Die Top-3-Vorteile von SASE und wie Sie sie erreichen

Warum Secure Access Service Edge (SASE)?

Moderne digitale Geschäftsmodelle ermöglichen eine ganz neue Art der Kunden- und Mitarbeiterbindung, indem sie weltweit den durchgängigen Zugriff auf Anwendungen und Services ermöglichen, unabhängig davon, von wo aus Mitarbeiter und Kunden eine Verbindung herstellen oder welche Geräte sie verwenden.

In einer digitalen Welt, in der Benutzer und Anwendungen räumlich verteilt sind, kommt man mit dem herkömmlichen Begriff von "Netzwerksicherheit" nicht mehr weiter. Gartner hat deshalb Netzwerke und Sicherheit neu überdacht und ein Modell entwickelt, das den Anforderungen des digitalen Unternehmens entspricht. Dieses Modell trägt den Namen Secure Access Service Edge (SASE).

> „Secure Access Service Edge ist ein neu entwickeltes Angebot, das die Leistungsfähigkeit von WAN mit umfassenden Netzwerksicherheitsfunktionen (wie SWG, CASB, FWaaS und ZTNA) kombiniert, um den Bedarf digitaler Unternehmen an dynamischem sicherem Zugang zu decken.“**-Gartner**[1]

VORTEIL
#1

Geringere IT-Kosten und Komplexität

Angesichts der Verteilung der Daten auf Cloud-Anwendungen und SaaS-Services und den geografisch mehr oder weniger weit verstreuten Zugriffen der Benutzer, stößt das herkömmliche netzwerkbasierte Sicherheitsmodell an seine Grenzen. Um dies zu kompensieren, mussten Organisationen die Sicherheitslücken durch die Bereitstellung zusätzlicher Services schließen, dabei aber, trotz eines Mangels an Fachkräften, erheblich höhere Bereitstellungs-, Verwaltungs- und Betriebskosten in Kauf nehmen. Allerdings ist dieses Netzwerksicherheitsmodell – trotz wachsender Kosten und Komplexität – immer noch nicht skalierbar, nicht agil und in einer digitalen Welt einfach nicht effektiv.

Anstatt zu versuchen, ein zeitgemäßes Problem mit einem alten Konzept zu lösen, stellt SASE das Sicherheitsmodell einfach auf den Kopf. Während ältere Ansätze darauf basierten, Perimeter rund um die Anwendungen zu errichten, zielt SASE auf Entitäten, zum Beispiel Benutzer, die auf die Anwendungen zugreifen, und rückt die Sicherheit so nahe wie möglich an diese Entitäten heran. Als Cloud-Service erlaubt oder verweigert SASE – dynamisch und gemäß den definierten Geschäftsregeln einer Organisation – Verbindungen zu Services und Anwendungen. Das alles wird über einen einzigen Service abgewickelt, der mehrere, bis dahin vereinzelte Funktionen, wie SWG, ZTNA usw. zusammenführt.

Worauf man achten sollte

Die wichtigste Komponente eines überzeugenden SASE-Angebots ist die jeweils zugrunde liegende Architektur. Gartner stellte spezifische Anforderungen an eine Architektur, mit der sich das Versprechen von SASE erfüllen lässt. Vor allem muss die Architektur von Grund auf neu aufgebaut werden, um die Anforderungen eines vollständig in der Cloud bereitgestellten Sicherheitsservice zu erfüllen.

Es muss sich um ein verteiltes Angebot handeln, das mandantenfähig ist und eine bedarfsabhängige globale und dynamische Skalierung ermöglicht. Das Angebot muss sich von herkömmlichen, auf Richtlinien und Policy-Layers basierenden, Netzwerkkonzepten lösen und stattdessen auf Business Policies aufbauen. Und schließlich muss diese Architektur eine tatsächlich integrierte Plattform mit einheitlichem Cloud-Management unterstützen.

Was man vermeiden sollte

Gartner warnt ausdrücklich vor herkömmlichen Netzwerksicherheitsansätzen, die sich auf VM-basierte Angebote stützen, die in Infrastrukturen von Cloud-Anbietern ausgeführt werden. Die Skalierung solcher VM-basierter Lösungsansätze ist in einer IaaS-Umgebung problematisch und bietet aufgrund der unausweichlichen Hairpin-Verbindungen zwischen den Cloud-Anbietern und den Benutzern der Anwendungen keine durchgängige Nutzererfahrung.

Dieses Modell basiert auf einer Single-Tenancy-Architektur, die in einem SASE-Modell auf dem Benutzerzugriff basierende, netzwerkbasierte Zugriffsrichtlinien zu verwenden versucht. Das führt zu erheblich komplexeren Deployments, die sich nicht in ein SASE-Modell übertragen lassen. Darüber hinaus arbeiten diese Ansätze häufig mit mehreren Produkten, die nicht wirklich integriert sind, sondern mittels einer Overlay-Benutzeroberfläche, die aus unabhängigen Services zusammenfügt wurde, welche häufig im Rahmen von Übernahmen erworben wurden.

> „SAS-Richtlinienentscheidungs- und Durchsetzungsfunktionen müssen überall verfügbar sein, wo sich die Endgeräte befinden ... SASE-Angebote, die nur die Internet-Backbone-Fähigkeit von IaaS nutzen, ohne lokale POPs / Edge-Funktionen zur ´Verfügung zu stellen, riskieren lange Wartezeiten, Leistungseinbußen und unzufriedene Benutzer.“ **- Gartner** [1]

VORTEIL #2

Vermittlung einer hervorragenden Nutzererfahrung

Es gibt einen guten Grund, warum der Schwerpunkt von SASE auf der Nutzererfahrung liegt. Solange die Benutzer im Netzwerk angemeldet waren, die Anwendungen im Rechenzentrum liefen und Server und Infrastruktur im Besitz der IT-Abteilung waren und dort verwaltet wurden, war die Nutzererfahrung leicht zu steuern und vorherzusagen. Nun sind die Anwendungen über mehrere Clouds verteilt, aber der Zugriff auf diese Anwendungen stützt sich weiterhin auf das alte Modell eines VPN, das aus Sicherheitsgründen eine Verbindung zu einem Netzwerk herstellt. Dieses Modell bringt den Benutzer zur Sicherheit und nicht die Sicherheit zum Benutzer, obwohl das für eine positive Nutzererfahrung unerlässlich ist. Um eine optimale Bandbreite und geringe Wartezeiten sicherzustellen, fordert SASE die Durchsetzung der Sicherheit in der Nähe der Benutzer, die intelligente Verwaltung der Benutzerverbindungen an den Internetknoten und die Optimierung der direkten Verbindungen (Peering) zu Cloud-Anwendungen und -Services.

Worauf man achten sollte

Entscheidend für eine sehr gute Nutzererfahrung ist die Bereitstellung der optimalen Bandbreite mit der geringsten Wartezeit. Das lässt sich nur effektiv bewerkstelligen, wenn man den Zugriff auf die Anwendungen beschleunigt und sicherstellt, dass im Rahmen der Bandbreitensteuerung die richtige Bandbreite zugewiesen wird.

Idealerweise liegt der Sicherheits-Stack so nah wie möglich am Standort des Benutzers, an Internetknoten in einer geografisch weit verteilten Bereitstellung. Der Zugriff auf Anwendungen über diese Vermittlungspunkte erfordert die Fähigkeit, den Datenverkehr durch direktes Peering intelligent zum nächstgelegenen geografischen Standort der Anwendung leiten zu können.

Was man vermeiden sollte

Angebote, die auf bei Cloud-Anbietern oder IaaS ausgeführten VMs basieren, erfordern Hairpin-Verbindungen. Solche Angebote werden im SASE-Dokument ausdrücklich als nicht der Definition einer SASE-Lösung entsprechend bezeichnet und sollten vermieden werden.

Dies liegt in erster Linie daran, dass VM-basierte Architekturen Verbindungen nicht vom Benutzer aus skalieren und steuern, sondern von der Anwendungsumgebung aus. Damit lässt sich jedoch keine gute Nutzererfahrung garantieren. Außerdem lassen sich diese Angebote nicht dynamisch skalieren und erfordern eine Nutzungsplanung, bei der spätere Änderungen nicht ohne geplante Ausfallzeiten möglich sind.

> "Es kommt auf die SASE-Architektur an. Im Idealfall ist das Angebot Cloud-basiert und stützt sich auf Mikroservices, die bei Bedarf skaliert werden können. Um die Wartezeiten zu minimieren, sollten Pakete in den Speicher kopiert, verarbeitet und weitergeleitet / blockiert werden und nicht von einer virtuellen Maschine (VM) an eine andere VM oder von Cloud zu Cloud weitergeleitet werden. Der Software-Stack sollte keine spezifische Hardware-Abhängigkeit aufweisen und zu jedem Zeitpunkt und an jedem Ort instanziiert werden, um die risikooptimierten und richtlinienbasierten Funktionen für die Endgeräte bereitzustellen. " **- Gartner** [1]

VORTEIL
#3

Vermindertes Risiko

Bei der Sicherheit dreht sich alles darum, Risiken zu erkennen und zu vermeiden. SASE als Cloud-Service wurde entwickelt, um den besonderen Risiken der neuen Gegebenheit geografisch weit verteilter Benutzer und Anwendungen begegnen zu können. Die Definition von Sicherheit als in die Struktur des Modells integrierte Funktion statt als Funktion, die von der Konnektivität der Services getrennt ist, stellt sicher, dass alle Verbindungen überprüft und gesichert werden, unabhängig davon, wo Benutzer eine Verbindung herstellen, auf welche Apps sie zugreifen oder ob eventuell eine Verschlüsselung zum Einsatz kommt.

Worauf man achten sollte

Entscheidend für die Risikominderung ist die Fähigkeit, die Konzepte der netzwerkbasierten Konnektivität aufzugeben und stattdessen die Benutzer auf der Grundlage eines echten Zero Trust Network Access (ZTNA) mit Anwendungen zu verbinden. ZTNA gewährleistet, dass nur zugriffsberechtigte Benutzer auf eine Anwendung zugreifen können. Diese Berechtigung wird aufgrund von Geschäftsregeln und nicht von komplexen mehrschichtige Richtliniendefinitionen erteilt.

Eine SASE-Plattform vermindert Risiken auch dadurch, dass sie die Angriffsfläche beseitigt. Sie verbirgt das Unternehmensnetzwerk und die Quellidentitäten vor dem Internet und verhindert damit, dass Sie zum Ziel von Angriffen, wie beispielsweise DDoS, werden.

Das SASE-Modell wird über eine Proxy-basierte Architektur bereitgestellt, welche die gesamte Kommunikation zwischen Benutzern und Anwendungen abwickelt. Diese Architektur gewährleistet, dass der gesamte Datenverkehr entschlüsselt und überprüft werden kann, und bietet umfassende Transparenz. Schlussendlich sorgt die SASE-Architektur für den Austausch des vollständigen Datenkontexts zwischen Entitäten und Anwendungen, um sicherzustellen, dass alle Verbindungen den Compliance- und Data Governance-Anforderungen entsprechen.

Was man vermeiden sollte

Herkömmliche Lösungen zur Perimetersicherheit haben sich auf ein Firewall-basiertes Modell gestützt, das Paket-Streams untersucht und Risiken anhand der Untersuchung dieser Streams bestimmt hat. Dieses Modell funktionierte zwar für die perimeterbasierte Sicherheit, ist jedoch den neuen Herausforderungen eines SASE-basierten Deployment nicht gewachsen.

Das größte Problem einer als Dienst ausgeführten Firewall-Architektur ist, dass Bedrohungen erst nachträglich erkannt werden und diesen ermöglicht wird, ihr Ziel zu erreichen, bevor sie entdeckt werden. Das hat einen einfachen Grund: Sie sind nicht in der Lage, die Daten vor dem Senden zurückzuhalten, um ihre Folgen zu ermitteln. Diese Einschränkung erschwert die Sitzungsentschlüsselung und den Datenschutz außerordentlich, da dies Funktionen sind, bei denen der Stream – ähnlich wie bei einem Proxy – zurückgehalten und neu zusammengesetzt werden muss.

Bei einem Firewall-Service ist für die Entschlüsselung, Überprüfung und Wiederherstellung von Funktionen ein separater Prozess erforderlich, der vom Dienst entkoppelt ist. Dieser Prozess kompliziert die Richtlinien, bringt Wartezeiten mit sich und führt und zu einer schlechten Leistung – im Rahmen der Implementierung ist häufig nur ein eingeschränkter Funktionsumfang möglich. Darüber hinaus erfordert SASE eine Single-Pass-Architektur, um den gesamten Inhalt auf einmal verarbeiten zu können. Stream-basierte Firewall-Angebote setzen die Source-IP-Adresse des Host-Netzwerks auch potenziellen Gegnern aus – im Prinzip machen sie auf ihre eigenen Angriffsflächen aufmerksam und laden praktisch zu gezielten Angriffen ein.

> „Viele Funktionen von SASE verwenden ein Proxy-Modell, um in den Datenpfad einzudringen und den Zugriff zu sichern. Anbieter älterer Inline-Netzwerke und Unternehmens-Firewalls verfügen nicht über das erforderliche Know-how, um verteilte integrierte Proxys zu skalieren. Dies birgt das Risiko höherer Kosten und / oder einer schlechten Leistung für SASE-Anwender. “ **- Gartner** [1]

Der Zscaler SASE-Ansatz

Die Cloud-Sicherheitsplattform von Zscaler ist ein SASE-Dienst, der von Grund auf für Leistung und Skalierbarkeit konzipiert ist. Da unsere Plattform weltweit verbreitet ist, befinden sich Benutzer immer in der Nähe ihrer Anwendungen, und da wir uns an wichtigen Internet Exchanges rund um den Globus mit Hunderten von Partnern austauschen, erhalten Sie optimale Leistung und Zuverlässigkeit für Ihre Benutzer.

Zscaler baute seine Plattform bereits bei seiner Gründung vor einem Jahrzehnt auf denselben Prinzipien auf, die auch SASE zugrunde liegen. Heute vertrauen mehr als 400 der Forbes Global 2000-Unternehmen darauf, dass Zscaler sie sicher ins digitale Zeitalter führt.

Im Laufe seiner Marktpräsenz hat Zscaler bewiesen, dass die Zscaler-Architektur skalierbar ist. Derzeit werden zu Spitzenzeiten bis zu Milliarden Transaktionen verarbeitet und spezifische Sicherheitsupdates pro Tag durchgeführt.

Die Zscaler SASE-Architektur wird in 150 Rechenzentren weltweit bereitgestellt, um zu gewährleisten, dass Benutzer sichere, schnelle und lokale Verbindungen erhalten, egal wo sie sich verbinden.

Mehr erfahren

Um noch mehr über SASE zu erfahren, rufen Sie **zscaler.com/gartner-secure-access-service-edge-sase** auf und lesen Sie, was Gartner über die Zukunft der Netzwerksicherheit zu sagen hat.

Weitere Informationen zum SASE-Modell von Zscaler finden Sie unter **zscaler.com/products/secure-access-service-edge**.

1. Gartner, The Future of Network Security Is in the Cloud; 30. August 2019; Lawrence Orans, Joe Skorupa, Neil MacDonald

Über Zscaler

Zscaler ermöglicht Organisationen eine sichere Transformation ihrer Netzwerke und Anwendungen für eine mobile Cloud-First-Welt. Zscaler verbindet Benutzer unabhängig von ihrem Gerät, Standort oder Netzwerk mit Anwendungen und Cloud-Services und bietet gleichzeitig umfassende Sicherheit und eine schnelle Nutzererfahrung. All dies ohne kostspielige, komplexe Gateway-Appliances.

© 2019 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ ist entweder (i) eine eingetragene Handelsmarke oder Dienstleistungsmarke oder (ii) eine Handelsmarke oder Dienstleistungsmarke von Zscaler, Inc. in den Vereinigten Staaten und/oder anderen Ländern. Alle anderen Handelsmarken sind Eigentum ihrer jeweiligen Besitzer.

zscaler™