



# LAN Device Security Manager



Foto: www.fotolia

**Vertrauen Sie auf ein  
abgesichertes Netzwerk!**

**hs<sup>2</sup>n LAN Device Security  
Manager bringt Ihnen Vorteile:**

- › schnelles Erkennen gefährdeter PCs
- › System stets auf dem aktuellsten Stand
- › dynamische VLAN-Zuweisung
- › Quarantäne-Netzwerk
- › keine Herstellerbindung
- › userfreundliche Update-Lösung
- › volle Integration in XEOX

**Wir beraten Sie gerne!**

**Infoline**

+43 720 505 765

office@hs2n.at

<http://hs2n.at>

# Warum LAN Device Security Manager verwenden?

Security Attacken häufen sich, neuartige und hochentwickelte Viren und Würmer können trotz gängiger Schutzmechanismen (Firewall und Viruscheck) PCs und Server befallen. Denn die neuen Viren werden hinter der Firewall durch betriebsfremde, ungesicherte Notebooks oder Memory Sticks in das System eingeschleust. Im internen Netz bestehen kaum Sicherheitsvorkehrungen, der Virus verbreitet sich schnell im gesamten Unternehmen aus. Ein tagelanger Ausfall der IT kann die Folge sein, die Produktion liegt still. Es entstehen hohe Kosten für die Virenentfernung und die Reparatur des Netzwerks, und noch weit höhere durch den Produktionsausfall und Imageschäden.

Der LAN Device Security Manager schützt das System vor Angriffen von innen, indem er schnell und zuverlässig gefährdete Geräte erkennt und diese erst in das Netzwerk zulässt, wenn die Sicherheitsmängel behoben sind.

## Wie funktioniert dieses Sicherheitssystem?

Die hs<sup>2n</sup> Security Lösung bewährt sich insbesondere in zwei Fällen:

- Sie möchten betriebsfremden Personen den Zugriff auf das interne Netzwerk verwehren.
- Einer Ihrer Mitarbeiter war auf längerer Geschäftsreise oder ein Außendienstmitarbeiter ist nach längerer Abwesenheit wieder im Büro. Externe und ungepatchte interne Geräte können Sicherheitslücken aufweisen und das gesamte System bedrohen. Ein schnelles und zuverlässiges Erkennen von gefährdeten PCs und Notebooks ist essentiell für die Sicherheit der IT. Es wurde folgendermaßen gelöst:

Das Kernstück des Systems ist die zentrale Datenbank (CMDB) in der sämtliche Informationen gespeichert werden. Dort werden Netzwerkgeräte VLANs zugeordnet. Eine hochverfügbare RADIUS-Datenbank wird mit der zentralen CMDB synchronisiert. Der Switch, über den das angeschlossene Gerät Zugang zum Unternehmensnetz erhalten will, fragt bei der RADIUS-Datenbank nach, welchem VLAN dieses Gerät zugewiesen werden soll. Stellt sich heraus, dass das Gerät nicht registriert ist, wird es automatisch

in ein eigenes Gäste-VLAN verschoben, das zum Beispiel direkt mit dem Internet verbunden ist.

Ist das Gerät bekannt, wird vor einer Netzwerkverbindung überprüft, ob es folgende Security Standards erfüllt:

- Ist das Betriebssystem auf dem aktuellsten Stand? (über WSUS)
  - Ist der Virens Scanner aktuell?
  - Sind Viren, Würmer oder Trojaner entdeckt worden? (Virens Scan)
- Besteht der PC diesen Test nicht, wird er in ein Quarantäne-Netzwerk verschoben, die VLAN-Zuweisung erfolgt wiederum dynamisch. Der Administrator erhält eine Alarmmeldung und eine Liste der fragwürdigen PCs. Ein Agent auf dem Client erkennt, dass er sich jetzt im Quarantäne-Netzwerk befindet und forciert die automatische Updatefunktion von Windows. Zusätzlich zum Betriebssystem wird der Virens Scanner auf die neueste Version gebracht. Ist der PC wieder auf dem aktuellen Stand, reicht ein Neustart und das Gerät gelangt sicher ins reguläre Netzwerk.

## Technische Details

Je flacher ein Netzwerk aufgebaut ist, desto einfacher können sich Viren verbreiten. Als Basis für eine sichere IT empfiehlt es sich das Netzwerk zu hierarchisieren, indem kleinere Broadcastdomains (Subnetze) gebildet werden. Die Zuweisung zu diesen VLANs erfolgt dynamisch über RADIUS. Dafür werden in der zentralen Datenbank die Netzwerkgeräte (Desktop-PCs, Notebooks, Drucker, etc.) VLANs zugeordnet. Die CMDB befüllt und synchronisiert die separate RADIUS-Datenbank. Die Verwendung eines

oder mehrerer auf Linux basierenden RADIUS-Server macht diese Security Lösung ausfallsicherer und für Viren unangreifbar. Durch mehrere synchrone RADIUS-Server kann die Zuverlässigkeit erhöht und Hochverfügbarkeit garantiert werden.

Für das Netzwerk sind dot1x-fähige Switch erforderlich, man ist jedoch nicht an einen bestimmten Hersteller gebunden. Bei Erweiterungen oder Umstellungen in der Infrastruktur ist für die Security Lösung kein Hardwaretausch notwendig.

# XEOX

## Vorteile von LAN Device Security Manager in Kombination mit XEOX

Der hs<sup>2n</sup> LAN Device Security Manager wurde als eigenständige und unabhängige Security Lösung entwickelt. Er kann allerdings auch als Erweiterung zu XEOX verwendet werden - ein von hs<sup>2n</sup> entwickeltes Tool mit dem die gesamte IT-Infrastruktur verwaltet werden kann. XEOX erfüllt ITIL Richtlinien: in der zentralen Configuration Management Database (CMDB) werden sämtlich Endgeräte (neben PCs und Notebooks auch Peripheriegeräte oder Netzwerkkomponenten) erfasst und in Verbindung gesetzt.

Die hs<sup>2n</sup> Security Lösung verwendet die CMDB von XEOX und ist optimal in das System Management integriert. Es können nicht nur Computer VLAN-Klassen zugeordnet werden, sondern beispielsweise auch Drucker oder Server. Die CMDB und die externe RADIUS-Datenbank stimmen jederzeit überein. Das garantiert ein sicheres Firmennetz, zu dem nur jene Geräte Netzzugriff erhalten, die gewollt und up-to-date sind.

Mehr Information über XEOX finden Sie auf: <http://xeox.com>



hs<sup>2n</sup>  
Informationstechnologie GmbH  
Infoline: +43 720 505 765  
<http://hs2n.at>

Willroiderstrasse 3  
A-9500 Villach  
Österreich

Schelleingasse 8/3  
A-1040 Wien  
Österreich