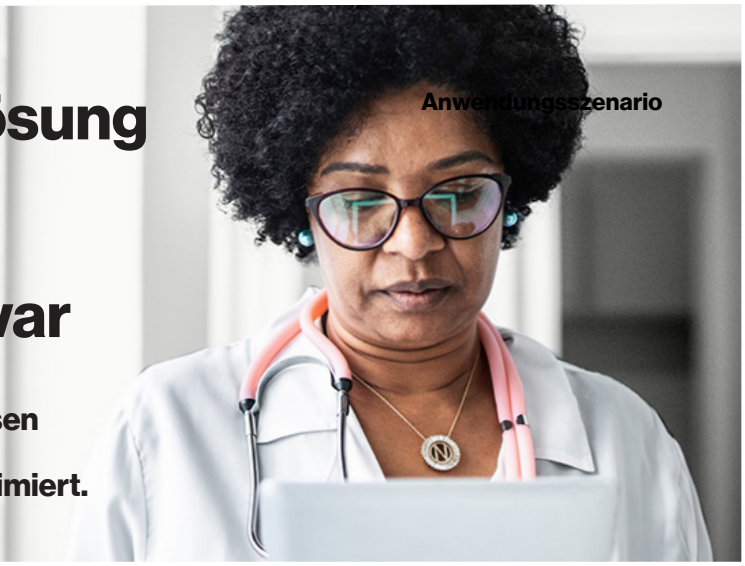
Warum eine SASE-Lösung das richtige Rezept für diese Marke im Gesundheitswesen war



Anwendungsszenario

Ein Großunternehmen im Gesundheitswesen hat seinen Sicherheitsbetrieb mit einer Secure-Access-Service-Edge-Lösung optimiert.

Schutz einer führenden Marke im Gesundheitswesen

Von Unternehmen im Gesundheitswesen wird erwartet, dass sie die Kundenbetreuung verbessern und dabei dafür sorgen, dass vertrauliche Patientendaten zuverlässig geschützt bleiben. Dies stellt eine größere Herausforderung dar, je größer das Unternehmen ist, denn mit jedem neuen Geschäftsbereich wird es schwieriger, unternehmensweit dasselbe hohe Sicherheitsniveau durchzusetzen.

Vor dieser Herausforderung stand auch ein großer, diversifizierter Konzern im Gesundheitswesen, als er sich 2020 an Verizon wandte, weil er einen Partner für die Umsetzung seiner mehrjährigen Cyber-Sicherheitsstrategie benötigte. Das Unternehmen beschäftigt weltweit Zehntausende Mitarbeiter und ist in mehrere Geschäftsbereiche unterteilt, die jeweils eigene Sicherheitsteams, -technologien und -ansätze haben. Im Laufe der Zeit hatte das Unternehmen zahlreiche Sicherheitslösungen implementiert, wodurch viele verschiedene Prozesse genutzt werden mussten, mit diversen Konsequenzen für den Sicherheitsbetrieb. All das beeinträchtigte die Cyber-Resilienz des Unternehmens. Die Unternehmensleitung wollte die Mitarbeitererfahrung verbessern, Technologieinvestitionen optimal ausnutzen und ein hervorragendes Sicherheitsmanagement erreichen.

Dazu war eine neue Methode zur Stärkung der Sicherheit erforderlich, die gleichzeitig die Prozesse und Technologien besser aufeinander abstimmte.

Ein solides Fundament

In Konsultation mit Verizon entschied sich das Unternehmen, die Herausforderung in mehreren Schritten anzugehen, und wählte einen Geschäftsbereich für ein Testprojekt aus. So wollte das Unternehmen den Prozess zur unternehmensweiten Sicherheitsoptimierung besser unter Kontrolle behalten. Wenn sich zusätzliche Sicherheitsfunktionen im Testprojekt bewährten, sollten sie schrittweise in die unternehmensweit genutzte Sicherheitsplattform integriert werden.

Das wichtigste Projektziel war, 30.000 Nutzern in Hunderten von Niederlassungen sicheren Zugriff auf das Internet und auf Geschäftsanwendungen zu bieten. Verizon war als Partner ausgewählt worden, weil es über ein leistungsstarkes globales Netzwerk verfügt und für seine hervorragenden Leistungen beim Design, Aufbau und Management integrierter Netzwerk- und Sicherheitsarchitekturen bekannt ist. Unser beratungsorientierter Ansatz, starkes Partnernetzwerk und die Fähigkeit, Lösungen mehrerer Anbieter miteinander zu verknüpfen, trugen das Ihre zur Auswahl von Verizon bei, denn das Unternehmen benötigte einen Partner mit genug Erfahrung und Sachkenntnis, um gängige Fallstricke zu vermeiden und rasch auf unerwartete Herausforderungen zu reagieren.

Der erste Schritt war eine Bewertung des vorhandenen IT-Ökosystems. Gemeinsam mit den IT- und Sicherheitsteams des Kundenunternehmens trug Verizon die kommerziellen und Technologieanforderungen zusammen, lotete die Leistungsgrenzen vorhandener Funktionen aus und ermittelte, welche Herausforderungen aufgrund der bereits genutzten Technologien bei der Implementierung zu erwarten waren.

Gemeinsame Innovation und Kollaboration

Als nächste Aufgabe stand das Skizzieren einer neuen Lösung an. Die Teammitglieder einigten sich auf Verizon Network-as-a-Service (NaaS) als Basis und Secure Access Service Edge (SASE) zur Bereitstellung sicherer Verbindungen zwischen Nutzern an nahezu jedem Ort der Welt und den Geschäftsanwendungen sowie allen Büros und Fertigungsstätten.

verizon business

Eine zusammenhängende Lösung

Diese Infrastrukturkombination verknüpft Netzwerk- und Sicherheitsfunktionen zu einer eng integrierten Lösung, die es allen Geschäftsbereichen gestattet, hybride Arbeitsmodelle souverän zu nutzen. Inzwischen können die Nutzer in allen 200 Büros und Produktionsstätten des Unternehmens über ihre Mobilgeräte sicher auf das Internet sowie auf die Geschäftsanwendungen und IT-Ressourcen des Unternehmens zugreifen, unabhängig davon, ob diese sich auf physischen oder cloudbasierten Servern befinden.

Das IT-Team nutzt statt zahlreicher Anbieter und deren Lösungen einen Technologiestack und ein Helpdesk. Und da Verizon sicherheitsrelevante Routineaufgaben wie das Einrichten neuer Nutzerkonten und den Transfer von Tickets zwischen den Kunden- und Anbieterplattformen übernommen hat, können die IT- und Sicherheitsteams des Kundenunternehmens sich auf strategisch wichtigere, wertschöpfende Tätigkeiten konzentrieren.

Die einfachere Architektur bietet auch mehr Transparenz und Kontrolle. Dadurch haben die Geschäftsbereiche eine bessere Übersicht über ihre Ressourcennutzung und ihre Ausgaben und die Sicherheits- und IT-Teams konnten Kosten einsparen. Sie haben die Systeme und Tools mit dem besten Preis-Leistungs-Verhältnis behalten und optimiert und so die Rendite der Technologieinvestitionen gesteigert. Überflüssige Technologien wurden ausgemustert.

Doch die vielleicht wichtigste Änderung ist, dass die Geschäftsbereiche nicht mehr eine geteilte Infrastruktur nutzen, wodurch ihre Anfälligkeit für Angriffe reduziert wurde. Darüber hinaus können sie ihre Sicherheitsrichtlinien nun sehr viel besser an die Sicherheitsstrategie der Unternehmensgruppe anpassen.

Ausblick

Da der Sicherheitsbetrieb nun mit Unterstützung durch Verizon optimiert wurde, hat die nächste Phase des Projekts begonnen. Verizon wird maßgeblich an der weiteren Optimierung des Sicherheitsbetriebs und der gesamten Plattform des Kundenunternehmens beteiligt sein. Dazu wird Verizon nach und nach mehr zukunftsweisende Sicherheitsfunktionen implementieren, die ihrerseits die SASE-Lösung einbeziehen werden, um auf einen MDR-Ansatz (einschließlich XDR und EDR) hinzuarbeiten.

Weitere Informationen

Wenn Sie wissen möchten, welche Vorteile eine SASE-Lösung für Sie hätte, wenden Sie sich an Ihren Account Manager oder schauen Sie unter https://www.verizon.com/business/de-de/resources/lp/secure-access-service-edge/ vorbei.

verizon business