which is of course well known and established in the UK as well. Five out of 18 sections of this standard refer to a similar predictive control mechanism:

Section 6: Organization of information security
6.2 Mobile devices and teleworking
"There should be security policies and controls for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets and other Boys Toys)..."

Section 8: Asset management
8.1 Responsibility for assets
"All information assets should be inventoried and owners should be identified to be held accountable for their security. 'Acceptable use' policies should be defined, and assets should be returned when people leave the organization."

Section 9: Access control
9.1 Business requirements of access control
"The organization's requirements to control access to information assets should be clearly documented in an access control policy and procedures. Network access and connections should be restricted."

Section 12: Operations security
12.1 Operational procedures and responsibilities
"IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Capacity and performance should be managed. Development, test and operational systems should be separated."

Section 13 Communications security
13.1 Network security management
"Networks and network services should be secured, for example by segregation."

Added value to protect the network of authorities

- ✓ Monitoring and controlling all the devices located in the network (live asset management).
- ✓ Documenting all the accesses to the public/administration networks, even in case of diversified organizational structures.
- ✓ Ensuring the integrity of the network by only granting network access for the defined (internal and approved) devices.
- ✓ Providing dedicated and temporary Internet access for visitors, without having to set up separate WLAN infrastructures for employees and guests.
- ✓ Protecting the administrative IT system from attacks on sensitive and personal data.
- ✓ Supporting the implementation of ISO and DPA recommendations covering large parts of the advises.
- ✓ Certified security based on the common criteria.

Asset overview as in section 8, network access restriction as in section 9 and network segregation as in section 13 are the epitome of Network Access Control. Additionally, there is no other way of achieving this while in the same time reducing the cost of effort.

The DPA & ICO

The UK Data Protection Act is the defining legislation for the UKs data protection standards. The Information Commissioners Office is the government body tasked with ensuring the Data Protection Act is adhered to and the act evolves with technological advances. The 7th principle of the UK Data Protection Act states that:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

macmon's VLAN management and compliance technologies ensure that only authorised & compliant devices can access the network and when they do they need to be in the correct group to obtain access to the most sensitive data.

Data controllers need visibility of their computer systems and network to undertake a reliable risk assessment. That's why the DPA advises that the Data Protection risk assessment should take account of factors such as: *"... the nature and extent of your organisation's premises and computer systems."*

As a summary, macmon allows you to gain complete overview of your network, control all access and raise the security level by dynamic segregation according to demanded and supposed access rights.

Certified security based on the common criteria

Related to the requirements mentioned above and the high demand for proven secure technologies, macmon achieved a certification based on the common criteria. The process of the certification itself was operated by the BSI, as a German governmental and trustworthy organisation.

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.

Contact

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