CASE STUDY
HASSBERG-KLINIKEN

Network Security for Haßberg-Kliniken

Protection of critical infrastructures

The municipal company Haßberg-Kliniken operates two primary health care facilities in Haßfurt and in Ebern, in the Würzburg area. A total of around 10,300 inpatient and almost 17,200 outpatient cases are treated by a highly qualified team of doctors and nurses each year.

Haßberg-Kliniken have a high level of competence in the field of modern surgical and diagnostic procedures. An IT network with 1,000 endpoints ensures high- quality, fast and reliable patient care. The network integrates modern medical devices via a network connection and can thus provide doctors and nurses with secure and direct access to digital information, such as MRI data.

Medical devices are particularly important for modern surgical and diagnostic procedures. macmon NAC protects these devices from unauthorized access.

The workstations of the clinic employees are equipped with 160 thin clients, 165 computers and 75 laptops. Among the endpoints are 250 printers. 76 medical devices such as MRI, sonography or X-ray machines are currently networked, and this figure is set to increase. Surveillance cameras or card readers are also part of the infrastructure. Traditional IT networks that integrate endpoints such as MRI systems are now becoming medical networks. This means that a risk assessment based on DIN 80001-1 must be carried out for every device, no matter how small, for example a camera or laptop. Effective monitoring and security of these hybrid networks is essential; a disruption can have life-threatening consequences for patients if, for example, ventilators in the intensive care unit are affected.

"The goal of our IT security concept is to protect against internal and external attacks, guarantee the functionality of all systems and, of course, to provide data security, as we are dealing with highly sensitive patient data.
The security of particularly critical areas such as the operating theaters or recovery rooms, the laboratory and the intensive care unit also forms part of our security concept. Systems that require special protection include: the hospital information system (HIS), the laboratory information system (LIS), the radiology information system (RIS) and various diagnostic systems."

Jan Schmitt, Systemadministrator for the Haßberg-Kliniken

Date : 07/2021

"A penetration test showed that there were significant deficits in network transparency. Based on a recommendation from a security advisor, we opted for macmon NAC. With macmon Network Access Control we know at all times which devices are on the network and can automatically grant or deny access to them using switch port-specific rules. The security vulnerability has been eliminated and the network security has been significantly improved."

Jan Schmitt,
Systemadministrator for the Haßberg-Kliniken

Medical staff will always require access to sensitive data. macmon NAC, however, prevents unauthorized third parties from accessing this data.

macmon NAC provides invaluable assistance when it comes to network security

In practice, the clinics use macmon NAC to block unknown MAC addresses as soon as they connect to the network, for example if an employee plugs a new device into the data socket. Likewise, an unknown device belonging to an attacker cannot access the company network and therefore cannot cause any damage — a major advantage given the increasing volatility of security issues for hospital IT. Since the clinic is housed across two locations, according to Schmitt, the IT department did not have an immediate overview of changes in the network before using macmon NAC. PCs or thin clients were reconfigured by the site maintenance team, or service engineers made changes to essential endpoints such as MRI machines without consulting IT.

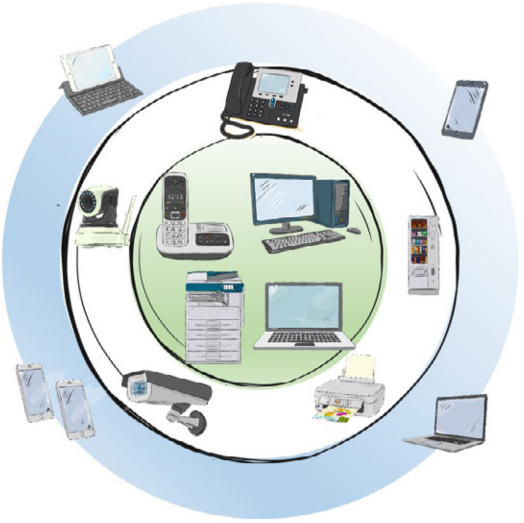
"macmon reliably supports the work of the IT department. Now the users and the service engineers keep us informed of changes well in advance, otherwise they cannot continue working."

Jan Schmitt, System Administrator for the Haßberg-Kliniken

Changes in the network are now immediately visible to the IT department and the devices are managed according to the situation. Untrustworthy devices can be switched to a visitor or quarantine VLAN by macmon as soon as they appear in the network. macmon NAC also shows when a device was last active in the network. According to Schmitt, this means that „dead entries can be identified in the network." Devices that have not been seen on the network for a long time or are classified as unsafe after a „compliance check" can be kept in a quarantine network until the status has been clarified.

In general, Haßberg-Kliniken have three security zones: Unauthorized devices in the LAN and WLAN are detected by macmon NAC and blocked. Devices that identify themselves using a known MAC address are permitted to access specific parts of the network. Devices with a recognized computer identity can work in a third zone. This includes, for example, laptops or PCs.

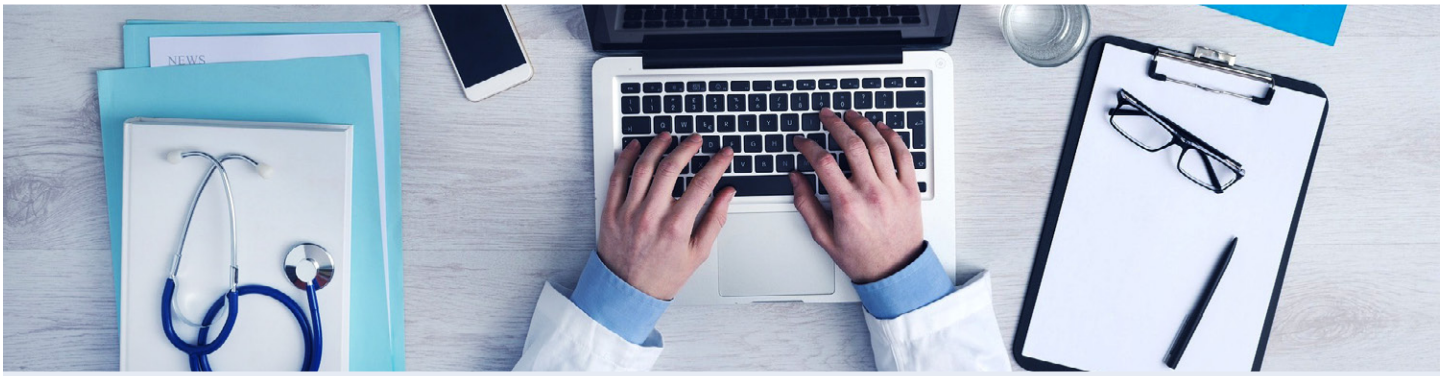
The three security zones at Haßberg-Kliniken



Zone 1: Authorized devices in the LAN/WLAN with computer identity

Zone 2: Authorized devices in the LAN/WLAN with MAC address

Zone 3: Unauthorized devices in the LAN/WLAN



Safe and sustainable investment in the security of critical infrastructures

The high level of security provided by macmon NAC not only makes the software easier to handle and operate, but also allows users to interface with other leading security products. In conjunction with IT

security solutions, macmon NAC can, for example, automatically quarantine a non-compliant device and inform the network administrator of an attack before it has a devastating impact on the hospital. macmon has interfaces to popular antivirus solutions, to endpoint security, IT incident management, intrusion detection or prevention systems (IDS/IPS), asset management, inventory, security incident & event management solutions (SIEM). macmon NAC can also be seamlessly integrated into other security products such as compliance connections, infrastructure connections, asset management and identity stores.

Users can exploit the full potential of existing solutions as well as macmon NAC and, thanks to its scalability, the software can be gradually adapted to growing requirements.

macmon NAC — comprehensive network protection for hospitals

- ✓ **Integration of all medical technology** without endangering the existing network or medical devices
- ✓ Enabling **physicians to have flexible access to patient data** in terms of time and location while **protecting against unauthorized access**
- ✓ **Provision** of dedicated and **time-limited Internet access for guests and patients** without having to set up separate WLAN infrastructures for doctors and patients
- ✓ **Ensuring the integrity of the network** by granting network access only to selected (internal and approved) devices
- ✓ **Monitoring and control of all devices** in the network (live inventory management) and documentation of all access to the hospital network
- ✓ **Support with certification in accordance with ISO 27001**, the implementation of the BSI standards for information security management, the IT baseline protection catalogs and hospital certification procedures (e.g. KTQ certification or DIN EN 80001)

Take a look at the use cases in the webinar.
This webinar is in German.
Turn on the English subtitles.
https://youtu.be/mKybXNITOqw

SUMMARY by Jan Schmitt:

“macmon NAC runs reliably in the background. I only need to access the web interface to activate MAC-addresses or to remove a device from the network. The implementation was smooth and quick. The OVA template was used and integrated into the virtual environment, the IP address was assigned and the switches were added. After a two-week test phase, we assigned the MAC addresses to the individual groups and were able to start live operation. Updates are easy to download from the macmon service portal.“ In summary, concludes Schmitt : ”macmon functions exactly as we had hoped.“

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