

### NAC-Lösung macmon überwacht lokale Netze von HARTING

Mit der Einführung einer automatisierten Netzwerk-Zugangskontrolle – NAC – hat der Weltmarktführer für Industriesteckverbindungen den vollen Überblick über nahezu 3.000 Endgeräte gewonnen.

Die Zugangskontrolle überwacht die fünf Netzwerksegmente am Stammsitz in Espelkamp und darüber hinaus auch fünf Auslandsnetze. Besonderes Augenmerk gilt den vielen mobilen Systemen. Ihre Bewegungen waren bisher nur vage oder gar nicht nachvollziehbar. Nun kann sich der Administrator auf die Minute genau anzeigen lassen, welches Gerät sich aktuell wo befindet, und vor allem, ob es sich um ein autorisiertes oder ein Fremdsystem handelt. Letzterem wird durch automatische Sperrung des Ports jeder Zugang zum Netz verwehrt.

### Im Fokus: Schutz der Produktions- und Fertigungsnetze zur Verhinderung von Produktionsausfällen

Die Ausgangssituation bei HARTING gleicht der in vielen Unternehmen. Mangels Zugangsschutz besteht das allgegenwärtige Risiko, dass Angriffe auf die lokalen Netze die Verwaltung und ganze Produktionslinien jederzeit lahmlegen können. Neben internen Servicemitarbeitern, die sich zur Wartung an unterschiedlichen Stellen in die Netze bei HARTING einklinken, sind externe Dienstleister wie Konstrukteure, Service-Techniker und Inbetriebnehmer mit ihren Notebooks in den Fertigungsnetzen aktiv. „Die Fremdsysteme stellen gerade für Produktionsrechner mit häufig älteren Betriebssystemgenerationen, die keine Sicherheitspatches erlauben, eine ständige Gefahrenquelle dar, Viren und Würmer einzufangen“, beschreibt Jens Wandelt die Sicherheitslücke in den lokalen Netzen.

Der Systemadministrator bei der HARTING Technologiegruppe in Espelkamp war darum schon seit längerem auf der Suche nach einem System, „mit dem sich die internen Zugänge zum Netz einfach absichern lassen“, als er durch einen Artikel in einer IT-Fachzeitschrift auf macmon stieß. Angesichts der heterogenen Netzwerkinfrastruktur schieden herstellerspezifische NAC-Systeme aus. Auch der IEEE 802.1X-Standard stellte für Wandelt keine umsetzbare Lösung dar, weil er nicht für alle Endgerädetypen einsetzbar und darüber hinaus sehr komplex in der Anwendung ist. „Das Prinzip von macmon, die Endgeräte über die MAC-Adresse zu identifizieren, versprach eine universell einsetzbare, unkomplizierte Lösung zu sein“, erinnert sich Wandelt. Er nahm Kontakt zum Hersteller macmon secure (zuvor mikado soft) GmbH auf. Danach ging alles Schlag auf Schlag. Von der Präsentation bis zum Echteinsatz verging nur ein halbes Jahr.



HARTING Hauptgebäude, Espelkamp

### Verblüffend einfache Einführung

macmon wurde im Stammwerk Espelkamp zentral auf einem Windows Server mit dem Microsoft SQL Server als Datenbank installiert. An die Implementierung und Inbetriebnahme erinnert sich Wandelt heute noch gern: „Mit der Unterstützung eines Spezialisten von macmon secure vor Ort konnten Installation und Schulung an nur einem Tag absolviert werden.“

Verteilt über fünf Werksbereiche galt es zunächst, etwa 60 Switches mit über 1.200 Endgeräten zu überwachen, von PCs über iPhones, Scanner und Drucker bis hin zu Fertigungsrobotern und Maschinensteuerungen. Bei der Installation konnten die abzufragenden Switches direkt aus einer bereitgestellten Excel-Datei importiert werden. Auch für den Aufbau der Referenzliste konnte ein wesentlicher Teil aus vorhandenen Datenbeständen übernommen werden.

„Natürlich wurden von macmon in der Anfangsphase, der sogenannten Monitoring-Zeit, noch eine Reihe unbekannter Geräte im Netzwerk gefunden, die nicht in den Bestandslisten gepflegt waren. Da Standort und Geräte name nun bekannt waren, konnten diese Informationen auch im NAC-System schnell nachgepflegt werden“, berichtet Wandelt über die Erfahrungen nach der Inbetriebnahme. Die Einordnung der Messgeräte gestaltete sich etwas aufwändiger, da für diese Systeme keine

DNS-Namen vergeben worden sind. Für eine zweifelsfreie Identifikation des Gerätes half hier letztendlich nur, das Gerät im Werksgelände aufzusuchen. „Nach zwei Wochen waren die Vorbereitungsarbeiten abgeschlossen und seither läuft das System zuverlässig und verursacht kaum Administrations- und Wartungsaufwand“, freut sich der IT-Profi. Auch ein zwischenzeitlicher Wechsel der Netzwerkkomponenten von Cisco und 3Com nach HP sei ohne Schwierigkeit bewältigt worden.

## Gewollter Automatismus

Die Switches, die mit ihren DNS-Namen in macmon hinterlegt sind, werden in einem Zeitintervall von zwei Minuten abgefragt. Erkennt das System, dass an einem Anschluss eine unzulässige MAC-Adresse auftaucht, wird der betreffende Port sofort gesperrt. Parallel geht eine Meldung per E-Mail direkt an das Helpdesk-System. Nach einer Sperrzeit von 15 Minuten wird der Port automatisch wieder freigegeben. Ist der unerwünschte Teilnehmer immer noch da, wird der Anschluss wieder geblockt. Im anderen Fall kann der Anschluss sofort wieder von einem zugelassenen Gerät benutzt werden. „Es muss also niemand eingreifen“, erläutert Wandelt den Vorteil der bewusst so gewählten Ereignissteuerung. Einen weiteren Vorteil von macmon sieht er darin, „dass es sich um ein passives System handelt“. Fällt die Überwachung aus, ist keine andere Anwendung davon betroffen. „Im Unterschied dazu besteht bei anderen NAC-Konzepten, die z. B. auf der Basis von 802.1X funktionieren, die Gefahr, dass beim Ausfall des Autorisierungssystems - z. B. des Radius-Servers – das gesamte Netzwerk beeinträchtigt wird, da kein Gerät mehr angeschlossen werden kann“, erläutert Wandelt.

Neue Endgeräte werden vom Desktop-Service der IT-Abteilung einfach über einen dort eingerichteten Lern-Port autorisiert, ohne die macmon-Oberfläche zu benutzen. Wenn das nicht möglich ist, meldet der Fachbereich die relevanten Daten vor der Inbetriebnahme an die IT-Abteilung, die diese manuell in das System eingibt. Mit macmon werden auch die Standorte der Geräte gepflegt.

Diese Daten haben eine sehr gute Qualität, da macmon Umzüge sofort erkennt und dann eine fällige Anpassung der Standortdokumentation anmahnt.

Neue Endgeräte werden vom Desktop-Service der IT-Abteilung einfach über einen dort eingerichteten Lern-Port autorisiert, ohne die macmon-Oberfläche zu benutzen. Wenn das nicht möglich ist, meldet der Fachbereich die relevanten Daten vor der Inbetriebnahme an die IT-Abteilung, die diese manuell in das System eingibt. Mit macmon werden auch die Standorte der Geräte gepflegt. Diese Daten haben eine sehr gute Qualität, da macmon Umzüge sofort erkennt und dann eine fällige Anpassung der Standortdokumentation anmahnt.



HARTING Fertigung

## Internationaler Einsatz von macmon

Nach den guten Erfahrungen mit macmon im Stammwerk Espelkamp startete alsbald das Rollout auf ausländische Tochtergesellschaften. Das internationale Netzwerk der HARTING Technologiegruppe umfasst über 30 Standorte weltweit, wobei die Netzwerksegmente über VPN miteinander verbunden sind. Fünf lokale Auslandsnetze stehen bereits unter dem Schutz der in Espelkamp installierten NAC-Appliance. Für die Aufnahme neuer Geräte stehen zum Teil auch dort Lern-Ports zur Verfügung. Andernfalls werden diese von der zentralen IT-Abteilung in Espelkamp freigeschaltet. Inzwischen ist die Anzahl der vom zentralen Server überwachten Geräte auf 3.000 angestiegen.

Die Zufriedenheit ist groß:

Für Wandelt ist „macmon ein schnell einzuführendes, effizientes und bedienungsarmes Tool“. Der reibungslose Einsatz bei den Tochtergesellschaften bestätigte diese immer wieder von Neuem.

Jens Wandelt,  
Systemadministrator

*„macmon ein schnell einzuführendes, effizientes und bedienungsarmes Tool für unser Stammwerk Espelkamp und unsere ausländischen Tochtergesellschaften an über 30 Standorten weltweit.“*

## Ausblick

Bislang ist macmon aus Gründen der Zugriffsregelung - zwar zentral - aber für jede Auslandstochter separat installiert. „Mit der in Kürze verfügbaren Mandantenfähigkeit braucht macmon nur einmal installiert zu sein“, beschreibt Wandelt eine Erweiterung, welche die standortübergreifende Administration der Anwendung vereinfacht.

## Die HARTING Technologiegruppe

Die HARTING Technologiegruppe entwickelt mit ihren Kompetenzen in den Bereichen elektrische, elektronische und optische Verbindungs-, Übertragungs- und Netzwerktechnik, Fertigung, Mechatronik und Software-Erstellung, maßgeschneiderte Lösungen und Produkte wie Steckverbinder für die Energie- und Datenübertragung, beispielsweise im Maschinenbau, der Bahntechnik, für Windenergieanlagen, die Fabrikautomation und den Telekommunikationssektor. Außerdem produziert HARTING elektromagnetische Komponenten für die Automobilindustrie und ist Spezialist für industrielle Anwendungen in Form von Gehäusen, Verkabelungen oder Konfektionen von Einzel- oder Komplettsystemen sowie automatisierten Verkaufssystemen. Weltweit beschäftigt HARTING mehr als 3.200 Mitarbeiter. Der Umsatz betrug im Geschäftsjahr 2007/08 (Stichtag 30.09.2008) 385 Mio. Euro.

## Kontakt

macmon secure GmbH  
Alte Jakobstraße 79-80 | 10179 Berlin  
Tel.: +49 30 2325777-0 | [nac@macmon.eu](mailto:nac@macmon.eu) | [www.macmon.eu](http://www.macmon.eu)