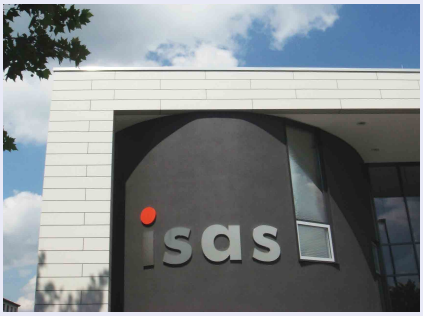
CASE STUDY ISAS

macmon
nac smartly simple

ISAS takes precautionary measures: macmon for effective protection of research and management data

The Leibniz-Institut für Analytische Wissenschaften (ISAS) not only safeguards its critical data reliably using macmon but it's also well equipped for the security requirements of the future.

The Leibniz-Institut für Analytische Wissenschaften e.V. (ISAS) is an independent research institute for physical and chemical analysis with focus on bio-analysis, material analysis and spectroscopy. Between 170 to 200 employees are constantly employed at the three locations of ISAS in Dortmund (two) and Berlin (one). 500 work-stations or lab computers, 1,100 ports, 90 servers, 60 switches, 30 printers and 80 network-compatible measuring devices are being used.



Leibniz Institute for Analytical Sciences (ISAS), Dortmund, TU campus

One VLAN management for several locations

Because of the heterogeneity of its systems and distributed responsibilities, the networks at the institute are exposed to a very high risk of spying of vulnerable research and management data. One of the most important IT security requirements in ISAS is to protect this data in the different networks at different locations using common rules. The need for having a reliable and secure access to the specific network resources of the various departments and research projects in the different locations, was the reason for procuring a NAC solution that provides a simple VLAN management and a secure network access protection. "Colleagues who visit us from other locations of the institute should be able to access their resources immediately. We wanted a dynamic VLAN connection using predefined device parameters. Irrespective of the location, the assignment responses have to be proper", says Jens Hinrichs, the Head of IT Service at ISAS.

The IT security software, macmon' from macmon secure GmbH (earlier mikado soft) enables such security structures to be implemented and made available and provides flexible access control to the network resources. In addition, visitor and quarantine networks can be provided for assigning the devices that are not trustworthy. Static and dynamic VLANs can be easily implemented and operated.

Implementing security policies for all the devices

"macmon provides us with a manufacturer-independent device support at the switch and terminal device-end and the option of even including devices on which NAC client software cannot be installed, like for example mass spectrometers, digital analyzers or oscilloscopes. We were using a client-based NAC solution earlier. Since we use many devices where a client could not be installed, they had to be managed as exceptions with a lot of effort. Manually blocking the ports in case security-critical devices were accessed, involved a lot of effort previously. Using macmon, we can implement security policies on every device in the network without much administrative effort and get our entire network checked by the macmon appliance."

Jens Hinrichs, Head of IT service, ,
Leibniz-Institut für Analytische Wissenschaft

"macmon supports us in optimizing our network and helps us in meeting the increased security requirements through a transparent and easy-to-manage system even in the future"

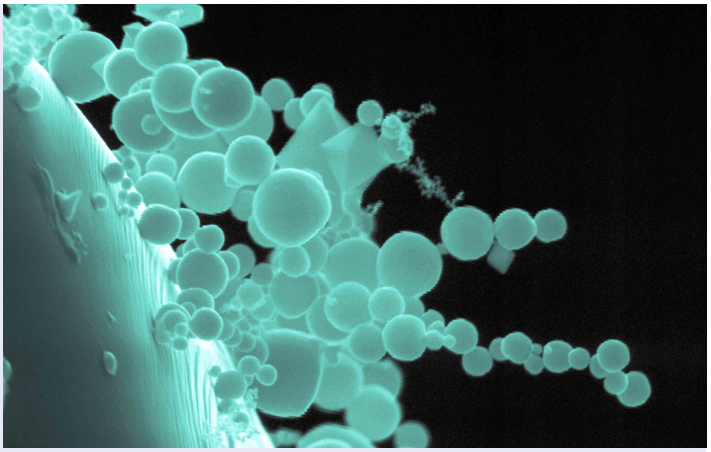
Modular concept for gradual expansion of the security level up to guest management for mobile devices

With the modular concept, macmon provides ISAS the option of increasing the security in the individual networks if required considering the growing demand for IT security and data security in the future. Thus, a WLAN management will be implemented in 2012 for effective access protection to the institute's internal WLAN, even for guest mobile terminal devices. A common WLAN policy for all the locations will be implemented using macmon. "We also have a lot of students at the Institute. A WLAN access using a common password is not sufficient here. This is the reason that we are so excited by the temporary ticket solution and guest management using macmon", says Hinrichs.

The macmon guest service meets all the requirements in this regard. The management and reporting system provides a controlled and time-based network access even for visitors with devices like smart phones, net books or iPads. This is especially important for mobile devices that are prone to specific security risks. The network access

Part of the device landscape at the Leibniz-Institut für Analytische Wissenschaften in Dort-mund: Mass spectrometer and digital analyzers

rights are managed using a voucher system. The administrator can define the networks and the duration of access granted to the guest. The macmon 802.1X option also provides a 802.1X authentication, either using a certificate or a registration, which is especially recommended for the WLAN area since MAC addresses do not provide adequate protection here.



Being used at ISAS: Electron microscopes (photo of filament remains, source)

In addition, the forthcoming BSI certification of macmon was also a factor that influenced ISAS in deciding for macmon. Jens Hinrichs says: "With macmon we are using a component that is verified according to leading international standards, whose security we do not have to evaluate by ourselves. Even our data security officer welcomed the use of macmon because this tool is already supporting us in the implementation of the BSI basic security with uniform documentation of the IT device landscape, as stipulated by the BSI under Measure M 2.10, and the introduction of unauthorized and unsecure devices into the network is effectively prevented (Measure M 2.216)."

Easy to implement and excellent usability

"The implementation after the previous test phase lasted just 2 days and was very easy. We first allowed macmon to detect all the network devices being used. Subsequently we could start using the system without much restrictions on users. What was satisfying here was the very high level of user-friendliness of macmon. The solution is so self-explanatory that users can immediately start working with the software without any training. The acceptance level for the new NAC solution is very high, the staff can now relocate even across locations along with their devices and can automatically find their correct VLAN, without the IT department having to intervene much."

Contact

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