Audibene GmbH

Mit Meraki konnte die Audibene GmbH ein verlässliches Netzwerk einrichten, das sich zentral steuern lässt: Sicherheitseinstellungen, das Einrichten von VPN und verschiedener SSIDs sowie Fehlerbehebungen sind eine Frage von wenigen Klicks.

- Internationaler Spezialist für den Vertrieb von Hörgeräten
- Installation von Wireless-, Switching- und Security-Lösungen an 13 Standorten
- Nahtloser standortübergreifender Zugriff auf von Ressourcen via Site-to-Site-VPN

Die Hörgeräte-Experten der Audibene GmbH wählen für ihre Kunden hochwertige, für die jeweilige persönliche Situation optimal geeignete Hörgeräte aus. Die Bedürfnisse des Kunden und erstklassiger Service stehen dabei stets im Vordergrund. Neben dem Onlineverkauf von Hörgeräten bringt Audibene seine Kunden auch mit Spezialisten vor Ort zusammen. Zur Vernetzung der Standorte in Europa, Nordamerika und Asien war Rainer Schmitt, Leader of Global IT Operations bei Audibene, auf der Suche nach einer zuverlässigen, einheitlichen Lösung, die mit minimalem Aufwand bereitgestellt und zentral verwaltet werden kann. Dazu war die Technologie von Cisco Meraki ideal geeignet.

Ursprüngliche Herausforderungen an das Netzwerk:

- Kundendaten und interne Ressourcen konnten nicht über alle Standorte hinweg ausgetauscht und gemeinsam genutzt werden.

- Bisheriges Netzwerk bot nur eine lokale, eigenständige Infrastruktur, die nicht übergreifend oder zentralisiert verwaltet werden konnte.

Warum Meraki?

- Über das intuitive Dashboard kann Rainer Schmitt das Netzwerk überwachen und entsprechend der Anforderungen der einzelnen Standorte bedarfsgerecht aktualisieren.

- Unified Threat Management Security Appliances unterstützen präzises Layer-7-Traffic-Shaping, Client-VPN, Firewall-Regeln und Netzwerkoptimierung.

- Globale Einschränkungen stellen sicher, dass kein Standort oder Client zu viel Bandbreite beansprucht oder auf unerwünschte Services zugreift.

- Live-Tools ermöglichen Problembehebung per Fernzugriff und bieten Einblick in potenzielle Probleme, ohne dass Mitarbeiter vor Ort erforderlich sind.

"Wir haben an jeder unserer weltweiten Niederlassungen einen separaten ISP. Ich verschicke einfach die Geräte an die Niederlassung, wo sie dann von einem Mitarbeiter mit dem WAN verbunden werden. Sobald die Geräte online sind, kann ich die Konfiguration und die am jeweiligen Standort benötigten Services überprüfen."

– Rainer Schmitt, Leader of Global IT Operations.

Die Lösung:

- Je nach Größe der 13 Standorte wurden UTM-Geräte (MX80, MX100 oder MX64W), Layer-3-Switches mit 48 Ports und MR32 802.11ac Access Points installiert.

- Ein Mitarbeiter am jeweiligen Standort übernahm die Anbindung der Geräte mit dem WAN. Anschließend konnte Rainer Schmitt alle erforderlichen Aktualisierungen der Konfiguration vornehmen.

- Cisco Meraki vernetzt alle Niederlassungen über ein automatisiertes, vollständig vernetztes Site-to-Site-VPN mit Self-Healing-Funktion.

Die Ergebnisse

- Jedes Netzwerk bietet jetzt mehrere SSIDs. So kann Audibene einfach per Mausklick Gastdatenverkehr vom Unternehmensdatenverkehr isolieren und zudem sichere Authentifizierung implementieren.

- Das IT-Team profitiert darüber hinaus von der Integration einer dynamischen VPN-Verbindung zu MS Azure Cloud Services.

- Durch das Cloud-basierte Management kann Audibene jeden Standort per Fernzugriff verwalten. Vor Ort werden somit keine IT-Mitarbeiter mehr benötigt.

- Unternehmenseigene Geräte, einschließlich Laptops und Smartphones, sowie BYOD- und Gastgeräte können nun problemlos eine Verbindung zum Netzwerk herstellen und bedarfsgerecht auf Ressourcen zugreifen.

- Der Managementaufwand für den Netzwerkadministrator reduzierte sich durch ein zentrales Dashboard mit einheitlicher Kontrolle und Transparenz.

- Die im Lieferumfang der Lizenz enthaltenen automatischen Firmware-Updates und neuen Funktionen sorgen für ein zukunftssicheres Netzwerk und erhebliche Kosteneinsparungen.