MARKET PERSPECTIVE

Clientseitige WAF: Die nächste Sicherheitsgrenze

Christopher Rodriguez

EXECUTIVE SNAPSHOT

ABBILDUNG 1

Executive Snapshot: Clientseitige Bedrohungen und neue Lösungen

Im Jahr 2018 haben Sicherheitsforscher eine neue Form der Cyberkriminalität identifiziert, die als Online-Skimming von Kreditkarten oder Web Skimming bezeichnet wird. Die Magecart-Angriffe nutzten den zunehmenden Trend zur Verlagerung von Anwendungsfunktionen vom Server auf den Client aus. Die Bedrohungsakteure konnten Schadcode in vertrauenswürdige Anwendungsquellen injizieren, der in den Browsern der Nutzer fernab des Schutzes einer WAF ausgeführt wurde. Letztlich erwiesen sich die Angriffe als eine lang anhaltende Datenschutzverletzung, die eine Schwachstelle in den Sicherheitspraktiken für Webanwendungen von Unternehmen aufdeckte.

Wichtige Erkenntnisse

- Clientseitige Skripte sind ein wertvolles Tool in der Anwendungsarchitektur, das ein besseres Nutzererlebnis bei gleichzeitig besserer Anwendungs-Performance, Analyse und Sicherheit bietet.
- Skripte sind allgegenwärtig. Websites verfügen heutzutage über Dutzende verschiedener Skripte, wobei zwei Drittel der Skripte von Drittanbietern stammen.
- Clientseitige Skripte bilden ein empfindliches, aber dynamisches Ökosystem von Funktionen, an dem viele Akteure beteiligt sind.
- Es gibt grundlegende Best Practices für clientseitige Sicherheit. Doch da clientseitige Sicherheit sehr komplex ist und hohe Anforderungen stellt, wird die Nachfrage nach Sicherheitslösungen für Unternehmen für diesen Bedrohungsvektor immer größer.

Empfohlene Maßnahmen

- Die auf dem Markt verfügbaren Lösungen unterscheiden sich drastisch in ihrer Funktionalität. Käufer wünschen sich ein Gleichgewicht zwischen Sicherheit und der geschäftlichen Anforderung, „nichts kaputt zu machen".
- Clientseitige Transparenz und Kontrolle sind für viele Anbieter kein einfaches oder vertrautes Terrain. Neue Marktteilnehmer werden sorgfältig abwägen, ob sie ihre eigenen Lösungen entwickeln oder sich für bestehende Lösungen entscheiden, mit deren Herstellern sie eine Partnerschaft eingehen oder die sie übernehmen.
- Viele IT-Unternehmen haben keinen Einblick in clientseitige Skripte oder Umgebungen – und noch weniger in die Sicherheitsaspekte. Es ist ein hohes Maß an Marktaufklärung einschließlich Demos, Recherchen, Machbarkeitsnachweisen und Testversionen erforderlich.

Quelle: IDC, 2021

April 2021, IDC Nr.US47623221

NEUE MARKTENTWICKLUNGEN UND -DYNAMIKEN

Diese IDC-Marktperspektive bietet eine Analyse des Bedrohungsvektors, neuer Lösungen und zukünftige clientseitige Web Application Firewalls (WAF). Akamai, Cymatic, PerimeterX und Tala Security beschreiten neue Wege, indem sie den WAF-Schutz auf clientseitige Bedrohungen ausweiten. Clientseitige Skripte erweisen sich als neuer Bedrohungsvektor und der Sicherheitsmarkt entwickelt sich ständig weiter, um diesem Bedarf gerecht zu werden.

Diese Sicherheitslösungen werden umgangssprachlich als *„Clientseitige WAF", „Anti-Scripting"* oder *„Skriptsicherheit"* bezeichnet, wobei diese Begriffe verwirrend sein können. Bedenken Sie Folgendes:

- „WAF" umfasst eine Art Paket bestehend aus Kontrollen, die für Webanwendungen gelten, während client-seitige Skripte von Natur aus einem anderen Kontrollpunkt im Paradigma der Anwendungssicherheit entsprechen.
- Schon der Begriff „Client-seitige WAF" zeigt, dass eine Verbindung zu einer gut etablierten Sicherheitskontrolle in der WAF hergestellt wird. „Skriptsicherheit" wirkt im Vergleich dazu nebulös und verwirrend.
- Der Begriff „Anti-Scripting" verallgemeinert Skripte als unerwünschte, fehlerhafte oder schlichtweg schädliche Technologie. In Wirklichkeit stellen Skripte jedoch ein wertvolles, leistungsstarkes Tool in der Anwendungsarchitektur dar.

Insgesamt bezeichnet IDC diese Lösungen vor allem wegen der mit WAF verbundenen Vorteile der Vertrautheit als „client-seitige WAF". Darüber hinaus bietet der Begriff „client-seitige WAF" die Möglichkeit einer zukünftigen Erweiterung der client-seitigen Bedrohungsarten über Skripte hinaus.

Einführung

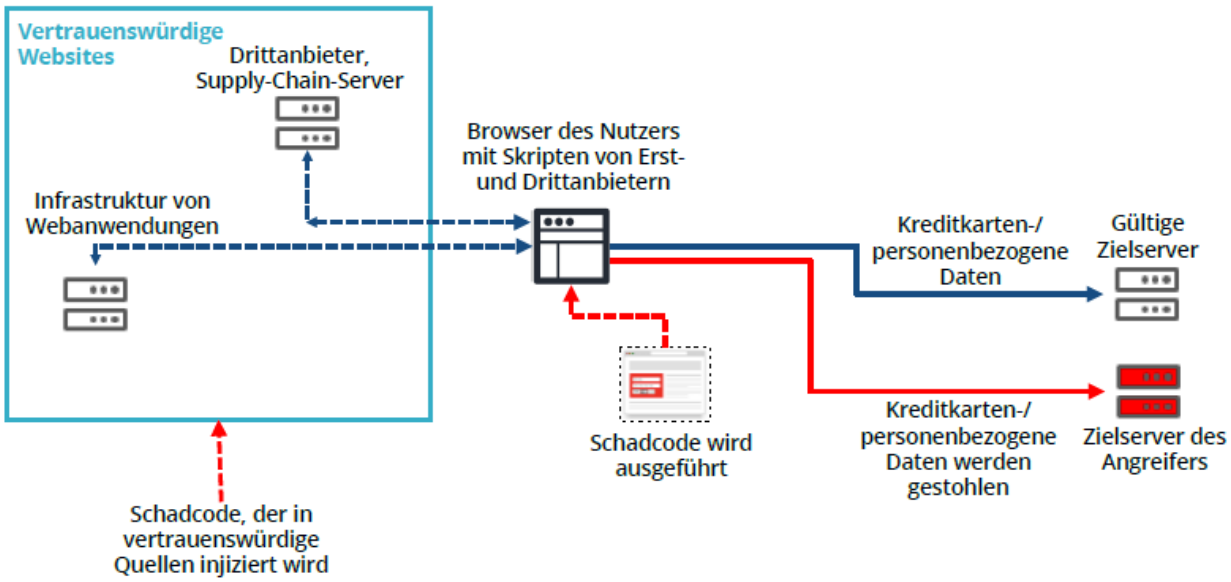
Im Jahre 2018 tauchte eine neue Technik zum Abschöpfen von Zahlungskartendaten auf, die der Hackergruppe Magecart zugeschrieben wurde. Die Magecart-Angriffe nutzten einen neuartigen Bedrohungsvektor: Skripte, die in Clientbrowsern ausgeführt werden. Nach Entdeckung der Angriffskampagne durchgeführte Untersuchungen zeigten, dass die Magecart-Gruppe die Websites großer Online-Unternehmen monatelang kompromittiert hatte, darunter Ticketmaster, NewEgg und British Airways.

Die Magecart-Kampagne nutzte client-seitige Angriffe, um Web Skimming (auch als „Online-Skimming" von Kreditkarten oder „Formjacking" bezeichnet) durchzuführen. Web Skimming ist eine sehr sichtbare Attacke dieses Bedrohungsvektors, aber der Bedrohungsvektor ermöglicht auch andere Angriffe wie Watering-Hole-Angriffe und Kryptojacking. Das Ziel dieser Angriffe kann variieren, aber die client-seitige Sicherheit bietet das Potenzial für Datendiebstahlkampagnen, die massive, langwierige Datenschutzverletzungen nach sich ziehen.

Abbildung 2 bietet einen Überblick über den Lebenszyklus eines client-seitigen Angriffs. Beachten Sie, dass der Schadcode im Browser ausgeführt wird, weit entfernt von den Schutzmechanismen einer WAF. Darüber hinaus kann Schadcode in Quellen von sowohl Drittanbietern als auch Erstanbietern injiziert werden.

ABBILDUNG 2

Aufbau eines Web-Skimming-Angriffs (im Browser)



Quelle: Akamai 2021

Branchendynamik

Die clientseitge WAF ist ein aufstrebender Markt mit starkem Wachstumspotenzial. Diese Technologie adressiert einen neuen Bedrohungsvektor, der das Ergebnis einer Verlagerung der Anwendungsentwicklungspraktiken ist. Die Anwendungsfunktionalität hat sich in den letzten Jahren von den Servern auf die Clients verlagert und es ist unwahrscheinlich, dass sich dieser Trend verlangsamen wird. Diese Verlagerung der Funktionalität vom Server auf den Client entlastet die Anforderungen an die Performance des Servers und sorgt damit für eine bessere Performance und ein interaktiveres Erlebnis für Endnutzer. Infolgedessen sind Skripte zunehmend beliebte Werkzeuge, um interaktive Online-Erlebnisse zu ermöglichen. Skripte werden für eine Vielzahl von legitimen Zwecken verwendet, einschließlich Nachverfolgung, Analyse, Nutzererlebnis und Sicherheit. Skripte sind bei Websites heute allgegenwärtig – nach manchen Schätzungen enthalten sie vielfach mehr als 15 verschiedene Skripte.

Darüber hinaus ist JavaScript so einfach, dass auch Nicht-IT-Experten immer häufiger mit Skripten arbeiten. So können Geschäftsbereiche mithilfe von Skripten außerhalb der IT-Abteilung Code für verschiedene Zwecke erstellen und in Web-Assets einfügen. Skripte ermöglichen außerdem eine einfachere Integration von Drittanbieterdiensten. Der Sicherheitsaspekt von Skripten wird jedoch weitgehend übersehen, insbesondere bei Unternehmen, die sich weiterhin auf wichtige Tools wie WAF konzentrieren.

Insgesamt besteht kein hinlängliches Verständnis für die Bedrohung. Die am häufigsten diskutierten Sicherheitsverletzungen in dieser Kategorie konzentrieren sich auf Drittanbieterskripte. Dafür liefert die Magecart-Kampagne ein anschauliches Beispiel. In diesem Fall hatten die Magecart-Hacker Zugriff auf den Code eines Zulieferers des angegriffenen Unternehmens und konnten Schadcode in vertrauenswürdige Skripte injizieren. Für einige Unternehmen mag sich der Bedrohungsvektor so anfühlen, als würde die Zielgerade für mehr Sicherheit immer weiter nach hinten verschoben. Schon jetzt ist es eine nicht triviale Aufgabe, eine Website vor den vielen verschiedenen Bedrohungen zu schützen, mit denen große Online-Unternehmen konfrontiert werden. Die Notwendigkeit, Schwachstellen in Partnersystemen zu berücksichtigen, erscheint praktisch unmöglich. Dabei sind Drittanbieterskripte am problematischsten, da IT-Organisationen weder Einblick noch Kontrolle über den Code, Updates und Änderungen der Partner haben.

Leider ist Web Skimming nur ein Teil des Problems, da Drittanbieterskripte nur ein Stück vom großen Kuchen der Skripte sind, die auf den meisten Webseiten vorhanden sind. Zur Referenz ist anzuführen, dass Researcher von Akamai geschätzt haben, dass etwa 67 % der Skripte von Drittanbietern stammen. Letztendlich sind die meisten Webseiten ein Ökosystem aus Skripten von internen Stakeholdern und Dritten. Diese internen Systeme können auch Schadcode bereitstellen, wenn die Server fremdgesteuert werden.

Es gibt einige Best Practices, die dazu beitragen können, Risiken zu minimieren. Eine strengere Kontrolle über Drittanbieterskripte ist dazu ein guter Anfang. Regelmäßige Überprüfungen von Codes und Anwendungstests sind ebenfalls zuverlässige Praktiken. Darüber hinaus können IT-Organisationen Technologien wie Subresource Integrity (SRI) nutzen, um Änderungen an Skripten zu hashen und zu erkennen. Diese Optionen können zwar eine notwendige Grundlage für den Schutz bieten, doch in der Vergangenheit hat sich gezeigt, dass hoch entwickelte Bedrohungsakteure stets fortschrittliche, intelligente Taktiken einsetzen, um eine Erkennung zu vermeiden. Daher sind SRI und andere Praktiken für den Anfang nützlich, aber gegen fortgeschrittene Angriffe nur begrenzt einsetzbar.

Darüber hinaus ist es unwahrscheinlich, dass Bedrohungsakteure ihre Bemühungen unterbrechen, wenn sie nicht dazu gezwungen werden. Seit den schlagzeilenträchtigen Magecart-Angriffen haben Hacker diese Angriffe auf vielfältige Weise verändert. So greifen sie beispielsweise jetzt gezielt Werbenetzwerke an, um Schadcode über Werbebanner einzuschleusen. Andere Mittel zielen auf Code-Repositorys wie GitHub ab. Diese Repositorys enthalten Open-Source-Bibliotheken und Code-Snippets, die in der Regel von vielen Unternehmen wiederverwendet und für die Verwendung in ihren Webanwendungen als vertrauenswürdig eingestuft sind. Diese vertrauenswürdigen Quellen dienen damit als ein potenzielles Vehikel für die Einschleusung schädlicher Skripte in ansonsten sichere Websites.

Jeder Anbieter geht das Problem etwas anders an. Die Lösungen im Markttrend werden größtenteils über JavaScript-Tags bereitgestellt, wodurch die Sicherheitsfunktion eingefügt werden kann, bevor Skripte ausgeführt werden können. Von dieser Stelle an divergieren die Lösungen erheblich. Zu den Kernfunktionen gehören in der Regel die Sichtbarkeit und Zuordnung von Skripten und Kommunikationen (z. B. Quelle und Ziel). Zusätzliche Funktionen decken das Schwachstellen-management, die Durchsetzung von Richtlinien und die Erkennung schädlicher Aktivitäten und verdächtiger Ereignisse ab. Weitergehende Funktionen sind möglich, z. B. die Verschlüsselung von Keys und eingebetteten Daten, Code-Verschleierung, Sandboxing sowie andere Abwehrmaßnahmen. Derzeit scheint der Ansatz darin zu bestehen, ausreichende Sichtbarkeit und Automatisierung von Kernsicherheitsfunktionen zu bieten. Auch wenn komplexere Erkennungsmaßnahmen im Laufe der Zeit willkommen sind, liegt der Schwerpunkt weiterhin auf der Bereitstellung ausreichender Sicherheit. Dabei dürfen weder die Enduser Experience noch andere Funktionalität der Website beeinträchtigt werden.

Beispiele von Anbietern

Derzeit sind einige kommerzielle Angebote für clientseitige WAF erhältlich, die in Umfang und Funktionalität unterschiedlich sind. Es gibt eine Handvoll Marktspezialisten, darunter Digital.ai (vormals Arxan), Source Defence, Cymatic, Tala Security und ChameleonX (2019 von Akamai übernommen). Andere verfügen über ein breites Portfolio für die Sicherheit von Webanwendungen. So hat Akamai 2020 den Page Integrity Manager als Teil seines Ansatzes zum Schutz vor Multivektor-Angriffen über ein ganzheitliches Portfolio mit Sicherheitslösungen für Webanwendungen und APIs eingeführt. In ähnlicher Weise führte PerimeterX 2019 sein Angebot als Ergänzung zur Bot-Management-Lösung für Unternehmen ein. Der jüngste Neuzugang ist Cloudflare, das seine neue Lösung im März 2021 vorstellte. IDC weist darauf hin, dass diese Unternehmen über Erfahrung im Bot-Management verfügen, mit der sie ein gewisses Maß an Vertrautheit mit clientseitigen Sicherheitssignalen geschaffen haben. Das Bot-Management ist ein anspruchsvoller Prozess und branchenführende Lösungen neigen dazu, mehrere Techniken (einschließlich JavaScript) einzusetzen, um Bot-Verhalten zu erkennen und zu kategorisieren.

Clientseitige Angriffe sind mitunter nur schwer zu erkennen. Sobald sie jedoch erkannt werden, sind diese Bedrohungen in Bezug auf die finanziellen Kosten für betroffene Unternehmen und ihre Kunden recht eindeutig. Diese Arten von Datenschutzverletzungen können beispielsweise häufig anhand der Anzahl gestohlener Kundendatensätze gemessen werden. Bestehende Wettbewerber in diesem Bereich haben ein hohes Maß an Effizienz bei der skriptbasierten Erkennung und Abwehr von Bedrohungen gezeigt. Dies führt dazu, dass sich die Bedrohungsakteure auf andere Bereiche konzentrieren, was in der Branche zu einem Versteckspiel führt. Für Angreifer besteht das Ziel darin, ungesicherte oder nicht ausreichend gesicherte Websites zu finden, um sie anzugreifen. Trotz der Sichtbarkeit der Magecart-Angriffe ist das Marktbewusstsein für den Bedrohungsvektor nach wie vor gering. Damit haben die Bedrohungsakteure ein leichtes Spiel, neue Ziele zu finden. All diese Faktoren werden wahrscheinlich das allgemeine Bewusstsein für den Bedrohungsvektor erhöhen, was die Nachfrage ankurbeln und in den kommenden Jahren weitere Unternehmen auf den Markt locken wird.

Marktstrategien

Clientseitige Bedrohungen werden große Online-Unternehmen so lange vor eine Herausforderung stellen, wie Cyberkriminelle den Angriffsvektor als profitabel erachten. Allerdings handelt es sich hierbei um einen Angriffstyp, der gezielter ist als massenhaft verbreitete Angriffe wie Ransomware. Es wird einige Zeit dauern, bis die meisten betroffenen Unternehmen skriptbasierte Angriffe erkennen und entschärfen können. Das Bewusstsein des Mainstream-Markts für diese Themen zu schärfen, kann ebenfalls Zeit und Mühe kosten. Anbieter stehen vor der Herausforderung, dieses Bewusstsein durch kontinuierliche Aufklärung, Demonstrationen und Proof-of-Concept-Tests zu steigern.

Weitere Unternehmen werden wahrscheinlich eigene Produkte und Funktionen einführen. So hat Akamai vor einem Jahr den Page Integrity Manager auf den Markt gebracht und kämpft damit gegen die wachsende Angriffsfläche, die durch Skripte in Browsern entsteht, in denen personenbezogene Daten übermittelt und abgerufen werden. Auch in diesem Bereich haben sich clientseitige Bedrohungen im Jahr 2020 deutlich ausgeweitet, da die Nutzung des Internets für Transaktionen während der Corona-Krise zugenommen hat.

Cloudflare, der jüngste Neuzugang auf dem Markt, hat die neue Lösung Cloudflare Page Shield eingeführt. Davor hat Cloudflare diesen Bedrohungsvektor über eine Technologiepartnerschaft mit Tala Security abgewehrt.

Cloudflare hat sich für die Entwicklung eigener clientseitiger Sicherheitsfunktionen entschieden. IDC merkt jedoch an, dass dieser Ansatz für andere möglicherweise nicht so einfach zu befolgen ist. Bei den meisten Anbietern auf dem Markt gingen der Entwicklung von clientseitigen WAF-Funktionen Bot-Erkennungstechniken voraus, die JavaScript-Clients nutzen. Ältere WAF-Lösungen verfügen nicht über diese Funktionen oder andere Erfahrungen mit clientseitigem Code.

Anbieter, die ihre Produktlinien für die Sicherheit von Webanwendungen und APIs weiter ausbauen, können spezialisierte Lösungen übernehmen, um dabei aufkommende Nachteile auszugleichen. Die Übernahme von ChameleonX durch Akamai ist ein Beispiel für die potenziellen Vorteile, die sich aus der Kombination von zweckbestimmten Technologien mit Cloud-Skalierung ergeben. Page Integrity Manager schützt jetzt mehr als 3,7 Milliarden Seitenaufrufe pro Monat durch die Analyse von 6,4 Milliarden Skriptausführungen täglich. Ca. 40 Millionen verdächtige und schädliche Interaktionen von Endnutzern werden wöchentlich beobachtet. Dadurch kann Akamai Echtzeit-Benachrichtigungen, Ursachenanalysen, sofortige Abwehrmaßnahmen und die Erstellung von Automatisierungsrichtlinien bereitstellen.

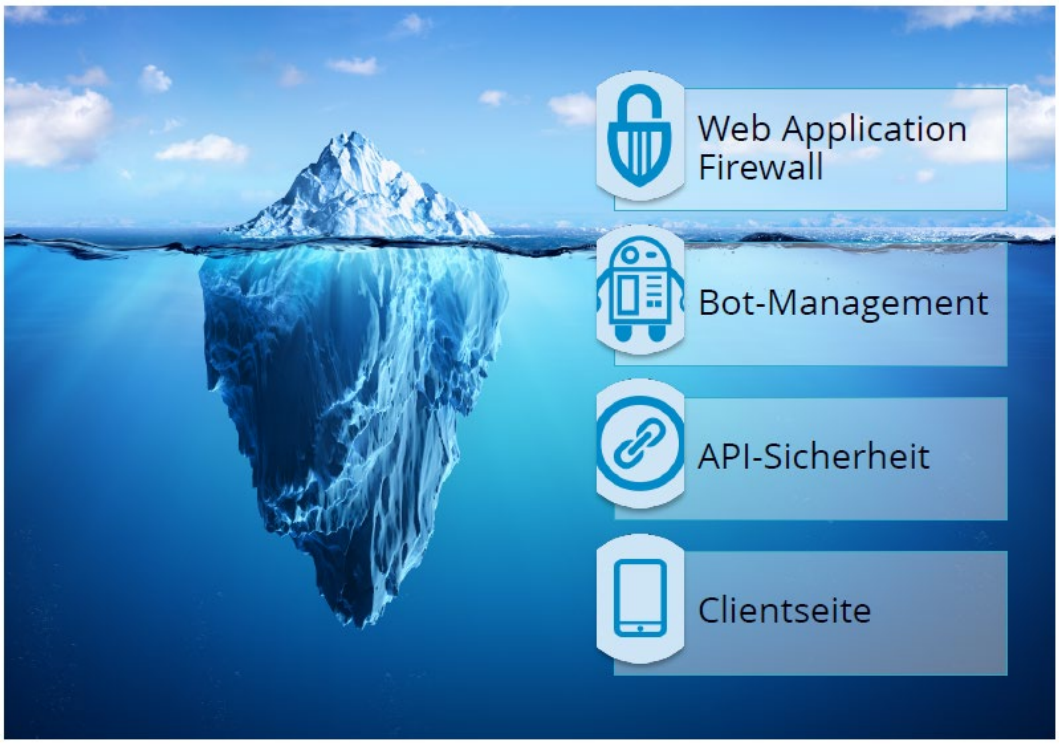
STANDPUNKT VON IDC

Clientseitige Angriffe werden eine wachsende Sicherheitslücke erzeugen, solange Cyberkriminelle den Angriffsvektor als profitabel erachten. Und das könnte noch viele Jahre lang der Fall sein. Ein wesentlicher Grund dafür besteht in der Tatsache, dass der clientseitige Bedrohungsvektor noch nicht richtig verstanden wird. Die Funktionsweise von WAF-Lösungen basiert normalerweise darauf, dass sie den Traffic von Webanwendungen analysieren, der auf den Webserver abzielt. Da JavaScript im Laufe der Jahre immer beliebter geworden ist, wurde ein großer Teil der Funktionalität in den Clientbrowser migriert. Viele Unternehmen übersehen diese Tatsache jedoch oder haben die Risiken und Sicherheitsauswirkungen dieser Migration von Webfunktionen in den Clientbrowser nicht richtig bewertet.

Diese Art von Angriff ist zielgerichteter als massenhafte verbreitete Angriffe wie Ransomware, was ebenfalls zur großen Verwirrung auf dem Markt beiträgt. Die meisten Unternehmen sind beispielsweise gut mit den Arten von Angriffen vertraut, die von WAF- und DDoS-Abwehrlösungen abgewehrt werden. Das Sicherheitsrisiko, das von unerwünschten oder schädlichen Bots ausgeht, ist eine weiteres Problem, das immer mehr ins allgemeine Bewusstsein rückt. Doch auch neuere Bereiche wie API-Sicherheit und clientseitige Sicherheit erzeugen erhebliche Risiken, die einfach nicht sichtbar sind – ganz wie die sich unter dem Wasser befindende Hälfte eines Eisbergs (siehe Abbildung 3).

ABBILDUNG 3

Eisberg der Sicherheit von Webanwendungen und APIs



Quelle: IDC, 2021

Sobald ein Unternehmen den potenziellen Bedrohungsvektor verstanden hat, kann eine neue Herkulesaufgabe auf sie zukommen: Sie müssen die Skripte, die in einer komplexen IT-Umgebung mit mehreren Domänen, Webseiten und Webanwendungen ausgeführt werden, katalogisieren und verstehen. Zum Zeitpunkt der Magecart-Angriffe musste Code manuell und zeilenweise überprüft werden, um Veränderungen und damit eingeschleuste schädliche Skripte zu erkennen. Dieser Prozess ist jetzt einfacher, da die Researcher die zugrunde liegenden Probleme und Best Practices verstehen. Dennoch benötigen die meisten angegriffenen Unternehmen Zeit, um skriptbasierte Angriffe zu erkennen und abzuwehren. Schließlich müssen sie zunächst den Bedrohungsvektor verstehen und anschließend die vorhandenen Sicherheitslücken oder Exploits identifizieren. Darüber hinaus ist der Bedrohungsvektor ein bewegliches Ziel, da jedes Quartal 75 % der Skripte geändert werden. Jede neue Änderung eröffnet die Möglichkeit, neue Schwachstellen und schädlichen Code einzuführen.

Die Zeit ist jedoch von entscheidender Bedeutung. Bereits heute waren die bekannten Sicherheitsverletzungen durch clientseitige Angriffe von langer Dauer und boten Angreifern einen monatelangen Vorsprung. In dieser Zeit wurden unzählige Kreditkarten und andere personenbezogene Daten gestohlen. Sobald ein Angriff erkannt wird, können Angreifer zum nächsten Opfer übergehen. Im Grunde genommen dauert es eine kleine Ewigkeit, bis clientseitige Angriffe entdeckt werden – ein Ungleichgewicht, das Cyberkriminellen einen enormen Vorteil verschafft und unbedingt verringert werden muss.

Die Zeit ist somit die größte Hürde für die Sicherheitsbranche, um das Bewusstsein der Käufer für das Thema zu schärfen und zu verbessern. Anbieter stehen vor der Herausforderung, dieses Bewusstsein durch kontinuierliche Aufklärung, Demonstrationen und Proof-of-Concept-Tests zu steigern. Akamai bietet beispielsweise eine kostenlose Testversion des Page Integrity Manager-Angebots an. Die Lösung bietet einen Überblick über das Skriptökosystem angegriffener Webseiten zusammen mit einer Analyse der verschiedenen Skripte, Schwachstellen und Risikofaktoren. Andere Anbieter bieten zudem Testversionen, Demonstrationen und Schulungsressourcen an.

IDC befürwortet diese Ansätze. Nichts vermittelt die Dringlichkeit einer Situation oder den Wert und die Effektivität einer Sicherheitslösung besser als ein Machbarkeitsnachweis. Für Anbieter liegen die Vorteile einer möglichen Premium-Abonnementkonversion auf der Hand. Käufer profitieren ebenfalls erheblich, denn sie erhalten Einblick in einen Bedrohungsvektor, der für die meisten Unternehmen bisher eine vollkommene Schwachstelle darstellte.

Auch in Zukunft wird IDC den clientseitigen WAF-Markt überwachen, um dessen Auswirkungen auf etablierte Märkte wie WAF, DDoS-Abwehr, Bot-Management und Schutz vor Online-Betrug zu verstehen. Sobald die Schwachstelle der clientseitigen Sicherheit erkannt ist, sind tiefere Diskussionen über die Auswirkungen der potenziellen Sichtbarkeit und Durchsetzungsfähigkeiten auf Clientseite als Sicherheitskontrollpunkt erforderlich.

WEITERE INFORMATIONEN

Verwandter Research

- *IDC FutureScape: Worldwide Future of Trust 2021 Predictions* (IDC #US46912920, Oktober 2020)
- *Pervasive Application Edge Defense: An Application-Based Framework for Trust* (IDC #US46810219, September 2020)
- *IDC Market Glance: Software-Defined Secure Access, 2Q20* (IDC #US46291520, Mai 2020)
- *Worldwide Internet Defense Forecast, 2020-2023: Infrastructure and Application Security Drive Business Value* (IDC #US46022619, Februar 2020)
- *Security Convergence at the Edge: Emerging Pervasive Data Defense and Response Platforms* (IDC #US46075520, Februar 2020)

Zusammenfassung

Diese IDC Market Perspective bietet eine Analyse des Bedrohungsvektors, neuer Lösungen und der Zukunft des clientseitigen WAF-Marktes. Nur wenige IT-Unternehmen verfügen über ein umfassendes Verständnis der Bedrohungen für clientseitige Skripte, die in ihren Webumgebungen ausgeführt werden. Cyberkriminelle haben es auf clientseitige Skripte abgesehen, um Schadcode heimlich auszuführen und so enorme finanzielle Gewinne zu erzielen. Dabei laufen sie nicht einmal Gefahr, erwischt zu werden. Da dieser Bedrohungsvektor in den kommenden Jahren immer mehr an Bedeutung gewinnt, wird die Nachfrage nach clientseitigen WAF-Lösungen für Unternehmen stetig steigen.

„Das clientseitige Skript ist die nächste Grenze für die Sicherheit. Cyberkriminelle sind nach wie vor unerbittlich auf der Suche nach lukrativen Exploits und haben eine neue Lücke in digitalen Sicherheitspaketen für Unternehmen gefunden“, so Christopher Rodriguez, Research Manager, IDC Network Security Products and Strategies.

Über IDC

International Data Corporation (IDC) ist der führende Anbieter von Marktanalysen, Beratungsservices und Events auf dem Markt der Informationstechnologien, Telekommunikation und Verbrauchertechnologien. IDC unterstützt IT-Experten, Führungskräfte und Investoren dabei, Entscheidungen zu Technologieeinkäufen und Geschäftsstrategien basierend auf Fakten zu treffen. Mehr als 1.100 IDC Analysten stellen globale, regionale und lokale Expertise zu neuen Chancen und Trends in Technologie und Branche zusammen – in über 110 Ländern weltweit. Seit über 50 Jahren bietet IDC strategische Einblicke, mit denen wir unsere Kunden dabei unterstützen, ihre Geschäftsziele zu erreichen. IDC ist eine Tochtergesellschaft von IDG, dem weltweit führenden Medien-, Research- und Eventunternehmen im Bereich Technologie.

Globaler Hauptsitz

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com