„Hallo, hier ist SASE.“ „SASE wer?“

Secure Access Service Edge, kurz SASE, ist eines der aktuellen Schlagwörter in der IT- und Sicherheitsbranche. Doch was ist es – und was bringt es?

Autor: Dheeraj Rawal

SolarWinds, Colonial Pipeline, ... In den letzten Jahren wurde die Welt immer wieder Zeuge schwerwiegender Cyber-Angriffe, die verdeutlichen, wie sich die Bedrohungslage für Unternehmen intensiviert.

Angesichts der verstärkten Bedrohung aus dem Cyberraum stellt sich für Unternehmen die Frage, ob ihre Sicherheitslösungen immer noch ausreichend sind. Denn sicher ist vor allem eins: Unternehmensnetzwerke sind heute verwundbarer denn je. Die zunehmende Vernetzung, vermehrte Fernzugriffe, das Internet of Things und Edge Computing erzeugen mehr Angriffsflächen.

Darüber hinaus hat die Pandemie die meisten User aus den Firmengebäuden vertrieben. Seitdem haben Unternehmen Mitarbeiter, die von überall aus auf Geschäftsanwendungen zugreifen: Von zu Hause, aber manchmal auch von Cafés oder aus Zügen. Dabei benutzen sie gar nicht so selten private IT-Endgeräte. Dadurch werden die Anforderungen an IT-Teams, Daten und Anwendungen zu schützen, ständig höher. Ergänzt werden die steigenden Anforderungen durch eine zunehmende Komplexität in puncto Datensicherheit. Secure Access Service Edge (SASE) verspricht eine Lösung für diese Herausforderungen.

Der Aufstieg von SASE – Wie alles begann

Seit Gartner vor gut drei Jahren 2019 den Begriff SASE prägte, hat sich das Akronym vor allem aus einem Grund rasend schnell zu mehr als nur einem Schlagwort entwickelt: In dem Maße wie Mitarbeiter von verschiedenen Orten auf das Unternehmensnetzwerk und die Unternehmensdaten zugreifen, verlor die auf dem Perimeter basierende Netzwerksicherheit an Bedeutung. Denn herkömmliche Netzwerk-Topologien führen den Datenverkehr durch ein zentrales Rechenzentrum. Dort wird dieser geprüft und dann an den User weitergeleitet.

Warum ist das für Unternehmen wichtig?

Mit SASE, das auf der Cloud basiert, wird dieses so genannte Backhauling umgangen. Der Datenverkehr wird direkt über den nächstgelegenen Präsenzpunkt geleitet. Das entlastet das Rechenzentrum und ist für die User vorteilhaft: Wenn sie auf Geschäftsanwendungen wie Microsoft 365 zugreifen, verbessert sich die User Experience durch bessere Reaktionszeiten.

Diese Rapid Response bedeutet jedoch nicht, dass die Sicherheit beeinträchtigt wird. SASE ermöglicht es Unternehmen, Netzwerk- und Sicherheitsdienste an Endpunkte zu verteilen. Das heißt, unabhängig davon, wo sich der User befindet, sind Dienste wie URL-Filtering, SD-WAN und Secure Web Gateways weiterhin verfügbar. Darüber hinaus sorgen Zero-Trust-Richtlinien dafür, dass der Zugriff auf Daten und Anwendungen kontextabhängig erfolgt.

Was können Unternehmen mit diesem Ansatz gewinnen?

Im Kern geht SASE Latenz- und Sicherheitsprobleme nicht mehr getrennt an: Bei der cloud-basierten Lösung werden Netzwerk- und Security-Services kombiniert. Das steigert die Performance und bringt mehr Sicherheit – davon profitieren Unternehmen doppelt. Zusätzlich reduziert SASE die Komplexität und sorgt für mehr Effizienz, Transparenz und Kontrolle über Sicherheitsarchitekturen.

Die Kombination dieser Vorteile macht SASE zu einer lohnenden Option, die sich bei Unternehmen schneller durchsetzt als erwartet. 2018 lag die Akzeptanz von SASE bei etwa ein Prozent. Bis 2024 sollen laut einer Prognose von Gartner etwa 40 Prozent der Unternehmen Strategien entwickeln, die SASE einbeziehen.

Pandemie und verteilte Belegschaft

Tatsächlich hat die Pandemie das Wachstum von SASE beschleunigt. Da ein Großteil der Belegschaft von zu Hause aus arbeitete, war die Zahl der an die Unternehmensnetze angeschlossenen Geräte um ein Vielfaches gestiegen. Vor dem Ausbruch der Pandemie sahen die IT-Abteilungen eine „verteilte Belegschaft“ als Synonym für über den Globus verteilte Niederlassungen. Doch seit Corona repräsentiert jeder Mitarbeiter, der von zu Hause aus arbeitet, eine Zweigstelle.

SASE geht die Latenz- und Sicherheitsprobleme gemeinsam an, indem es Netz und Sicherheit zusammenführt.

Der Wechsel von traditionellen Netzwerkkonzepten zu SASE ist der erste Schritt zur Umsetzung echter Zero-Trust-basierter Modelle. Perimeter-basierte Netzwerksicherheit wird der verteilten Belegschaft und Cloud-Workloads nicht mehr gerecht.

Thomas Tschersich, Chief Security Officer bei der Deutschen Telekom

Das Chaos der Konnektivität

Mit Beginn der Pandemie arbeiteten mitunter Zehntausende von Mitarbeiter plötzlich von zu Hause aus – statt aus dem Büro. Sie wollten Anwendungen wie Zoom und MS Teams nutzen. Die Überlastung des Netzwerks stellte Unternehmen vor enorme Herausforderungen. SASE half, dieses Problem zu überwinden; Unternehmen, die sich hingegen auf herkömmliche VPNs verließen, mussten erhebliche Schwierigkeiten in Kauf nehmen.

Diese „hyperverteilte“ Belegschaft wird so bald auch nicht mehr verschwinden – im Gegenteil: Das Homeoffice wird zur Norm. Immer mehr Unternehmen führen hybride Arbeitsmodelle ein und bieten ihren Mitarbeitern in manchen Fällen sogar permanente Remote-Work-Optionen.

Mit SASE gewinnen Unternehmen einen besseren Überblick über die Netzleistung und können Sicherheits- sowie Leistungsprobleme leichter diagnostizieren und beheben. Sie müssen keine Leistungseinbußen hinnehmen. Aber nicht nur Netzwerkverantwortliche profitieren von SASE – CISOs erzielen mit SASE ein höheres Maß an Sicherheit.

Milliardenschäden durch Cyberattacken

Angesichts der zunehmenden Zahl von Angriffen ist Cybersicherheit ein wichtiges Thema für Unternehmen. Einem Bericht von Cybersecurity Ventures zufolge beliefen sich die Schäden durch Cyberkriminalität im Jahr 2015 weltweit auf drei Milliarden USD. 2025 sollen sie auf 10,5 Milliarden USD ansteigen.

Dieser Trend wird die Einführung von SASE zusätzlich fördern. Der Gartner-Bericht über die SASE-Konvergenz 2021 betont die Notwendigkeit, über neue Sicherheitsarchitekturen aus der Cloud nachzudenken.

Ähnlich sieht es auch Thomas Tschersich, Chief Security Officer der Deutschen Telekom: „Der Wechsel von traditionellen Netzwerkkonzepten zu SASE ist der erste Schritt zur Umsetzung echter Zero-Trust-basierter Modelle. Perimeter-basierte Netzwerksicherheit wird der verteilten Belegschaft und Cloud-Workloads nicht mehr gerecht.“

Worauf Unternehmen bei der Entwicklung einer SASE-Strategie achten sollten

Viele Anbieter, die früher SD-WAN-Lösungen angeboten haben, sind dazu übergegangen, ihre Lösungen in Richtung SASE weiterzuentwickeln, um der wachsenden Marktnachfrage gerecht zu werden. Unternehmen, die SASE einführen wollen, sollten zur Anbieterauswahl einen strukturierten Anforderungskatalog einsetzen. Gleichzeitig sollten Quick-Fix-Deployments vermieden werden – sie führen in der Regel zu erhöhter Komplexität und damit hohen Folgeaufwänden.

Grundlegend lässt sich festhalten, dass SASE als Service aus der Cloud bereitgestellt werden sollte. Dabei müssen SD-WAN- und Sicherheitsfunktionen im Angebot des jeweiligen Anbieters integriert sein. Vor einer umfassenden Implementierung kann eine Machbarkeitsstudie angeraten sein. Doch zumindest sollten Unternehmen (sich) die richtigen Fragen stellen, um den passenden Anbieter zu finden. Diese Best Practices können als Richtschnur dienen:

1 Benutzer und Anwendungen identifizieren

Wer sind Ihre User, welche Bedürfnisse haben sie? Die Kenntnis Ihrer Nutzer erlaubt die richtige Konfiguration Ihres SASE. Die existierende IT-Umgebung, Use Cases, Migrationsplan und Zeitplan müssen gründlich geprüft werden.

2 Sicherheitsrichtlinien verstehen

Wie stellen Sie sicher, dass Gesetze wie die DSGVO und der California Consumer Privacy Act, der als das strengste Datenschutzgesetz der USA gilt, berücksichtigt werden? Erlaubt die SASE-Lösung des jeweiligen Providers die Konfiguration von Zero Trust Network Access und Software-Defined Perimeter Richtlinien?

3 Das Einverständnis aller Beteiligten holen

Haben Sie die Zustimmung aller Beteiligten für die Ablösung von Legacy-Architektur/-Anwendungen? Die Umstellung auf die Cloud ist eine grundlegende Entscheidung, die Bedeutung für das ganze Unternehmen hat. Beziehen Sie daher IT- und Sicherheitsbeauftragte, Führungskräfte, Vorstand usw. ein.

4 Mit SASE-Lösungen hybrides Arbeiten erleichtern

Die User wechseln im Rahmen eines hybriden Arbeitsmodells vom Büro nach Hause – und umgekehrt. Kann die SASE-Lösung smart und ohne Brüche beide Arbeitsszenarien für den Endnutzer ermöglichen?

5 Erkennen, wie der Datenverkehr abgewickelt wird

Bietet die SASE-Lösung weltweite Verfügbarkeit mit mehreren Präsenzpunkten? Transparenz über Ihren Datenverkehr erlaubt Ihnen zu prognostizieren, ob es zu Leistungsproblemen kommen könnte.

6 Ausfallsicherheit überprüfen

Welche Service Levels bietet der Provider an? Wie sichert er die Bereitstellung seines Dienstes? Ausfälle und Stillstandzeiten sind schmerzhaft – sorgen Sie daher bestmöglich vor.

7 Nach einer Komplettlösung suchen

Wie hoch ist der Integrationsgrad der Lösung? Wenn ein Anbieter zu viele getrennte Dienste integriert, ist auch die Wahrscheinlichkeit groß, dass Sie all diese Dienste mit unterschiedlichen Konsolen, Konfigurationen und Richtlinien (vielleicht sogar mit mehr Hard- und Software) verwalten müssen. Dadurch kann sich nicht nur die Verwaltung, sondern auch die Untersuchung und Behebung eines Problems während einer Ausfallzeit als schwierig erweisen. Ideal ist eine einheitliche SASE-Lösung mit einer einzigen Konsole für die Verwaltung.

8 Nichts überstürzen

Bei der SASE-Einführung müssen immer die existierende IT-Umgebung, der Status des Legacy-Systems und die Geschäftsanforderungen des Unternehmens berücksichtigt werden. Das heißt, dass auch Altsysteme nicht auf einen Schlag abgeschafft werden. Daher wird SASE in der Regel im Rahmen eines längeren Entwicklungsprozesses peu à peu eingeführt, nicht mit einem Big Bang. Bedenken Sie, dass häufig auch Anpassungen der SASE-Lösung an Ihre Unternehmensbedürfnisse notwendig sind. ■

Lieber konsolidiert

Die Einbindung verschiedener Anbieter erhöht häufig die Komplexität der resultierenden Landschaft. Darüber hinaus können bei einem solchen Multi-Provider-Ansatz Lücken in der SASE-Lösung entstehen. Es ist daher empfehlenswert, auf einen oder zwei Anbieter zu fokussieren. Diese sollten anhand der oben genannten Aspekte bewertet werden. Nicht zuletzt sollten Unternehmen auch die Fähigkeit des Anbieters zur Innovation und zur Anpassung an Marktveränderungen in diese Bewertung einfließen lassen.

Eine benutzerfreundliche SASE-Netzwerk- und -Sicherheitslösung aus der Cloud sollte unter dem Strich vielfältige Vorteile erzielen. Unternehmen, die SASE mit Blick auf Skalierbarkeit, Flexibilität, Transparenz, Einfachheit und Leistung planen, stoßen die Tür in die Zukunft auf.

SASE ist für Sie interessant? Für die Planung Ihrer nächsten Schritte, lesen Sie unser Whitepaper zum SASE Self Check auf unserer Website.