



LAN Device Security Manager



Photo: www.fotolia.

**Rely on a
secure network!**

We are happy to advise you!

Infoline

+43 720 505 765

office@hs2n.at

<http://hs2n.at>

**Features and benefits of
hs²n LAN Device Security
Manager:**

- › fast detecting of compromised PCs
- › system always up to date
- › dynamic VLAN assignment
- › quarantine network
- › manufacturer independent
- › user friendly solution for updates
- › standalone or fully integrated in XEOX

Why use LAN Device Security Manager?

In the past years security attacks steadily increased. New and high sophisticated kinds of viruses and worms find ways to infect PCs and servers despite common security measures (firewall and antivirus software). The main reason for this problem is that the malware gets introduced on your network behind the firewall by an unsecured computer or memory stick. Usually there are hardly any security measures against internal attacks. The virus spreads through the corporate network rapidly. This might result in an downtime of the entire IT for days, the production is stopped. High costs for virus removal and repair of the network are to bear, and even higher costs by the loss of production and damage to your public image.

LAN Device Security Manager protects your system from the insider threat by detecting potential unsecure devices quickly and reliably. Only if their security posture is up to date they are permitted onto the corporate network.

How does LAN Device Security Manager work?

The hs²ⁿ security solution has proven itself especially in two cases:

- › you want to deny external people the access to the internal network.
- › an employee was on an extended business trip or a field representative is in the office again after a long absence.

External and unpatched internal devices can be sources of security vulnerabilities and threaten the entire system. A fast and reliable detection of compromised PCs and notebooks is essential for the security of the IT. LAN Device Security Manager solves this problem:

The core of the system is the central database (CMDB) in which all the information is stored. There all network devices are assigned to VLANs. A high available RADIUS database is synchronized with the central CMDB. The switch through which a device gets access to the corporate network, asks the RADIUS database to which VLAN the device belongs to. If the requesting device is not registered, it will be forwarded in a separate

guest VLAN which is for example directly connected to the Internet. In case of an authenticated device, before permitting a network connection the security posture and health of this client is evaluated:

- › Is the operating system up to date? (via WSUS)
- › Does it have an up to date operational antivirus software?
- › Are viruses, worms or Trojans discovered? (VirusScan)

Clients that fail this series of checks are sequestered in the quarantine subnet, the routing is again automatically with dynamic VLAN. The administrator gets alerted and receives a list of suspicious PCs. An agent on the client recognizes that the PC is now in the quarantine network and forces the automatic update function of Windows. Additionally the antivirus software is updated to the latest version. After updating the client is forwarded to the regular corporate network after just one reboot.

Technical details

A flat network is more vulnerable and makes it easier for a virus to spread across the entire network. For a secure IT it is advisable to structure the network hierarchically by forming smaller broadcast domains (subnets). The assignment of devices to these VLANs is done dynamically with RADIUS. In the central database all network items (desktop PCs, notebooks, printers, etc.) are mapped to a VLAN. The CMDB fills and synchronizes the separate RADIUS database. Since the RADIUS server is Linux-based

it is less vulnerable for viruses and therefore makes the security solution more failsafe. Using more than one RADIUS server increases the reliability and guarantees a high availability.

Regarding the network, just dot1x-capable switches are required, independent of which manufacturer. hs²ⁿ LAN Device Security Manager is high scalable, if the existing IT infrastructure gets expanded or changed the security solution does not require more equipment than before.

XEOX

Benefits of LAN Device Security Manager in combination with XEOX

The hs²ⁿ LAN Security Device Manager was developed as a separate and independent security solution. But it can be used also as an extension to XEOX - a tool by hs²ⁿ to manage the entire IT-infrastructure of a company. XEOX fulfills ITIL guidelines: all IT items (clients as well as peripheral devices and network items) are stored and mapped in the central Configuration Management Database (CMDB). The hs²ⁿ security solution uses the CMDB of XEOX and is integrated

in the system management software. In the CMDB not only clients as PCs and notebooks are assigned to VLAN groups, but also, for example, printers or servers. The CMDB and the separate RADIUS database are synchronous at any time. This guarantees a secure corporate network to which only those devices which are permitted and up to date are allowed to connect.

More information about XEOX on: <http://xeox.com>



hs²ⁿ
Informationstechnologie GmbH
Infoline: +43 720 505 765
<http://hs2n.at>

Willroiderstrasse 3
A-9500 Villach
Austria

Schelleingasse 8/3
A-1040 Vienna
Austria