Akamai

KAUFRATGEBER

Leitfaden für die Auswahl eines cloudbasierten Secure Web Gateway

Remote-Mitarbeiter schützen und Unternehmenssicherheit vereinfachen

Inhaltsverzeichnis

Sicherheit in modernen Unternehmen: Überdenken des Backhauls im Rechenzentrum 2

Neue IT- und Sicherheitsanforderungen durch Zunahme der Remote-Arbeit 3

Was spricht für ein cloudbasiertes Secure Web Gateway? 5

Hauptkriterien für die Auswahl eines Secure Web Gateways 6

- Auswertung aller DNS- und URL-Anfragen 6
- Mehrere Techniken der Payload-Analyse 7
- Zero-Day-Phishing-Erkennung 7
- Untersuchung von verschlüsseltem Traffic 7
- Integrierter Schutz vor Datenverlust 8
- Shadow-IT-Erkennung und -Management 8
- Schutz überall und für jedes Gerät 9
- Sicherer Zugriff auf alle Unternehmensanwendungen 9
- Optimale Performance 11
  - Microsoft 365-Integration 11

Sicherheit an die Edge verlagern 12

Sicherheit in modernen Unternehmen: Überdenken des Backhauls im Rechenzentrum

Cloud Computing, Software-as-a-Service (SaaS), Mobilität und moderne Netzwerkarchitekturen haben in vielen Fällen die Geschäftsabläufe drastisch verändert. Für IT-Teams brachen damit stürmische Zeiten an, mussten sie doch für die Sicherheit der Mitarbeiter sorgen, ohne den Nutzen der neuen Technologien zu beschränken. Und schon gibt es eine neue Herausforderung: Unabhängig davon, wo Unternehmen auf ihrem Weg hin zur digitalen Transformation standen, mussten sie sich schnell umstellen, um den drastischen Anstieg der Remote-Nutzerzahlen im Jahr 2020 zu bewältigen.

Ein Secure Web Gateway ist eine wichtige Komponente für den Schutz der unternehmensweiten Belegschaft. Allerdings verwenden viele Unternehmen noch physische Appliances, die in Rechenzentren bereitgestellt werden. Diese Hardware erfordert einen hohen Verwaltungs- und Wartungsaufwand sowie ständige Upgrades und ein umständliches Traffic-Backhauling zur Überprüfung und Kontrolle des Webtraffics, was letztendlich die Performance beeinträchtigt.

Unternehmen benötigen einen modernen, schlanken Ansatz, um dieser neuen Realität einer verteilten Unternehmensumgebung gerecht zu werden. Die Lösung: Verzichten Sie auf Hardware-Appliances und verlagern Sie die Secure Web Gateway-Funktionen in die Cloud.

Dieser Kaufratgeber beschreibt die Vorteile eines cloudbasierten Secure Web Gateways und erklärt, auf welche Funktionen Sie bei einer modernen Web-Gateway-Technologie achten sollten.

Neue IT- und Sicherheitsanforderungen durch Zunahme der Remote-Arbeit

In den letzten zehn Jahren hat sich die Zahl der Remote-Mitarbeiter in Unternehmen stetig erhöht. COVID-19 hat diesen Trend noch beschleunigt und er wird sich voraussichtlich weit über die Pandemie hinaus fortsetzen. Laut einer Studie von Gartner gaben 74 % der befragten CFOs an, dass mindestens 5 % ihrer bisher vor Ort beschäftigten Mitarbeiter auch nach dem Ende der Pandemie dauerhaft im Homeoffice arbeiten werden.[1]

Gleichzeitig ist die Zahl gezielter Angriffe durch Phishing, Ransomware und Malware sprunghaft angestiegen. In einer kürzlich durchgeführten Studie gaben 53 % der Befragten an, seit Beginn der COVID-19-Pandemie einen Anstieg der Phishing-Aktivitäten beobachtet zu haben.[2] In einem aktuellen Bericht des US-Finanzministeriums heißt es, dass Lösegeldzahlungen aufgrund von Ransomware-Angriffen während der COVID-19-Pandemie zugenommen haben, da Cyberakteure auf Onlinesysteme abzielen, auf die Menschen zur Weiterführung ihrer Geschäfte angewiesen sind.[3]

Traditionell sicherten Unternehmen den Internetzugang sowohl für Nutzer am Hauptstandort, in Niederlassungen als auch für Remote-Mitarbeiter durch die Installation von Sicherheits-Appliances, wie z. B. Secure Web Gateways, in ihren Rechenzentren. Der gesamte Webtraffic wurde dann zur Überprüfung und Kontrolle an diesen zentralen Standort weitergeleitet.

Unternehmen haben diese Secure Web Gateways eingesetzt, um unerwünschte Malware aus dem von Nutzern initiierten Webtraffic zu filtern, Nutzer am Zugriff auf bösartige Websites zu hindern und Unternehmens- und gesetzliche Richtlinien durchzusetzen.

Diese Gateway-Lösungen wurden ursprünglich für Umgebungen entwickelt und eingesetzt, in denen die meisten Mitarbeiter vom Unternehmen verwaltete Geräte an ihrem Arbeitsplatz verwendeten. Aber mit steigender Nutzerzahl an entfernten Standorten und Zweigstellen sowie einer Zunahme des Traffics für den Zugriff auf SaaS-Anwendungen über das öffentliche Internet mussten Unternehmen mehrere redundante Secure Web Gateways im zentralen Rechenzentrum installieren, um eine zufriedenstellende Performance aufrechtzuerhalten. Die Beschaffung und Verwaltung dieser Module wurde zunehmend komplexer, kostspieliger und zeitaufwändiger.

> **„Der prozentuale Anteil des IT-Budgets, der für Rechenzentren ausgegeben wird, ist in den letzten Jahren gesunken und macht nur noch 17 % des Gesamtbudgets aus.“**
>
> — Gartner, IT Key Metrics Data 2019

Alternativ wurden Niederlassungen von Unternehmen auch mit Secure Web Gateway-Appliances ausgestattet und der Traffic für alle Remote-Nutzer über Backhaul bereitgestellt. Diese Redundanz hatte zur Folge, dass sowohl die Anzahl der Appliances als auch die damit verbundenen Kosten anstiegen und eine arbeitsintensive Implementierung und Verwaltung erforderlich waren.

Außerdem wurde es immer schwieriger, konsistente Sicherheitsrichtlinien über eine große Anzahl von Standorten hinweg aufrechtzuerhalten. Selbst wenn Unternehmen virtuelle Appliances implementierten, um die Anhäufung dieser Geräte zu reduzieren, mussten sie dennoch zusätzliche Hardware bereitstellen und verwalten.

Ein dritter Ansatz war die Hybridbereitstellung. Hierbei verwendeten Unternehmen lokale Secure Web Gateways weiterhin für wichtige Standorte, leiteten den Webtraffic der Niederlassungen jedoch an ein cloudbasiertes Secure Web Gateway weiter – auch hier erfolgte ein Backhauling des Traffics für Remote-Mitarbeiter. Mit diesem Ansatz konnten zwar vorhandene Hardware-Investitionen in Ausrüstung vor Ort geschützt werden. Allerdings erhöhte er auch die Komplexität, da die Unternehmen am Ende unterschiedliche Systeme verwalten mussten. Die zusätzliche Ausrüstung und der Verwaltungsaufwand waren nicht nur sehr viel teurer als ein reiner Cloudansatz, es war auch schwierig, konsistente Richtlinien über lokale und cloudbasierte Systeme hinweg durchzusetzen.

> **Gartner zufolge werden bis 2025 80 % aller Unternehmen ihre traditionellen Rechenzentren schließen.[4]**

Erschwerend kommt hinzu, dass Unternehmen, die diese immer komplexeren Lösungen eingeführt haben, mit einem Mangel an Cybersicherheitspersonal konfrontiert wurden. Eine Studie von (ISC)[2] ergab, dass ein Anstieg der Facharbeiterzahlen um 62 % erforderlich wäre, um den derzeitigen Mangel an benötigten Cybersicherheitsmitarbeitern in den USA zu beheben.[5]

Was spricht für ein cloudbasiertes Secure Web Gateway?

Unternehmen benötigen einen modernen Ansatz für ihre Websicherheit – einer, der für die Cloudstrategie des Unternehmens geeignet ist und gleichzeitig Remote-Arbeit ermöglicht und fördert. Ein cloudbasiertes Secure Web Gateway bietet Unternehmen ein hohes Maß an Sicherheit und reduziert gleichzeitig die Komplexität. Es ist direkt mit dem Internet verbunden, sodass auf die ausufernde Implementierung von Appliances und Backhauling verzichtet werden kann.

Cloudbasierte Secure Web Gateways bieten Unternehmen folgende Vorteile:

Verringerte Komplexität: Als Service in der Cloud kommen Secure Web Gateways ohne die Bereitstellung von Hardware oder virtuellen Appliances sowie die Konfiguration, Verwaltung und den Austausch bzw. die Aktualisierung der Hardware im Dreijahresrhythmus aus.

Weniger Performance-Engpässe: Mit internetbasierten Secure Web Gateways ist es nicht mehr erforderlich, zusätzliche Appliances einzusetzen, um immer mehr Webtraffic und die zunehmende Menge an verschlüsseltem Traffic zu bewältigen. Weitere Services können von Kunden mit minimalen Auswirkungen auf die Performance nach Bedarf hinzugefügt werden.

Weniger Kosten durch Traffic-Backhauling/ -Hairpinning: Cloudbasierte Secure Web Gateways sichern den Webtraffic und machen das Backhauling von Traffic durch eine direkte Verbindung zum Internet überflüssig, sodass gleichzeitig Netzwerkkosten für Multiprotocol Label Switching reduziert werden.

Höhere Effizienz der für Sicherheit zuständigen IT-Teams: Da Secure Web Gateways in der Cloud praktisch ohne Wartung der Hardware oder Software auskommen, hat das knapp bemessene Sicherheitspersonal mehr Zeit, sich auf andere proaktive Sicherheitsmaßnahmen zu konzentrieren.

Einheitliche Sicherheitsrichtlinien: Unternehmen können Richtlinien verwenden, die zentral verwaltet, aber global eingesetzt werden, und zwar für alle Nutzer und von jedem Gerät aus. Selbst wenn das Unternehmen unterschiedliche Richtlinien für unterschiedliche Regionen vorhalten muss, können diese alle über die gleiche Nutzeroberfläche verwaltet werden.

Hauptkriterien für die Auswahl eines Secure Web Gateways

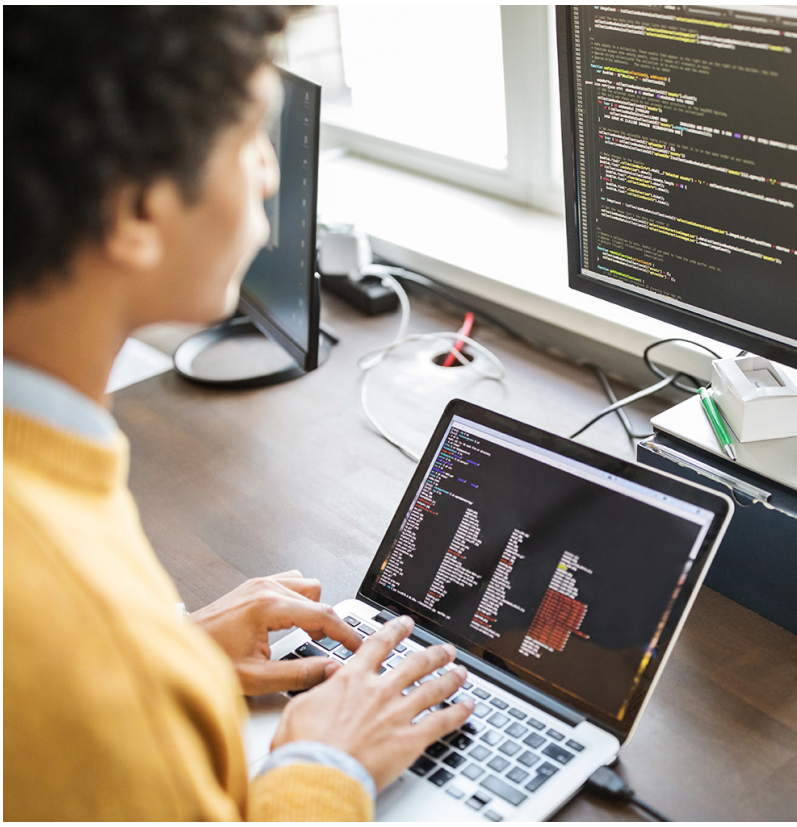
Bei der Auswahl eines cloudbasierten Secure Web Gateway muss unbedingt berücksichtigt werden, dass die Sicherheit das Hauptanliegen darstellt. Viele ältere Secure Web Gateways weisen Funktionen auf, die nicht mehr existente Probleme lösen sollen. Beispielsweise eine Kontrolle der Bandbreitennutzung, die für eine Zeit entwickelt wurde, als Bandbreite noch teuer war. Oder sie sperren die Nutzung von YouTube oder Facebook während der Arbeitszeit. Heute sind diese Funktionen nicht mehr notwendig, da Bandbreite reichlich vorhanden ist und so viele Menschen ihre mobilen Geräte nutzen, dass Unternehmen nicht mehr daran interessiert sind, diese Dienste auf Firmengeräten zu sperren.

Unternehmen benötigen heute ein cloudbasiertes Secure Web Gateway, das speziell darauf ausgelegt ist, moderne Sicherheitsbedenken auszuräumen. Die Lösung muss insbesondere eine umfassende Verteidigungsstrategie beinhalten, bei der mehrere Sicherheitsmaßnahmen eingesetzt werden, um ein Höchstmaß an Sicherheit zu ermöglichen. Ein solcher Ansatz sollte alle Bereiche der Cybersicherheit abdecken und redundante Sicherheitsmaßnahmen umfassen. Wenn also eine Verteidigungslinie durchbrochen wird, sind zusätzliche Verteidigungsschichten vorhanden, die verhindern, dass Angreifer die entstandenen Lücken ausnutzen können. Dieser mehrschichtige Ansatz sorgt dafür, dass Bedrohungen wie Malware, Ransomware und Phishing früher und schneller blockiert werden können, vor allem bevor sie das Gerät des Nutzers infizieren können.

Ein Secure Web Gateway, das eine Defense-in-Depth-Strategie beinhaltet, sollte die folgenden Sicherheitsfunktionen bieten:

Auswertung aller DNS- und URL-Anfragen

Bei einer cloudbasierten SWG-Lösung sollten alle URL- und DNS-Anfragen gegen Echtzeit-Threat-



Intelligence abgeglichen und schädliche Anfragen frühzeitig in der Kill Chain blockiert werden. Wenn das Secure Web Gateway Bedrohungen blockiert, bevor eine ausgehende Verbindung zustande kommt, müssen zurückgegebene Inhalte nicht mehr geöffnet und überprüft werden. Dank dieser Effizienz werden rechnerintensive Prozesse vermieden und die Menge des Traffics reduziert, die das Secure Web Gateway in der Payload-Phase analysieren muss. Das Ergebnis? Eine insgesamt verbesserte Performance der Secure Web Gateways.

Die Threat Intelligence muss Schutz vor Malware, Ransomware, Phishing und geringem Durchsatz durch DNS-basierte Datenextraktion bieten. Sie sollte zudem einen aktuellen und zweckdienlichen Schutz mit einer möglichst geringen Rate an False Positives bieten.

Mehrere Techniken der Payload-Analyse

Da alle Bedrohungen unterschiedlich sind und daher keine einzelne Erkennungstechnik oder -methode jede Art von Malware abdecken kann, sollte die Secure Web Gateway-Lösung über mehrere Engines für die Malware-Analyse verfügen. Die Engines sollten HTTP- und HTTP-Payloads entweder inline oder offline mit einer Vielzahl von Erkennungstechniken scannen, wie z. B. signaturbasierte und signaturlose Erkennung, maschinelles Lernen und Sandboxing. Diese Analysen liefern einen umfassenden Zero-Day-Schutz vor potenziell schädlichen Objekten wie ausführbaren Dateien und Dokumenten.

Zero-Day-Phishing-Erkennung

Remote-Mitarbeiter sehen sich seit dem Ausbruch der COVID-19-Pandemie weiterhin mit einer Zunahme von Phishing-Angriffen konfrontiert. Cyberkriminelle starten diese Angriffe über E-Mail, soziale Medien und Instant-Messaging-Anwendungen sowie über Onlinekanäle für Dateifreigabe und Zusammenarbeit, um Anmeldedaten von Unternehmen zu stehlen, die ihnen Zugang zum Unternehmensnetzwerk verschaffen. Wenn sie einmal drin sind, können sie sich nahezu frei bewegen, um Daten und geistiges Eigentum abzugreifen oder Ransomware-Kampagnen zu veröffentlichen.

Die Schritte der Sicherheitsanbieter zum Erkennen und Blockieren von Zugriffen auf Phishing-Seiten sehen in der Regel wie folgt aus:

1. **Beobachten ungewöhnlicher Traffic-Aktivitäten in einer Domain**
2. **Analysieren dieser Domain**
3. **Feststellen, ob es sich um eine Phishing-Domain handelt**
4. **Hinzufügen der Domain zu einer Sperrliste**
5. **Senden der aktualisierten Sperrliste an Kunden**

Dieser Prozess kann Stunden in Anspruch nehmen. Und schlimmer noch: Cyberkriminelle von heute starten mithilfe von Phishing-Kits nur kurzlebige Angriffe, was die Erkennung noch schwieriger macht. Bis die Phishing-Domain oder -URL gefunden wird, ist der Angriff bereits vorüber. Je ausgefeilter und gezielter der Phishing-Angriff ist, desto kürzer ist seine Dauer.

Doch auch wenn diese Kampagnen schnell beendet sind, können sie von einer fortschrittlichen Zero-Day-Phishing-Erkennungs-Engine identifiziert und blockiert werden. Die wiederkehrenden Elemente dieser kitbasierten Angriffe sind im Code der Phishing-Seiten zu sehen. Anhand dieser Informationen ist es möglich den „Fingerabdruck“ dieser Seiten zu identifizieren, der eine genaue Zuordnung ermöglicht.

Eine Secure Web Gateway-Lösung sollte eine Engine für die Zero-Day-Phishing-Erkennung umfassen, mit der angefragte Webseiten analysiert und mit den digitalen Fingerabdrücken von bekannten Phishing-Seiten verglichen werden können.

Untersuchung von verschlüsseltem Traffic

Das Internet ist ein von Natur aus unsicherer Kanal für die Datenübertragung. Daher wird Webtraffic umfassend verschlüsselt, um Angreifer zu stoppen, die den Datenverkehr abhören, fälschen oder manipulieren wollen. Transport Layer Security (TLS) ist der de facto Verschlüsselungsstandard für sicheres Surfen im Internet. TLS erzeugt einen sicheren Tunnel zwischen zwei Endpunkten, in diesem Fall zwischen Client-Browser und Webserver.

> **Der Anteil des verschlüsselten Webtraffics im Internet ist stetig gestiegen, von etwa 50 % im Jahr 2014 auf heute zwischen 80 % und 90 %. Die meisten (96 %) der 100 populärsten Websites weltweit verwenden HTTPS.**
>
> – Google Transparenzbericht 2020

Aber nicht jeder HTTPS-Traffic ist harmlos. Angreifer und Malware-Autoren setzen ebenfalls auf Verschlüsselung, um ihre Aktivitäten zu verbergen, Nutzer (durch Ransomware) am Zugriff auf Dateien zu hindern und ihre bösartige Netzwerkkommunikation zu verbergen. Eine aktuelle Studie ergab, dass etwa ein Viertel der im Internet verbreiteten Malware Kommunikation per TLS verwendete.[6]

Für eine proaktive Überprüfung und Kontrolle des HTTPS-Webtraffics ist es erforderlich, sich den sicheren Tunnel genauer anzuschauen und den verschlüsselten Traffic mithilfe eines Proxyservers (als vertrauenswürdigem Vermittler) zu untersuchen. Der Proxyserver sollte den HTTPS-Traffic in Klartext entschlüsseln, ihn analysieren, den Traffic erneut verschlüsseln und dann eine weitere sichere Verbindung mittels MITM-Technik (Machine in the Middle) aufbauen. MITM prüft angeforderte URLs, um festzustellen, ob sie sicher oder bösartig sind, bietet Einblick in den TLS-verschlüsselten Traffic und schützt das Unternehmen vor Bedrohungen. Die Vertraulichkeit und Integrität des Traffics zu den Ursprungswebsites bleiben dabei gewahrt.

MITM-Überprüfungen erfordern eine erhebliche Verarbeitungskapazität. Das Surfen im Internet kann sich daher aufgrund von Latenzzeiten verlangsamen. Mittels Secure Web Gateway sollten Services angeboten werden, die zur Verbesserung der Anwendungsperformance beitragen. Diese sollten ein global verteiltes Servernetzwerk und intelligente Software in der Nähe der Nutzer und Rechenzentren weltweit für Weboptimierungen beinhalten, die die Anwendungsperformance und -verfügbarkeit verbessern.

Es lohnt sich für die MITM auch zu überprüfen, ob der Anbieter des cloudbasierten Secure Web Gateway eine zentrale Liste nicht ordnungsgemäß funktionierender Domains und URLs pflegt, die umgangen werden sollten. Darüber hinaus sollte das Cloud-SWG die Möglichkeit bieten, die MITM-Überprüfung für bestimmte Arten sensibler Webinhalte, wie Finanzdienstleistungen und Gesundheitsdaten, zu umgehen.

Integrierter Schutz vor Datenverlust

Den Verlust personenbezogener Daten (Personal identifiable information, PII) und anderer vertraulicher Geschäftsdaten proaktiv zu verhindern ist angesichts möglicher wirtschaftlicher Schäden oder Reputationsverluste entscheidend. Ein cloudbasiertes Secure Web Gateway sollte daher integrierte Funktionen zum Schutz vor Datenverlust beinhalten, die leicht zu konfigurieren und bereitzustellen sind. Häufig aktualisierte Wörterbücher sollten Datenschutz- und Sicherheitsvorschriften wie PII, PCI-DSS und HIPAA umfassen, und Unternehmen sollten die Möglichkeit haben, nutzerdefinierte Wörterbücher zu erstellen.

Shadow-IT-Erkennung und -Management

Nutzern stehen Hunderttausende von Anwendungen zur Verfügung, die sie herunterladen, installieren und auf verwalteten Geräten nutzen können, ohne dass das Sicherheitsteam des Unternehmens davon Kenntnis hat. Aber die Verwendung nicht genehmigter Anwendungen kann die Angriffsfläche des Unternehmens erheblich vergrößern und sein Risikoprofil erhöhen.

> **Im Durchschnitt nutzen Unternehmen über 1.295 Apps und Cloudservices. Mehr als 95 % davon sind ungemanagt und ohne IT-Administrationsrechte.**
>
> – Cybersecurity Insiders, Cloud Security Report 2019

Ein cloudbasiertes Secure Web Gateway sollte umgehend erkennen können, welche Anwendungen genutzt werden und wie viele Nutzer bestimmte Anwendungen installiert haben. Außerdem sollte es die Anwendungen sichtbar machen, die ein potenzielles ernstes Sicherheitsrisiko darstellen. Einmal identifiziert, sollte die Lösung in der Lage sein, die gesamte Anwendung oder bestimmte Anwendungsoperationen zu blockieren (z. B. Uploads zulassen, aber keine Downloads).

Schutz überall und für jedes Gerät

Flexible Arbeitsmodelle haben im letzten Jahrzehnt einen massiven Aufwärtstrend erfahren. Nutzer können nun von überall und von jedem Gerät aus arbeiten. Und als Folge der Homeoffice-Entwicklung während der Pandemie haben sich 59 % der Endnutzerdatenverarbeitung in Unternehmen auf Mobilgeräte verlagert, die PCs und Laptops ergänzen oder ersetzen. Und dieser Wandel wird sich voraussichtlich auch nach der Rückkehr in den normalen Büroalltag fortsetzen.[7]

Der Umstieg auf Mobilgeräte und die verstärkte Nutzung von WLAN-Netzwerken können Schwachstellen in der Sicherheitsstruktur eines Unternehmens darstellen. Unternehmen müssen daher in der Lage sein, ein einheitliches, universelles Sicherheitsniveau umzusetzen, ohne die Performance der Geräte zu beeinträchtigen.

Ein Cloud Secure Web Gateway sollte gezielte Bedrohungen wie Malware, Ransomware, Phishing, DNS-Datenextraktion und Zero-Day-Angriffe auf jedem Gerät (iOS, Android OS, Chrome OS) und in jedem Netzwerk, auf das der Nutzer zugreift, proaktiv erkennen, blockieren und verringern. Die Gateway-Lösung sollte umfassende Kontrollmöglichkeiten und eine modernisierte Verwaltung auf globalem Niveau bereitstellen und gleichzeitig eine optimale Mobilgerät-Performance gewährleisten.

Sicherer Zugriff auf alle Unternehmensanwendungen

Ein Cloud Secure Web Gateway schützt Nutzer und Geräte beim Zugriff auf das öffentliche Internet vor Malware. Dies ist jedoch nur ein Puzzleteil des gesamten Sicherheitsansatzes eines Unternehmens.

Um einen ganzheitlichen Sicherheitsansatz für das Unternehmen zu schaffen, müssen Unternehmen auch unternehmenseigene und -verwaltete Anwendungen vor böswilligen Akteuren schützen: unabhängig davon, ob sie sich im Unternehmensrechenzentrum oder in einer IaaS-Umgebung befinden. Herkömmliche Netzwerksicherheitstools sichern den Netzwerkperimeter, aber wenn Angreifern hier der Einbruch gelingt (beispielsweise durch Diebstahl der Nutzeranmeldedaten oder Installation von Malware auf einem Nutzergerät), können sie sich im Netzwerk praktisch frei bewegen.

Unternehmen benötigen daher ein Cloud Secure Web Gateway, das auch eine Zero-Trust-Netzwerkzugriffstechnologie (ZTNA) zum Schutz unternehmensinterner Anwendungen bietet. ZTNA ist eine wichtige Komponente für die Einführung eines Zero-Trust-Sicherheitsmodells, das Nutzern nur den Zugriff auf bestimmte Anwendungen (nicht auf ganze Netzwerke oder Segmente) basierend auf der Nutzeridentität gewährt. Die Lösung schützt die Nutzeridentität durch Identitäts- und Zugriffsmanagement, Multi-Faktor-Authentifizierung (MFA) und Single-Sign-on-Technologien. Durch den Einsatz eines ZTNA-Tools entfällt für Unternehmen die Komplexität der sicheren Verwaltung von Geräten oder die Aufrechterhaltung komplexer WAN- oder VPN-Konnektivität. Nach der ordnungsgemäßen Authentifizierung erhalten Nutzer nur Zugriff auf die Anwendungen und Daten, die sie benötigen. Damit werden die Angriffsfläche für Anwendungen auf null reduziert und das Risiko von unerwünschten Zugriffen minimiert. Wenn Unternehmen ein Secure Web Gateway für die

Phishing-Angriffe gegen Unternehmen sind auf dem Vormarsch

Beobachtete Angriffe, März bis Oktober 2020

ZUNAHME DER ANGRIFFE GEGEN

UNTERNEHMEN

ZUNAHME DER ANGRIFFE GEGEN

VERBRAUCHER

Quelle: Akamai Enterprise Threat Protector – Secure Web Gateway

Cloud bewerten, sollten sie die Fähigkeiten des ZTNA-Service des Anbieters berücksichtigen. Kann der Service sowohl Zugriff auf moderne Webanwendungen als auch auf ältere Anwendungen bieten, die nicht webbasiert sind? Kann der Service in den bestehenden Identity-Provider-Service des Unternehmens integriert werden? Unterstützt er die Multi-Faktor-Authentifizierung?

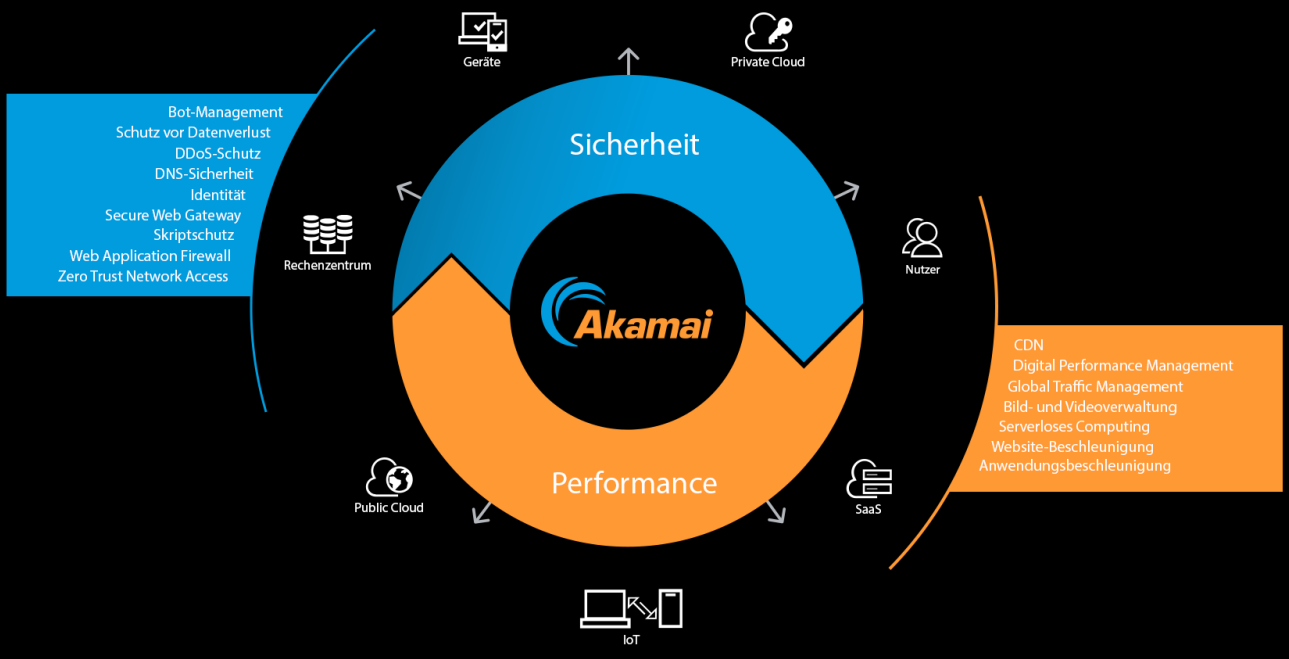
Das Secure Web Gateway sollte sich in den ZTNA-Service integrieren lassen und mit diesem Hand in Hand arbeiten, sodass ein als infiziert erkanntes Gerät keinen Zugriff auf Unternehmensanwendungen erhält. Die Protokolle eines Secure Web Gateways können durch die Erfassung von Bedrohungssignalen dazu beitragen, ein genaueres Bild der Sicherheitslage eines Geräts zu erhalten. Wenn das Gerät beispielsweise auf Command-and-Control-Server zuzugreifen versucht, sollte dies als Signal verstanden werden, den Anwendungszugriff zu beschränken, bis das Problem behoben ist.

Durch Hinzufügen von Secure Web Gateway- und ZTNA-Funktionen machen Unternehmen einen Schritt hin zur Etablierung eines SASE-Frameworks (Secure Access Service Edge). SASE verlagert das Zentrum der Sicherheitsbemühungen eines Unternehmens weg von den rechenzentrums- und hardwarebasierten Sicherheitsarchitekturen, die für heutige hochgradig verteilte Arbeits- und Geschäftsumgebungen nicht mehr funktionieren. SASE liefert stattdessen einen richtlinienbezogenen Zugriff basierend auf der Identität des Nutzers und/oder des Geräts. SASE bietet zudem eine Vielzahl zusätzlicher Sicherheitskontrollelemente, unter anderem eine Web Application Firewall, API-Schutz, Bot-Management, und DDoS-Schutz für Webanwendungen.

> **ZTNA verbessert die Flexibilität, Agilität und Skalierbarkeit des Anwendungszugriffs. So können Unternehmen erfolgreich sein, ohne dass ihre internen Anwendungen direkt über das Internet zugänglich sind – was wiederum ein geringeres Angriffsrisiko bedeutet.**
>
> – Gartner, Market Guide for Zero Trust Network Access, Steve Riley, Neil MacDonald, Lawrence Orans, 8. Juni 2020

Darüber hinaus werden Sicherheitsmaßnahmen auf der SASE-Plattform nur einen Internet-Hop vom Nutzer entfernt bereitgestellt, sodass ein Zugriff mit geringer Latenz für Nutzer, Geräte und Cloudservices von überall aus möglich ist.

Cloudbasierte SASE von Akamai



Optimale Performance

Auch wenn die Sicherheit höchste Priorität hat, darf das Nutzererlebnis nicht darunter leiden. Ein cloudbasiertes Secure Web Gateway sollte nicht nur einen tiefgehenden Verteidigungsansatz bieten, sondern auch die oben genannten Services ohne Latenzzeit bereitstellen.

Um Latenz zu vermeiden, ist eine globale Implementierung mit Points of Presence in der Nähe aller Nutzerzugriffe erforderlich. Schließlich macht es wenig Sinn, eine Form des Backhauling durch eine andere zu ersetzen.

Die Cloudplattform sollte daher eine schnelle Skalierung ermöglichen, damit das Endnutzererlebnis auch in Spitzenzeiten nicht beeinträchtigt wird. Dies ist insbesondere dann wichtig, wenn es um die Untersuchung von HTTPS-Traffic geht, der exponentiell anwächst und letztlich bis zu 100 % des gesamten Webtraffics ausmachen wird. Die Untersuchung des verschlüsselten Traffics mit minimalen Auswirkungen auf Endnutzer ist extrem wichtig, da der Großteil der Malware bereits über HTTPS verteilt wird. Die Plattform sollte zudem ein SLA mit 100-prozentiger Verfügbarkeit bieten.

> **Microsoft 365-Nutzer machen jetzt mehr als die Hälfte der 81 % aller Unternehmen aus, die auf Cloudservices umgestiegen sind.[8]**

Microsoft 365-Integration: Da viele Unternehmen Microsoft 365 als unverzichtbare Produktivitätslösung nutzen, ist es extrem wichtig, ein hohes Maß an Sicherheit und Performance für Microsoft 365 zu gewährleisten. Eine Herausforderung bei der Bereitstellung eines cloudbasierten Secure Web Gateway besteht darin, dass Microsoft 365 – wie auch viele andere beliebte SaaS-Anwendungen – schlechte Performance liefern, wenn Nutzer über einen Weiterleitungsproxy für die TLS-MITM-Prüfung auf die Anwendungen zugreifen.

Damit die Microsoft 365-Performance nicht beeinträchtigt wird, sollte das Cloud-SWG unbedingt über eine globale Edge-Plattform bereitgestellt werden, die folgende Merkmale unterstützt:

- Die Anfrage wird anhand der Quell-IP der Anfrage an das geografisch nächstgelegene Microsoft 365-Rechenzentrum weitergeleitet. Dabei werden DNS-Backhaullösungen vermieden und die Anfrage wird an den unternehmenseigenen DNS-Resolver weitergeleitet. Ein Nutzer, der beispielsweise von Singapur aus auf Microsoft 365 zugreift und an einen Microsoft 365-Server in New York weitergeleitet würde, hätte sicher kein positives Nutzererlebnis.
- Die Standorte der Secure Web Gateway-Server sollten sich in der Nähe der Microsoft 365-Rechenzentren befinden und diese Server und Rechenzentren sollten idealerweise untereinander verbunden sein.
- Die Performance lässt sich für Microsoft 365-Traffic mit einem Klick optimieren. Dazu wird eine Liste der Domains und IP-Adressen von Microsoft 365 verwendet, die von Microsoft veröffentlicht und aktualisiert werden. Anfragen an diese Domains sollten entsprechend den Microsoft-Empfehlungen direkt an Microsoft 365-Server gesendet werden. Da die Notwendigkeit entfällt, Firewalls und andere Sicherheitsprodukte manuell zu aktualisieren, wenn Microsoft neue Domains oder IP-Adressen hinzufügt, sinkt der Zeit- und Arbeitsaufwand.

Sicherheit an die Edge verlagern

Die starke Zunahme der Remote-Arbeitskräfte hat auch die Anfälligkeit für Cyberangriffe ansteigen lassen, die wiederum immer zahlreicher und schwerwiegender werden. Bei den besten cloudbasierten Secure Web Gateway-Lösungen liegt der Fokus vor allem darauf, modernen Sicherheitsanforderungen gerecht zu werden, indem sie eine umfassende Verteidigungsstrategie bieten. Sie unterstützen zudem moderne Unternehmenssicherheitsmodelle wie Zero Trust und SASE, indem sie den Zugang zum Internet für alle Nutzer sichern, unabhängig davon, wo sie sich befinden.

Ein umfassendes cloudbasiertes Secure Web Gateway sollte alle DNS- und URL-Anfragen auswerten, mehrere Verfahren zur Nutzdatenanalyse bereitstellen, Zero-Day-Phishing-Erkennung ermöglichen, verschlüsselten Traffic überprüfen, Schutz vor Datenverlust integrieren, Shadow-IT identifizieren und verwalten sowie überall und für jedes Gerät Schutz bieten – und das alles mit hoher Performance und Integration in Sicherheitstechnologien für Unternehmensanwendungen Mit einer solchen Lösung können Unternehmen die Komplexität in Bezug auf ihre Sicherheitslösungen reduzieren, kostspieliges Backhauling vermeiden, die Effizienz des Sicherheitsteams verbessern und konsistente Sicherheitsrichtlinien umsetzen.

Weitere Informationen zu Secure Internet Access, das cloudbasierte Secure Web Gateway von Akamai, sowie eine kostenlose Testversion finden Sie unter akamai.com.

1. https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2
2. https://www.helpnetsecurity.com/2020/09/02/phishing-attacks-pandemic/
3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
4. https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/
5. https://www.brinknews.com/a-global-shortage-of-cybersecurity-professionals-leaves-businesses-at-risk/
6. https://news.sophos.com/en-us/2020/02/18/nearly-a-quarter-of-malware-now-communicates-using-tls/
7. https://www.mobolize.com/2020/10/29/mobolize-announces-technology-partnership-with-akamai-to-enable-security-on-mobile-devices/
8. https://blog.goptg.com/microsoft-office-365-statistics#:~:text=According%20to%20Bitglass%2C%20usage%20of,the%20shift%20to%20cloud%20services

Akamai

Akamai unterstützt und schützt das digitale Leben. Führende Unternehmen weltweit setzen bei der Erstellung, Bereitstellung und beim Schutz ihrer digitalen Erlebnisse auf Akamai. So unterstützen wir täglich Milliarden von Menschen in ihrem Alltag, bei der Arbeit und in ihrer Freizeit. Mithilfe der am meisten verteilten Computing-Plattform – von der Cloud bis zur Edge – ermöglichen wir es unseren Kunden, Anwendungen zu entwickeln und auszuführen. So bleiben die Erlebnisse nahe beim Nutzer und Bedrohungen werden ferngehalten. Möchten Sie mehr über die Sicherheits-, Computing- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf Twitter und LinkedIn. Veröffentlicht: 06/22.