AKAMAI-PRODUKTBESCHREIBUNG

Brand Protector

Erkennen und stoppen Sie Phishing-Websites, gefälschte Shops und Markenimitationen, um Schaden für Endnutzer sowie Geschäftsverluste zu vermeiden

Sicherheitsteams haben sich lange Zeit auf den Schutz der Burg konzentriert – die Abwehr schädlicher und versteckter Angriffe auf die digitalen Assets von Organisationen. Aber nicht alle Angriffe zielen auf das Haupttor einer Organisation ab. Angreifer nutzen die langjährigen Beziehungen, die globale Marken zu ihren Kunden pflegen, um an wertvolle Anmeldedaten oder Direktzahlungen zu gelangen. Dafür treten Sie mithilfe digitaler Fälschungen als Ihre Marke auf.

Die Herausforderung besteht darin, das wertvollste Asset des Unternehmens – seinen Ruf – außerhalb seiner eigenen digitalen Domains zu schützen. Akamai Brand Protector bewahrt Unternehmen vor Umsatzverlusten und erhöhten Risiken durch den Verkauf gefälschter Waren, welche die Nachfrage und Marge senken, und schützt zudem vertrauliche Kundendaten und Kontoinformationen.

Akamai Brand Protector ist eine Komplettlösung zum Erkennen und Abwehren von gezielten Angriffen wie Phishing, Imitationen und Markenpiraterie.

Ihre bekannte Marke schafft messbaren Mehrwert – sowohl außerhalb als auch innerhalb Ihres Unternehmens. Ein höherer Markenwert führt nachweislich zu einer geringeren Kundenabwanderung und höheren Konversionsraten und Pipelines. Eine Stärkung der Marke bringt auch intern Vorteile, denn sie senkt die Mitarbeiterfluktuation und die Einstellungskosten.

Brand Protector wurde entwickelt, um betrügerische Imitationen mit einem vierstufigen Ansatz einfach und effizient zu bewältigen: Informationsgewinnung, Erkennung, Transparenz und Abwehr.

Informationsgewinnung

Die Herausforderung bei der Erkennung von Phishing- und anderen -Websites zur Markenimitation beginnt in der Phase der Informationsgewinnung und Datenerfassung.

VORTEILE FÜR IHR UNTERNEHMEN

Zuverlässige Angriffserkennung
Unser proprietäres globales Netzwerk und zusätzliche Feeds sind ein einzigartiger Vorteil bei der Erkennung von Markenimitierungen.

Kundenspezifische Transparenz
Spezielle Informationen für Ihre Marke, Produkte und Bedingungen.

Genauigkeit und Geschwindigkeit
Schnelle algorithmusgestützte Bedrohungserkennung, die häufig schon beim ersten Besuch Warnungen ausgibt und gleichzeitig die Zahl der False Positives minimiert.

Umsetzbare Erkenntnisse
Umfassende Daten werden als verwertbare Erkenntnisse bereitgestellt, wobei Risikobewertungen den Schweregrad und die Reichweite auf einen Blick zusammenfassen.

Brand Protector basiert auf der Akamai Intelligent Edge Platform. Als größte globale Edge-Plattform überblickt unsere proprietäre Sicht auf die Datenströme des Internets fast 30 % des weltweiten Traffics und analysiert jeden Tag mehr als 300 TB an Daten. Diese gewonnenen Informationen werden durch Datenfeeds von Drittanbietern erweitert, um einen umfassenden Einblick in Angriffsaktionen zu erhalten.

Mithilfe der einzigartigen Position und exklusiven Sicherheitsdatenprotokolle von Akamai sammelt die Lösung Informationen, die betrügerische Websites schneller und effizienter erkennen als andere Marktlösungen.

Erkennung

Jede Woche werden mehr als 50.000 neue Phishing-Websites erstellt. Akamai Brand Protector untersucht täglich Milliarden digitaler Aktivitäten aus internen und externen Quellen, um den Missbrauch der Marke oder der Markenelemente Ihres Unternehmens aufzudecken – und das häufig, bevor ein Angriff gestartet wird.

Transparenz

Nachdem wir die Informationen aus verschiedenen Quellen erhalten haben, werden die Datensignale durch eine Reihe heuristischer und KI-Detektoren geleitet. Obwohl eine überwältigende Menge an Daten und Beweisen erfasst wird, bietet die vereinfachte Nutzeroberfläche von Akamai einen Überblick über Echtzeitbedrohungen für Ihre Kunden in Bezug auf Imitationen.

Kundenspezifischer Traffic sowie Bedrohungserkennungen und -daten werden im Kundenportal von Akamai zu umsetzbaren Erkenntnissen zusammengeführt. Dabei werden eine Bedrohungsbewertung, eine Vertrauensbewertung und eine Bewertung des Schweregrads bereitgestellt und die Anzahl der betroffenen Nutzer für jede Erkennung quantifiziert. Sie erhalten Beweise zur Warnmeldung mit Screenshots, Erkennungsindikatoren sowie Domaindetails.

Abwehr

Integrierte Services zur Seitenschließung schließen den Kreislauf und bekämpfen Markenbetrug. Bei diesem Schritt erhält der Nutzer die automatisierte Option, Abwehrmaßnahmen anhand der gesammelten Beweise anzufordern. Nutzer können den Status im Portal einsehen und verfolgen.

VORTEILE FÜR IHR UNTERNEHMEN

Nutzerfreundlichkeit
Erhalten Sie Echtzeiteinblicke und leiten Sie innerhalb von Minuten Gegenmaßnahmen für diesen wachsenden Angriffsvektor ein.

Integrierte Seitenschließung
Nutzen Sie Ihren eigenen Service zur Seitenschließung oder machen Sie vom Service im Brand-Protector-Portal Gebrauch, um die Produktivität zu erhalten.