ANWENDERBERICHT
UNIVERSA VERSICHERUNGEN

macmon
nac intelligent einfach

Einführung der Network Access Control (NAC)-Lösung macmon bei uniVersa

Die uniVersa Versicherungen sind eine Unternehmensgruppe mit langer Tradition und großer Erfahrung, deren Ursprünge bis zum Jahr 1843, dem Gründungsjahr der uniVersa Krankenversicherung, der ältesten privaten Krankenversicherung Deutschlands, zurückreichen.

Bei der uniVersa legt man Wert auf individuelle Vorsorgelösungen. Deshalb werden keine Produkte von der Stange, sondern individuelle Lösungen zur finanziellen Vorsorge angeboten, bei denen langfristiger Kundennutzen und hohe Servicequalität eindeutig im Vordergrund stehen.

Neben der Kundenzufriedenheit nimmt die Wahrung der unternehmerischen Unabhängigkeit eine zentrale Position in der Firmenphilosophie ein. Im Sinne der Vorsorge und Absicherung hat sich die IT-Abteilung der uniVersa Lebensversicherung a.G. intensiv mit dem Thema der Netzwerk-Zugangskontrolle auseinander gesetzt. Auf Basis der internen Anforderungsbeschreibung des Unternehmens mit einer zentralen Hauptverwaltung, verteilten Standorten sowie einer Außendienststruktur wurden verschiedene Lösungen betrachtet.

Die Anforderungen

Ein wesentlicher Punkt der Anforderungen war die Herstellerunabhängigkeit in Bezug auf die eingesetzten Netzwerkkomponenten (Switche, Router, etc.), damit die zukünftige Lösung auch bei einem Wechsel einzelner Komponenten oder eines kompletten Systems vollständig weiter betrieben werden kann. Dementsprechend wurden vorrangig Produkte betrachtet, die nicht den Einsatz zusätzlicher Netzwerkkomponenten oder gar Kollektoren etc. erfordern. Zusätzlich bestand die Maßgabe, vor allem offene Standards zu unterstützen, um keine Insellösung zu produzieren.

Weiterhin muss die NAC-Lösung unabhängig von den Geräteklassen wie z.B. Drucker, PCs, Kartenleser und weitere Sondergeräte agieren und auch den Betrieb von zwei Geräten an einem Port ermöglichen (z.B. PC und VoIP Telefon). Der Einsatz eines zusätzlichen Agenten sollte gerade aufgrund der vielen verschiedenen Systeme unbedingt vermieden werden.

Um die verteilte Struktur zu berücksichtigen, musste die Lösung alle Vorgaben sowohl für die Hauptverwaltung als auch für alle Geschäftsstellen erfüllen, wobei die notwendige interne Kommunikation der Komponenten untereinander zwingend verschlüsselt erfolgen sollte.

Ein weiterer wesentlicher Punkt war die Anforderung, die zukünftige NAC Lösung auch in einer Art „Mixed-Mode" betreiben zu können – das heißt die Authentifizierung der Endgeräte anhand von MAC-Adressen, Zertifikaten (per 802.1X) oder anderen Methoden zeitgleich zu ermöglichen.

Neben diesen vielen wichtigen Funktionen wurde aber auch der grundsätzliche Betrieb genauer definiert. Dementsprechend sollte das System als Virtueller Server, hochverfügbar und per Web GUI bedienbar sein, während ein trotzdem eintretender Ausfall den Betrieb der uniVersa auf keinen Fall behindern darf. Durch die Nutzung verschiedener Betriebsmodi wie „nur Beobachten",

Stand: 08/2014

„Lernen“, „Simulation“ und „Aktiv“ sollte eine schrittweise Implementierung ermöglicht werden.
Als weitere wichtige Anforderung ist zu erwähnen, dass die Verwaltung von Gastzugriffen und privaten Geräten über ein geeignetes Ticketmanagementsystem möglich und eine sichere Integration für WLAN und drahtgebundene Anschlüsse gegeben sein sollte.

Die Auswahl

Auf Grund des umfangreichen Anforderungskataloges wurden verschiedene Hersteller von NAC-Lösungen angesprochen und je nach Erfüllung des Kataloges zur Vorstellung im Haus uniVersa eingeladen. In diesem Rahmen erfolgte eine Produktvorstellung vor dem Projektteam durch verschiedene Hersteller. Neben der differenzierten Preisgestaltung waren auch die Herangehensweisen und die verwendeten Technologien der Anbieter sehr unterschiedlich. Der deutsche Hersteller macmon secure konnte sich durch das intelligent einfache Konzept und durch die vergleichsweise schnellere Implementierung seiner NAC-Lösung positiv hervorheben.

Innerhalb des Auswahlverfahrens wurden die Funktionen der verschiedenen Lösungen gegeneinander abgewogen. Ziel war es, das getestete Produkt möglichst nach der Testphase direkt in den unternehmensweiten Produktivbetrieb übernehmen zu können. Auf Basis der vorhandenen Erkenntnisse, des fundierten Ausblicks auf weitere Entwicklungen und unter Einbezug der Erfahrungen aus Referenzinstallationen fiel die Wahl letztendlich auf macmon als Favorit.

Der Proof of Concept

Seitens macmon wurde ein Zeitrahmen von 2 Tagen für den PoC veranschlagt. Über eine virtuelle Appliance waren die Inbetriebnahme sowie die Aufnahme des Netzwerkes innerhalb kurzer Zeit erledigt. Die Konfiguration von macmon wurde bereits am ersten Tag soweit gebracht, dass eine Produktivsetzung des Systems möglich gewesen wäre. Lediglich die im Netzwerk erkannten Endgeräte mussten noch kategorisiert und die Konfiguration von wenigen nicht automatisch erkannten Uplink-Ports überprüft werden.

Die Konfiguration von MAC-Authentication-Bypass auf den Switches sowie der Test des Gäste-Portals unter Verwendung von MAB im WLAN-Bereich konnten ebenfalls erfolgreich durchgeführt werden. Zur Freude des uniVersa Projektteams war die

„Der geringere Implementierungsaufwand im Vergleich zum Wettbewerb hat uns überzeugt.“

Michael Herbig, Projektleiter, uniVersa

Integration des Gästenetzes über WLAN inklusive 802.1x Authentifizierung möglich. Ein in einer speziellen Konfiguration des Remediation-VLANs entdeckter Bug wurde noch am gleichen Tag durch die Entwickler der macmon secure GmbH behoben.

Am Ende des ersten Tages wurde nach diesen Ergebnissen entschieden, dass der zweite geplante Tag vor Ort nicht mehr benötigt wird. Zusätzlich zu den geplanten Schritten konnten bereits erste Tests mit der multiplen compliance von macmon gemacht werden.
Das einfache Handling des macmon-Systems sowie die erfolgreiche Einführung in das System durch den macmon-Consultant in Verbindung mit dem im uniVersa-Projektteam bereits vorhandenen Know-How ermöglichten es, dass alle weiteren Testszenarien durch uniVersa ohne weitere Unterstützung seitens macmon durchlaufen werden konnten. Es erfolgte eine Testphase von ca. vier weiteren Wochen zur Beobachtung des fortlaufenden Betriebs.

Die Umsetzung

Innerhalb der Testphase wurden keine Stolpersteine oder Mängel festgestellt, so dass die Entscheidung für macmon fiel. Das macmon-NAC konnte damit so wie geplant aus dem Testbetrieb in die Produktivumgebung übernommen werden und schützt heute effektiv alle Netzwerkzugänge aller Standorte der uniVersa Versicherungen.

„Wir waren überrascht, dass es möglich ist, Network Access Control innerhalb von 5 Projekttagen effektiv einzuführen.“

Michael Herbig, Projektleiter, uniVersa

Stand: 08/2014

„Die Anbindung unserer bestehenden Systeme zur Richtliniendurchsetzung ist eine tolle Möglichkeit, die wir noch weiter ausbauen werden."

Christian Knauer, Netz- und Kommunikationstechnik, uniVersa

FAZIT:

Als wesentlicher Faktor in der Entscheidungsfindung, der Umsetzung und dem letztendlich erfolgreichen Projektabschluss ist vor allem die intuitive und einfache Verwendung von macmon zu nennen. Die schnelle Reaktion des Teams der macmon secure GmbH auf Anforderungen sowie die unkomplizierte und direkte Abstimmung mit diesem deutschen Hersteller unterstützten den reibungslosen Ablauf. Network Access Control ist damit auch in einer verteilten Umgebung, wie sie sich in der uniVersa abbildet mit unterschiedlichsten Endgeräten erfolgreich und mit relativ geringem Aufwand umsetzbar.

Kontakt macmon secure GmbH | Alte Jakobstraße 79-80 | 10179 Berlin | Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu

Stand: 08/2014