Akamai

WHITEPAPER

Schützen Sie Ihr Unternehmen vor fortschrittlichen Angriffen

Da IT-Umgebungen immer komplexer werden, haben sich auch Cyberangriffe weiterentwickelt, um neue Schwachstellen auszunutzen. Anwendungen, APIs, Microservices und Komponenten werden ständig erweitert und verändern die Art und Weise, wie Onlinegeschäfte getätigt werden. Leider schaffen diese Veränderungen jedoch auch neue Schwachstellen und Angriffsflächen, die Cyberkriminelle ausnutzen können. Cybersicherheitslösungen müssen sowohl innere Bedrohungen (Schutz der eigenen Daten) als auch äußere Bedrohungen (Abwehr von Ransomware, DDoS, Ressourcenüberlastung und anderen Angriffen) berücksichtigen.

Wir wissen dies aus erster Hand, da die Forscher von Akamai durchschnittlich 788 TB Daten täglich analysieren. Mit dem gewonnenen Wissen verbessern wir unsere Produkte kontinuierlich, um Sie und Ihre Nutzer vor den gefährlichsten Angreifern und fortschrittlichsten Kampagnen zu schützen, selbst wenn sich Angriffe weiterentwickeln.

Was sind die gefährlichsten Angriffe, denen Ihr Unternehmen ausgesetzt sein könnte, und wie können Sie sich auf sie vorbereiten?

Ransomware ist auf dem Vormarsch

Der Verlust des Zugriffs auf Ihre Daten – und die Daten Ihrer Kunden – ist eine der größten Bedrohungen für Ihr Unternehmen. Zwischen dem ersten Quartal 2022 und dem ersten Quartal 2023 stieg die Zahl der Ransomware-Angriffe nach dem Akamai-Bericht „Ransomware auf dem Vormarsch“ weltweit um 143 %, wobei Angreifer vor allem Zero-Day- und One-Day-Schwachstellen ausnutzten. Sie können die Wahrscheinlichkeit und die Auswirkungen fortschrittlicher Angriffe mit Segmentierung verringern.

Während Segmentierung ein architektonischer Ansatz ist, bei dem ein Netzwerk in kleinere Segmente unterteilt wird, um Performance und Sicherheit zu verbessern, ist Mikrosegmentierung eine Sicherheitstechnik, mit der Sie ein Netzwerk logisch in unterschiedliche Sicherheitssegmente bis hin zur Workload-Ebene unterteilen können. Sicherheitskontrollen und Servicebereitstellung können dann für jedes einzelne Segment definiert werden.

Akamai Guardicore Segmentation, Teil der Akamai Guardicore Platform für Zero-Trust-Sicherheit, wehrt Angriffe auf allen wichtigen Systemen ab und verhindert, dass diese sich über Ihre Assets verteilen – so genannte East-West-Bewegungen. Anschließend unterstützt es die Reaktion und Wiederherstellung, damit Sie vor Reputationsschäden, Datenverlust und Umsatzeinbußen geschützt sind.

Da es sich um eine agentenlose Mikrosegmentierungslösung handelt, kann die Akamai Guardicore Platform schnell und einfach bereitgestellt werden, ohne dass Sie physische Änderungen an Ihrem Netzwerk vornehmen müssen oder sich Gedanken darüber machen müssen, wo sich Ihre Server und Geräte befinden. Sie generiert eine interaktive visuelle Darstellung aller Verbindungen in Ihrem Netzwerk und hilft Ihnen dabei, eines der wichtigsten Hindernisse für die Bereitstellung zu überwinden: mangelnde Transparenz. Darüber hinaus hat Akamai aktive Wege entwickelt, um potenzielle Performanceengpässe und Compliance-Anforderungen anzugehen sowie Richtlinien durchzusetzen, die viele verschiedene Arten von Infrastrukturen abdecken können. So haben Sie umfassende Transparenz und granulare Kontrolle über alle Umgebungen hinweg und das alles in einer einzigen Plattform.

Akamai verfügt über unübertroffene Transparenz über den Online-Traffic in unserem stark verteilten globalen Netzwerk. Die Akamai Guardicore Platform nutzt dies, um Ihnen einen Einblick in Ihre eigene Umgebung, Ihre Ressourcen, Ihren Zugriff und Ihre Netzwerkflüsse zu bieten. Dank dieser Echtzeitinformationen können Sie sich darauf verlassen, dass Ihr Unternehmen sicher ist.

Anwendungen und APIs unter Beschuss

Wie viele Anwendungen verwendet Ihr Unternehmen? Es sind sicher mehr, als Sie denken. Das durchschnittliche Unternehmen verwendet mehr als 1.000 Anwendungen. Die starke Abhängigkeit von APIs bei fast allen Online-Transaktionen und die zunehmende Einführung von Mikroservices-basierten Architekturen führen auch dazu, dass Anwendungen komplexer werden. Leider führt der Druck, durch Innovationen schnell zu wachsen, häufig dazu, dass Unternehmen Anwendungen veröffentlichen, bevor sie auf potenzielle Sicherheitsprobleme getestet wurden, was ein erhöhtes Risiko für das gesamte Anwendungssystem bedeutet.

Laut dem jüngsten „State of the Internet“-Bericht von Akamai zielen 29 % der Angriffe weltweit auf Anwendungsprogrammierschnittstellen (APIs) ab, die das Herzstück der meisten digitalen Transformationen sind. In der Region Europa, Naher Osten und Afrika betrug der Anteil etwas über 47 %. APIs sind ein gängiges Angriffsziel für Cyberkriminelle, die sowohl traditionelle als auch API-spezifische Techniken verwenden. Bots, DDoS-Angriffe (Distributed Denial of Service) und Multi-Vektor-Angriffe müssen alle berücksichtigt werden.

Mit Akamai App & API Protector können Sie Ihren Workflow, Ihre Nutzer und Ihr Unternehmen vor schädlichen Aktivitäten und Betrug in Ihren Webanwendungen schützen. Er bietet konfigurierbaren Firewall-Schutz, der Angriffe auf Anwendungsebene abwehren kann, einschließlich solcher, die über APIs gestartet werden. Dank Echtzeit-Transparenz des Bot-Traffics können Sie verfälschte Webanalysen untersuchen, eine Überlastung des Ursprungs verhindern und Berechtigungen anpassen, um Drittanbieter- und Partner-Bots ungehinderten Zugriff zu ermöglichen.

Aber um zur ursprünglichen Frage zurückzukommen: Was ist, wenn Sie nicht alle Ihre Anwendungen und APIs kennen? Transparenz ist auch hier der Schlüssel: Akamai API Security identifiziert alle Ihre APIs, bewertet deren Risikostatus und reagiert auf Angriffe. So wird verhindert, dass Angreifer auf Ihre Daten zugreifen, schädliche Dateien auf Server laden oder Server mit großen Trafficmengen überfordern können.

Schon gewusst?

DDoS-Angriffe nahmen zwischen 2021 und 2023 um 50 % zu

Mehr als 60 % der gesamten DDoS-Angriffe im Jahr 2023 hatten eine DNS-Komponente

Schützen Sie sich vor DDoS und Ressourcenüberlastung

Wenn es ein Problem gibt, auf das Sie wirklich gefasst sein sollten, dann sind es Denial-of-Service-Angriffe. Solange es das Internet gibt, gab es auch DDoS-Angriffe – und ihre Auswirkungen sind mit allem anderen im Netz gewachsen. In den letzten Jahren sind DDoS-Angriffe immer größer, länger und ausgefeilter geworden, setzen häufig mehrere Angriffsvektoren ein und nehmen zahlreiche Ziele ins Visier. Die Zahl der hochvolumetrischen DDoS-Angriffe stieg zwischen 2021 und 2023 um 50 % und mehr als 60 % der gesamten DDoS-Angriffe im Jahr 2023 hatten eine DNS-Komponente.

Selbst die größten Unternehmen können von diesen feindlichen Botnets zerstört werden, was den Service für Millionen von Kunden beeinträchtigt und das Geschäft zum Stillstand bringt. Cyberkriminelle, Akteure aus Nationalstaaten und geopolitisch motivierte Hacktivisten nutzen große und verteilte Botnetze, um nicht nur die größten Unternehmen, sondern auch kritische Infrastruktur wie Schulen und Krankenhäuser bis hin zu Flughäfen und Versorgungsunternehmen lahmzulegen. Verheerende DDoS-Angriffe und Ressourcenüberlastungen richten sich gegen alle Ebenen, Ports, Protokolle und sogar das DNS von Unternehmen und Institutionen.

Der Schutz Ihrer Infrastruktur vor DDoS-Angriffen erfordert Bedrohungsinformationen in Echtzeit. Die von uns gesammelten Daten kommen in Prolexic zum Einsatz, unserer Lösung zum Schutz vor und zur Abwehr von DDoS-Angriffen. Prolexic schützt die zugrunde liegende digitale Infrastruktur, auf der die digitalen Anwendungen und Erlebnisse eines Unternehmens ausgeführt werden, und verhindert Angriffe über alle Ihre Ports und Protokolle – in der Cloud, vor Ort oder hybrid – bevor diese sich auf Ihr Unternehmen auswirken.

In den letzten Jahren kam es zu einem erheblichen Wiederaufleben von Angriffen auf die DNS-Infrastruktur von Unternehmen, die auf die Überlastung von Ressourcen abzielen. DNS ist das Grundelement der Online-Präsenz eines Unternehmens. Wenn das DNS-System ausfällt, verschwindet die Online-Präsenz des Unternehmens. Die Lösungen Edge DNS und Shield NS53 von Akamai reduzieren den Traffic zur Überlastung von DNS-Ressourcen an der Edge und erlaubt es nur legitime DNS-Abfragen, den Ursprung eines Kunden zu erreichen.

DDoS-Schutz ist seit langem ein wichtiger Faktor für Online-Unternehmen, da sich die Anzahl der Angriffe alle zwei Jahre verdoppelt und gleichzeitig auch die Komplexität der Angriffe zunimmt. Um Umsatzverluste zu vermeiden und das Kundenvertrauen zu sichern, ist es notwendig, alle potenziellen Schwachstellen abzusichern.

Was passiert, wenn es einen Angriff gibt?

Es ist davon auszugehen, dass jede digitale Präsenz irgendwann von einem Angriff betroffen sein wird. Ein Zweck einer Sicherheitsstrategie besteht darin, Sie vor dem Angriff zu schützen – Sie werden weniger zu einem Ziel, indem Sie kritische Ressourcen schützen, Transparenz im gesamten Netzwerk sicherstellen, damit Sie sehen können, was passiert, und die Angriffe erkennen, sobald sie beginnen.

Aber was, wenn etwas wie ein Zero-Day-Angriff passiert? Hier kommt die Verhaltensanalyse ins Spiel, die für Lösungen wie Akamai App & API Protector von zentraler Bedeutung ist.

Akamai kombiniert hochautomatisierte Lösungen und maschinelle Intelligenz mit der menschlichen Intelligenz von mehr als 225 Mitarbeitern unseres globalen Security Operations Command Center (SOCC), um die Daten, die Infrastruktur und die digitalen Erlebnisse von Endnutzern zu schützen.

Akamai prüft täglich mehr als 13 Billionen DNS-Abfragen (Domain Name System) und wehrt jedes Quartal mehr als 12 Milliarden WAF-Angriffe (Web Application Firewall) ab. Wir sehen alles und haben unsere Kunden im Blick und nutzen unsere Angriffsanalyse für stärkere Abwehr. Wir nutzen diese Bedrohungsinformationen, um unsere Lösungen reaktionsschneller und effektiver zu gestalten.

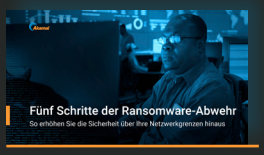
Selbst wenn Sie die Sicherheitslösungen von Akamai noch nicht nutzen, können Sie sich bei Angriffen über unsere Hotline für Cyberbedrohungen an uns wenden. Ein Sicherheitsexperte wird Sie anrufen und Sie bei den nächsten Schritten zur Angriffsabwehr unterstützen.

Sicherheit überall dort, wo Ihr Unternehmen online aktiv ist

Cyberangriffe sind zweifellos eine Gewissheit in dieser Welt. Sie können Ihr Unternehmen und Ihre Kunden jedoch mit Sicherheitslösungen schützen, die aktuelle Bedrohungsinformationen nutzen, tiefgreifende Einblicke in Ihre Anwendungen und Netzwerke bieten und sich mit der Bedrohungslandschaft weiterentwickeln.

Akamai schützt Ihr Kundenerlebnis, Ihre Systeme und Daten und integriert Sicherheit in alle von Ihnen erstellten Inhalte – überall dort, wo Sie sie erstellen und bereitstellen. Unser breites Lösungsportfolio nutzt die Bedrohungstransparenz unserer globalen Plattform und bietet branchenführende Zuverlässigkeit, sodass Sie Bedrohungen immer einen Schritt voraus sind und sich schnell an die sich ändernde Sicherheitslandschaft anpassen können.

Weitere Ressourcen



Erfahren Sie, welche fünf Schritte Sie unternehmen müssen, um die Ransomware-Kill-Chain zu unterbrechen

Verbessern Sie Ihre Hybrid-Cloud-Strategie und schützen Sie sich vor DDoS-Angriffen

Schützen Sie die wichtigsten Bausteine Ihres Unternehmens mit starker API-Sicherheit

Akamai schützt Ihr Kundenerlebnis, Ihre Mitarbeiter, Systeme und Daten und integriert Sicherheit in alle von Ihnen erstellten Inhalte – überall dort, wo Sie sie erstellen und bereitstellen. Dank der Einblicke unserer Plattform in globale Bedrohungen können Sie Ihre Sicherheitsstrategie anpassen und weiterentwickeln, um Zero Trust zu implementieren, Ransomware zu stoppen, Anwendungen und APIs zu schützen oder DDoS-Angriffe abzuwehren. Das gibt Ihnen das nötige Vertrauen, um kontinuierlich Innovationen zu entwickeln, zu expandieren und alles zu transformieren, was möglich ist. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf X (ehemals Twitter) und LinkedIn. Veröffentlicht: 06/24.