

10

PUNKTE,

auf die Sie bei Anbietern von Cloudsicherheitslösungen achten sollten

Die Suche nach dem richtigen Cloudsicherheitsanbieter ist kein einfaches Unterfangen. Viele Anbieter scheinen auf den ersten Blick gleich: ähnliche Kennzahlen, ähnliche Versprechungen. Um allerdings einen echten Vergleich ziehen zu können, müssen Sie Informationen sammeln, Fragen stellen und Details herausfinden, die viele Cloudanbieter nur ungern preisgeben.

Mithilfe dieser Liste können Sie sich anhand fundierter Informationen für den richtigen Cloudsicherheitsanbieter entscheiden, der Ihr Unternehmen vor Cyberangriffen schützt.

- 1. Erfahrung:** Wie lange ist der Anbieter schon in der Cloudsicherheitsbranche tätig? Wie viele Kunden schützt der Anbieter aktuell weltweit? (Einblicke in die globalen Angriffsvektoren sind hilfreich.) Kann der Anbieter Ihr Unternehmen im erforderlichen Umfang schützen?
- 2. Kapazität und Umfang:** Viele Cloudsicherheitsanbieter behaupten, ausreichend Umfang zu bieten. Es kommt allerdings darauf an, wie dieser gemessen wird. Finden Sie heraus, ob der Anbieter bei Bedarf skalieren kann. Fragen Sie: Bis zu welcher Größe können Sie DDoS-Angriffe handhaben? Können Sie das belegen, z. B. mit Daten von echten Angriffen auf Ihr Netzwerk?
- 3. Performance, Verteilung und Verfügbarkeit:** Bietet der Anbieter vollständig integrierte Cloudsicherheitslösungen mit einem globalen Servernetzwerk, das durch datenbasierte Algorithmen und Automatisierung gestützt wird? Können Sie zwischen DDoS-Scrubbing und CDNs wählen oder sich für beides entscheiden?
- 4. Kollektive Intelligenz:** Verfügt der Cloudsicherheitsanbieter über den Umfang und den weltweiten Traffic, um aussagekräftige Informationen bereitzustellen? Kann er diese Kompetenz so einsetzen, dass seine Kunden vor, während und nach einem Angriff davon profitieren? Nutzt der Anbieter umfassende Big-Data-Analysen, um einzelne Angreifer zu identifizieren, die auch andere Kunden bedrohen könnten?
- 5. IP-Reputation:** Welche Quellen nutzt der Cloudsicherheitsanbieter, um die Reputation von IP-Adressen zu bewerten? Einige Produkte für IP-Reputation unterscheiden sich qualitativ und verwenden eine binäre Risikobewertung: Angreifer oder kein Angreifer. Besser sind verschiedene Bewertungskriterien, die kriminelle Aktivitäten über einen bestimmten Zeitraum berücksichtigen.
- 6. Genauigkeit:** Die Behauptungen verschiedener WAF-Anbieter (Web Application Firewall) bezüglich ihrer Genauigkeit zu deuten, ist schwierig. Die Genauigkeit zweier Anbieter miteinander zu vergleichen, macht wenig Sinn, sofern nicht beide mit dem gleichen Test geprüft wurden. Finden Sie heraus, was und wer getestet wurde und wie viele Tests in das Gesamtergebnis eingeflossen sind. Es ist wichtig, dass Sie Äpfel mit Äpfeln vergleichen.
- 7. Kontinuierliche Verbesserung:** Der entscheidende Punkt für Genauigkeit ist die regelmäßige Feinabstimmung von Regeln. Nur so kann man in Bezug auf neuen Traffic immer auf dem neuesten Stand bleiben. Wie oft prüft der Cloudsicherheitsanbieter die Sicherheitsinfrastruktur – monatlich, wöchentlich oder täglich? Wie viel Traffic wird für die Prüfung verwendet?

10 Punkte, auf die Sie bei Anbietern von Cloudsicherheitslösungen achten sollten

- 8. Zeit bis zur Abwehr:** Enthält das Service Level Agreement (SLA) des Cloudsicherheitsanbieters Angaben zu Geschwindigkeit und Qualität der Abwehr oder lediglich eine Reaktionszeit? Die meisten Anbieter versprechen, innerhalb weniger Minuten zu reagieren, doch damit ist meist nur eine Untersuchung gemeint. Spezielle und vertraglich garantierte SLAs zur Abwehr sind eine greifbare Kennzahl, um das Schutzniveau genauer zu vergleichen.
- 9. Die menschliche Komponente (Security Operations Centers):** Viele Anbieter werben mit einem rund um die Uhr verfügbaren SOC. Sie müssen allerdings herausfinden, wie viele Einrichtungen Ihr Cloudsicherheitsanbieter hat, wo sich diese befinden und wie diese besetzt sind. Wie viele Personen sind gleichzeitig verfügbar? Welche Protokolle nutzt der Anbieter, um sicherzustellen, dass Sie bei einem anhaltenden Angriff auch bei Schichtwechsel geschützt sind?
- 10. Mehrschichtige/umfassende Abwehr:** Keine einzige Sicherheitslösung ist zu 100 Prozent effektiv. Basieren jedoch alle von Ihnen eingesetzten Tools auf der gleichen Technologie oder Hardware, finden Angreifer auf allen Ebenen dieselben Schwachstellen und Sicherheitslücken, was den Angriff vereinfacht. Es empfiehlt sich, mehrere branchenführende Technologien übereinanderzuschichten.

Wenn es um Internetsicherheit geht, vertrauen immer mehr Unternehmen auf die Cloud. Cloudbasierter Schutz bietet Unternehmen mehr Umfang, höhere Genauigkeit und bessere Performance als eine Vor-Ort-Lösung allein. Damit Sie eine Cloudsicherheitslösung finden, die perfekt zu Ihrer bestehenden Sicherheitsinfrastruktur passt, müssen Sie das Angebot genau verstehen.

Weitere Informationen finden Sie in dem kostenlosen E-Book von Akamai „Why Cloud? The Buyer's Guide to Cloud Security“ (Was spricht für die Cloud? Ein Kaufberater für Cloudsicherheit).



@Akamai #MobileWeb



Auf Facebook teilen



Auf LinkedIn veröffentlichen



Akamai ist der führende Anbieter von Content-Delivery-Network (CDN)-Services, die das Internet schnell, zuverlässig und sicher machen. Die leistungsstarken Lösungen von Akamai auf den Gebieten Web Performance, Mobile Performance, Cloud Security und Media Delivery revolutionieren die Art und Weise, wie Unternehmen das Nutzererlebnis von Webseiten, Web-Applikationen und Unterhaltungsangeboten für Privat- und Geschäftskunden optimieren können. Weitere Informationen zu den Akamai-Lösungen und wie das Team von Internetexperten Unternehmen dabei unterstützt, Innovationen schneller voranzutreiben, gibt es unter <http://www.akamai.de>, im Blog blogs.akamai.com oder auf Twitter unter @AkamaiDACH sowie @Akamai.

Akamai hat seinen Hauptsitz im US-amerikanischen Cambridge, Massachusetts und betreibt mehr als 57 Niederlassungen weltweit. Unser Serviceangebot und eine erstklassige Kundenbetreuung ermöglichen es Unternehmen, ihren Kunden ein bisher unerreichtes Interneterlebnis zu bieten. Die Anschriften, Telefonnummern und Kontaktdaten aller Standorte sind unter www.akamai.de/locations aufgeführt.

©2016 Akamai Technologies, Inc. Alle Rechte vorbehalten. Eine vollständige oder auszugsweise Vervielfältigung dieses Dokuments gleich welcher Art ist ohne ausdrückliche schriftliche Genehmigung nicht gestattet. Akamai und das Wellenlogo von Akamai sind eingetragene Marken. Andere im vorliegenden Text aufgeführte Marken sind Eigentum der jeweiligen Inhaber. Akamai geht davon aus, dass die im vorliegenden Text angegebenen Informationen zum Zeitpunkt ihrer Veröffentlichung korrekt sind. Diese Informationen können ohne vorherige Ankündigung geändert werden. Veröffentlicht: Dezember 2016