Wie SASE in einem Fertigungsunternehmen zur Basis einer sicheren Zukunft wurde

Anwendungsszenario

Durch den Wechsel zu Secure Access Service Edge (SASE) wollten die Entscheidungsträger eines wachsenden Fertigungsunternehmens ihre Sicherheitsinfrastruktur modernisieren, die Betriebstechnologie schützen, die Voraussetzungen für die Digitalisierung und Cloud-Nutzung schaffen – und zudem die Cybersicherheitsvorkehrungen mit einem einheitlichen Framework für die Sicherheitsrichtlinien vereinfachen, ohne die Resilienz oder die Geschäftskontinuität zu gefährden.

Schutz einer aufstrebenden Marke

Geschäftswachstum kann äußerst profitabel sein – bringt aber auch neue Risiken mit sich. Mit Fusionen und Übernahmen kommen neue Systeme, Netzwerke und Prozesse in Unternehmen. Es ist nicht immer leicht, diese in einer Wachstumsphase so in die vorhandene Infrastruktur einzugliedern, dass alles sicher und effizient zusammenarbeitet. Heutzutage kommt erschwerend hinzu, dass Unternehmen ihre Infrastrukturen ununterbrochen vor Cyberangriffen schützen müssen und gleichzeitig deren Nachhaltigkeit verbessern sollen.

In dieser Situation befand sich ein im Vereinigten Königreich ansässiges Fertigungsunternehmen, als es Verizon 2019 kontaktierte. Das Unternehmen nutzte schon seit geraumer Zeit ein Netzwerk von Verizon, doch durch das Geschäftswachstum war die Komplexität der Sicherheitsvorkehrungen und Bedrohungserkennung gestiegen und ihre Verwaltung kompliziert geworden. Einige in den vorangegangenen Monaten und Jahren ausgenutzte Schwachstellen waren nicht vollständig behoben worden und stellten daher weiterhin eine Gefahr dar. Das hatte bereits dazu geführt, dass Angreifer sich Zugang zu Systemen verschaffen konnten. Die resultierenden Ausfälle, Social-Engineering- und Ransomware-Angriffe hatten die Verfügbarkeit und Produktivität an mehreren Standorten beeinträchtigt.

Daraufhin hatte das Unternehmen weltweit Endpunktschutzmaßnahmen und mehr als 140 physische Firewalls implementiert. Das mit dem Sicherheitsmanagement beauftragte Unternehmen war jedoch nicht weltweit aktiv und daher nicht in der Lage, in den mehr als 140 Niederlassungen des Fertigungsunternehmens in aller Welt für eine belastbare, konsistente Sicherheit zu sorgen und diese kontinuierlich zu stärken.

Ransomware-Angriffe bleiben die dominante Angriffsform. Im Jahr 2022 wurde nach 24 % aller Datenschutzverletzungen Ransomware gefunden. [1]

verizon business

Von der Stabilisierung zur Innovation

Nachdem Verizon das Management der Netzwerksicherheitsinfrastruktur des Unternehmens übernommen hatte, musste diese zuerst stabilisiert und standardisiert werden. Dazu mussten etwaige Schwächen in den Sicherheitsregeln identifiziert und adäquate Cyberhygieneprozesse in die gesamte Infrastruktur integriert werden. Nach der Erledigung dieser Aufgaben hatte das Team von Verizon eine bessere Übersicht über die vorhandene Umgebung und konnte das Unternehmen beim Übergang zu einem proaktiveren Sicherheitsansatz unterstützen. Das war auch notwendig, da die physischen Firewalls des Kunden dringend ersetzt werden mussten. Die unternehmensweite Implementierung dieser Firewalls hatte mehr als drei Jahre in Anspruch genommen.

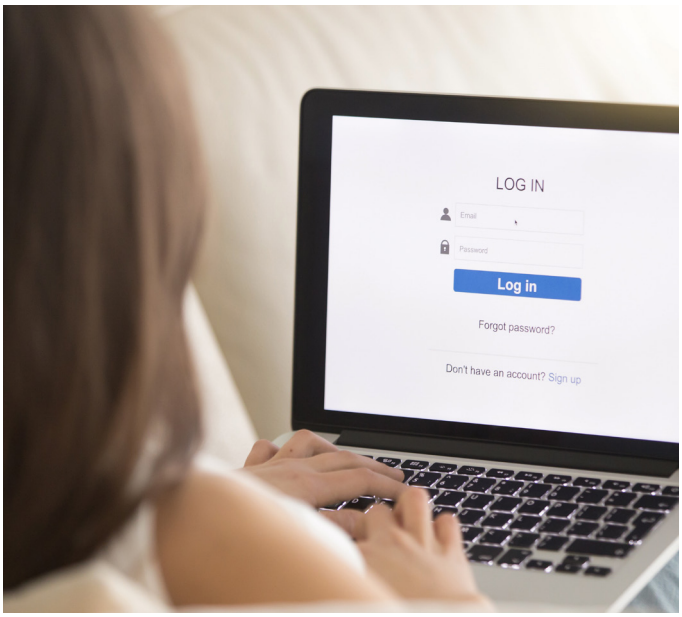
Da das Unternehmen bereits das globale MPLS-Netzwerk von Verizon nutzte, war die Migration zu einer SASE-Umgebung der nächste logische Schritt. SASE vereint Netzwerkzugang, Verkehrsoptimierung und Sicherheitsrichtlinien in einer sicheren, holistischen Lösung. Damit versetzt es Unternehmen in die Lage, Sicherheitsbedrohungen rasch zu erkennen und effektiv abzuwehren, um ihren Nutzern – unabhängig von deren Standort – eine konsistente Netzwerkerfahrung zu bieten. Im hier beschriebenen Fertigungsunternehmen wurde Zero Trust-Netzwerkzugang (ZTNA) implementiert, sodass nichts und niemand ohne Authentifizierung auf das Netzwerk zugreifen konnte. Gleichzeitig konnte das Unternehmen nun cloudbasierte Sicherheitsdienste nutzen und die Anzahl der physischen Firewalls reduzieren.

> **„Mit einem einheitlichen Richtlinienframework konnte Verizon die Sicherheitsvorkehrungen vereinfachen und vereinheitlichen, die Transparenz verbessern und die Anzahl der Sicherheitsvorfälle reduzieren. Dadurch stieg die Resilienz des Geschäftsbetriebs, was die sichere Umsetzung eines nachhaltigen Programms für die Cloud-Nutzung ermöglichte.“**
>
> **Claudio Testa,**
> Security Solutions Executive, Verizon Business

Die Verlagerung von Services in die Cloud vereinfachte nicht nur die Überwachung von Schwachstellen und die Verbesserung der Resilienz, sondern auch die Erfüllung der rasch zunehmenden Forderungen nach hybriden Arbeitsmodellen. Angesichts der Tatsache, dass 74 % der Datenschutzverletzungen[1] ganz oder teilweise auf menschliche Fehler zurückzuführen sind, sollte die Lösung Anmeldedaten unbedingt zuverlässig schützen und auf sämtlichen Geräten, an allen Standorten und in allen Ländern die strengsten Sicherheitsstandards umsetzen.

Ein auf Zusammenarbeit basierter Sicherheitsansatz

In enger Zusammenarbeit mit Mitarbeitern des Fertigungsunternehmens entwickelte und implementierte das Team von Verizon eine holistische Lösung aus Technologie, Beratungsdiensten und Managed Services, die den spezifischen Anforderungen des Kundenunternehmens sowohl kurz- als auch langfristig gerecht wird.



Eine umweltfreundlichere und sicherere Lösung

Diese Lösung entlastete die alternde physische Infrastruktur des Unternehmens, reduzierte die Anzahl der Schwachstellen und verkleinerte die Angriffsfläche, wodurch der Sicherheitsbetrieb vereinfacht und die Sicherheit gestärkt wurden. Die Ergebnisse sprechen für sich. Die Anzahl der Ransomware-Angriffe ging erheblich zurück und die Ausgaben des Unternehmens für die Reaktion auf Cybersicherheitsvorfälle, deren forensische Untersuchung und die anschließende Wiederherstellung und Schadensbehebung sanken im vergangenen Jahr erheblich. Gleichzeitig trug die Partnerschaft mit Verizon zur Verbesserung der Nachhaltigkeit des Kundenunternehmens bei, da die SASE-Lösung weniger Strom verbraucht als eine aus dedizierter Hardware bestehende Umgebung.

Ausblick

Das Fertigungsunternehmen verfügt nun über eine zuverlässige, cloudbasierte Sicherheitsinfrastruktur, die mit Unterstützung durch Verizon von mehreren Standorten rund um den Erdball aus verwaltet werden kann. Das Unternehmen konnte seine Sicherheitslösung modernisieren, die Angriffsfläche reduzieren und die Verfügbarkeit und Resilienz verbessern. Da das Unternehmen – unter anderem durch weitere Fusionen und Übernahmen – nach wie vor wächst, trägt die Flexibilität der SASE-Lösung dazu bei, dass neue Netzwerke und deren Nutzer rasch integriert werden können, während die Sicherheitsinfrastruktur fortlaufend auf dem neuesten Stand gehalten wird und effektiv bleibt.

Weitere Informationen:
SASE-Sicherheitslösungen

[1] Data Breach Investigations Report 2023. Verizon Business. https://www.verizon.com/business/de-de/resources/reports/dbir/

verizon business