Kasseler Sparkasse

Rundum lückenlos sicher

Die Kasseler Sparkasse optimierte ihr Netzwerkmanagement durch den ARP-GUARD der Hagener ISL GmbH. Fazit: Mehr Komfort, ein deutliches Plus an Flexibilität trotz bestehendem BVSN-Vertrag und das gute Gefühl zukunftsorientierter und undurchlässiger Sicherheit.

Die Kasseler Sparkasse ist mit einer Bilanzsumme von fast 5 Milliarden die drittgrößte Sparkasse in Hessen und mit ca. 1.100 Mitarbeiterinnen und Mitarbeitern einer der großen Arbeitgeber in der Region. In insgesamt 90 Lokationen werden fast 5.000 Netzwerkendgeräte (Server, Notebooks, Drucker, VoIP-Telefone etc.) betrieben. Die Netzwerkadministration und die damit verbundene Netzwerksicherheit der Kasseler Sparkasse wird, wie bei vielen Sparkassen üblich, durch ein Verbandsrechenzentrum im Rahmen von BVSN (Betriebsverantwortung Sekundärnetz) gewährleistet. Die vorhandenen Maßnahmen zur Netzwerksicherheit wurden von der Kasseler Sparkasse um eine Port-Security Lösung mit Cisco „Bordmitteln“ ergänzt. Bei dieser Lösung wurden die autorisierten Geräte manuell in die Port-Security-Liste der Netzwerkswitche eingetragen.

Kasseler Sparkasse

Hoher Administrationsaufwand bei geringer Flexibilität

Die Methode, bestimmte Geräte zur Gewährleistung der Netzwerksicherheit manuell in eine Port-Security-Liste einzutragen, war aber sehr pflegeaufwendig und mobile Arbeitsplätze, die sich an unterschiedlichen Stellen im Netzwerk anmelden müssen, waren besonders aufwendig in der Administration. Für die Kasseler Sparkasse war dies ein Hauptgrund, sich auf die Suche nach einer neuen Lösung für den Netzwerkschutz zu begeben. Diese Lösung musste auch den besonderen Sicherheitsanforderungen im Selbstbedienungsbereich genügen.

Suche nach Alternativen

Zuerst dachte die Sparkasse an die Implementierung einer 802.1X Lösung. 802.1X ist ein standardisiertes Protokoll, über das jedes Endgerät mit dem jeweiligen Switch kommuniziert und so die Authentifizierung für das Netzwerk erhält. Hierfür benötigen Unternehmen jedoch eine der jüngsten Generationen an Switchen und Endgeräten. Außerdem war eine solche Lösung unter den Vorgaben des Rechenzentrums nur schwer im Eigenbetrieb umsetzbar.

Eine andere Möglichkeit wäre es gewesen, RADIUS (Remote Authentication Dial-In User Service) in der Sparkasse zum Einsatz zu bringen. Auch der alternative Einsatz einer RADIUS basierten Lösung scheiterte an den BVSN-Rahmenbedingungen des Verbandsrechenzentrums.
Fazit: Beide Methoden erschienen ungeeignet.

Voraussetzung für ein für die Sparkasse geeignetes Produkt war es also, dass die Aufwände für die Administration deutlich reduziert werden. Es sollte außerdem eine Sicherheitsstufe erreicht werden, die gleichwertig zu einer 802.1X Lösung ist. Jedoch sollte sich der Investitionsaufwand in einem angemessenen Rahmen halten und keine größeren Veränderungen im internen Netzwerk benötigen, um nicht die Rahmenbedingungen von BVSN zu verletzen.

"Der ARP-GUARD hilft uns unsere Sicherheitsanforderungen ohne hohe Kosten und mit wenig Aufwand in kürzester Zeit umzusetzen."

S. Kulla,
Netzwerk- und Systemspezialist der Kasseler Sparkasse.

ARP GUARD by ISL

SUCCESS STORY

Kasseler Sparkassen

Vollständiger Überblick und Netzwerkkontrolle

Nach intensiver Evaluierung des Marktes hat sich die Kasseler Sparkasse für den ARP-GUARD der Hagener ISL GmbH entschieden. Das Unternehmen hat ein wirksames System zum Aufbau eines aktiven Schutzschildes für das Netzwerk (insbesondere gegen fremde Geräte) entwickelt.

Der ARP-GUARD durchsucht selbsttätig das Netzwerk nach Geräten, indem er mit den darin enthaltenen Routern und Switchen kommuniziert. Administratoren erhalten so schnell einen Überblick über alle angeschlossenen Geräte. Damit schalten sie zwei Nachteile der bisherigen Vorgehensweise aus: Zum einen waren die herkömmlichen Bestandslisten für den Netzwerkschutz meistens schnell veraltet, und zum anderen war die händische Vorgehensweise, bei der das IT-Personal einzelne Geräte an bestimmten Ports zulässt, stets mit einem erheblichen Aufwand verbunden.

„Viele Firmen scheuen eine aufwendige manuelle Netzwerkverwaltung und geben deshalb sämtliche internen Büroports frei, da sie davon ausgehen, dass sich fremde Geräte nur in öffentlich zugänglichen Räumen ins Unternehmensnetz einklinken“, weiß Dr. Andreas Rieke, Geschäftsführer der ISL, zu berichten. „Bei Evaluationen entdecken wir dann immer wieder, dass plötzlich unbekannte Geräte auch an diesen Stellen auftauchen. Das muss nicht jedes Mal unbedingt ein Sicherheitsproblem darstellen, doch so etwas sollte dann Unternehmen grundsätzlich zu denken geben“, so Rieke weiter.

Der Einsatz von ARP-GUARD brachte auch die gewünschte Lösung bezüglich älterer Switchmodelle: Diejenigen Switche, die bereits kompatibel zum Simple Network Management Protocol (SNMP) V3 sind, konnten automatisiert aufgrund des umfangreichen Regelwerkes im ARP-GUARD verwaltet werden, so dass hier ein manuelles Eingreifen von keiner Seite mehr notwendig war. SNMP in der Version 3 hat einen erhöhten Sicherheitsstandard, indem es verschlüsselt kommuniziert und vorher noch eine sichere Authentifizierung mit dem Gesprächspartner realisiert. Um bei Switchen mit der älteren SNMP V2 einen ebenso hohen Sicherheitsstand zu erfüllen, erhielt ARP-GUARD für diese Switche eine andere Policy, so dass bei unbekannten Geräten nur Benachrichtigungs-E-Mails verschickt werden. Der Administrator kann dann situationsbedingt entscheiden, was passieren soll.

Fazit:

Der Einsatz von ARP-GUARD brachte die gewünschte Lösung, da nun lästige und zeitaufwendige Administrationsaufgaben entfallen und sämtliche Geräte zuverlässig erkannt werden - auch in heterogenen Switch-Umgebungen. Mit anderen Worten: Dem Administrator entgeht nun nichts mehr.

„Unser Schutz mit ARP-GUARD lässt sich immer einsetzen, absolut unabhängig von der Hardware-Ausstattung oder von laufenden BVSN-Verträgen. Das ist ein Grund, warum viele Sparkassen unserem Produkt bereits heute vertrauen“, sagt Dr. Andreas Rieke.

Die Kasseler Sparkasse hat mit ARP-GUARD hohe Neuinvestitionen und lange Projektlaufzeiten vermieden, und sogar eine ausgesprochene Optimierung ihres Netzwerkmanagements erfahren. Der Einsatz des Tools ist kostengünstig, Prozesse wurden automatisiert, und das IT-Personal hat stets den Überblick über aktive Geräte. „Der ARP-GUARD hilft uns unsere Sicherheitsanforderungen ohne hohe Kosten und mit wenig Aufwand in kürzester Zeit umzusetzen. Auch eine eventuelle zukünftige vollständige Umsetzung von 802.1X oder RADIUS können wir mit ARP-GUARD realisieren und haben somit einen Investitionsschutz, der uns insbesondere eine fließende Migration ermöglicht“, resümiert S. Kulla, Netzwerk- und Systemspezialist der Kasseler Sparkasse.

ÜBER ARP-GUARD
Die Merkmale:

- Hoher Sicherheitsstandard
- Zu BVSN kompatibel
- Kurze Implementierungsphase
- Support aller SNMP-Versionen
- Flexible Regelgestaltung z. B. anhand unterschiedlicher SNMP-Versionen
- Geringer Administrationsaufwand
- Ideal für heterogene Switch-Umgebungen
- Netzwerkveränderungen nicht nötig
- Investitionsschutz
- Aktuellste Hardwarebestandslisten

ISL Internet Sicherheitslösungen GmbH

ARP-GUARD ist die innovative Lösung, IT-Netzwerke vor internen Angriffen und dem unbemerkten Eindringen nicht autorisierter Geräte zu schützen. Im Jahr 2002 als weltweit erstes Produkt in diesem Bereich von der ISL Internet Sicherheitslösungen GmbH entwickelt, sorgt ARP-GUARD für die interne Sicherheit und schließt eine Sicherheitslücke, die konventionelle Sicherheitssysteme wie Firewall und Intrusion Detection/Prevention nicht abdecken.

Die Sicherheitsexperten der ISL GmbH entwickeln seit der Gründung des Unternehmens 1999 in Hagen IT-Security Lösungen mit dem Schwerpunkt des Network Access Control (NAC) und dem Schutz vor internen Angriffen durch unerwünschte Hardware.

ISL Internet Sicherheitslösungen GmbH

Kasseler Sparkasse

WWW.ARP-GUARD.COM