WHITEPAPER

APP-SICHERHEIT GEHT VOR

ADVANCED WAF: KOMPLEXE ANWENDUNGSBEDROHUNGEN

ERFORDERN EINE HOCHENTWICKELTE LÖSUNG

Die Bedrohungslandschaft hat sich im Vergleich zur Situation vor fünf Jahren dramatisch verändert. Die herkömmliche Web Application Firewall (WAF) war eine sehr effektive Lösung zur Abwehr von Angriffen auf Anwendungsebene, schafft es aber jetzt nicht mehr ohne Probleme, mit den hochentwickelten Fähigkeiten und der Agilität der Angreifer mitzuhalten. Häufig hinken die Signaturen den immer neuen Exploits hinterher. Selbst wenn es eine herkömmliche WAF schafft, die Bedrohung abzuwehren, kann ihre saubere Implementierung und ihr Management eine Herausforderung sein. Um die Abwehr von sich schnell entwicklenden Bedrohungen effektiv zu automatisieren, sind jetzt neue Methoden erforderlich.

Warum reichen herkömmliche WAFs nicht mehr aus?

Herkömmliche WAFs sollten das Problem verhindern, dass Code auf Web-Anwendungsservern ausgeführt wurde, der für unzählige bekannte Angriffe, speziell Cross-Site-Scripting (XSS) und SQL-Injection, anfällig war. WAFs wurden über die Jahre hinweg eingesetzt, um diese häufigen Sicherheitslücken zu schließen, wobei sich Probleme durch Falschmeldungen sowie Komplexität im Betrieb jedoch nie vermeiden ließen. Die ursprüngliche Open-Source-WAF ModSecurity ist oft Ziel von Bypass-Angriffen oder Umgehungstechniken. Sie versuchen, die größtenteils passiven, filterbasierten Mechanismen auszuschalten, die die WAF einsetzt, um böswillige Anfragen zu erkennen.

Firewalls der nächsten Generation (so genannte NGFW) verfügen zwar über „anwendungsbezogene" Funktionen und können auch einige Injection-Attacken (XSS, SQLi usw.) aufhalten, doch die NGFW setzt eine passive Filtererkennung ein und prüft nicht jede HTTP-Anfrage. Stattdessen funktioniert sie wie ein IPS (Intrusion Prevention System), nimmt also Stichproben bei den Anfragen und überprüft nur die ersten Bytes und nicht die komplette Anfrage-Payload. Bypass-Angriffe auf NGFW-Technologien kommen deshalb auf Anwendungsebene häufig vor. Zudem hat sich gezeigt, dass auf der NGFW und anderen Firewall-Technologien implementierte Reputation-Feeds für IP-Adressen bei Botnets und anderen automatisierten Bedrohungen unwirksam ist.

Die WAF-Technologie hat sich im Laufe der Jahre verbessert, nutzt aber noch immer größtenteils diese passiven, filterbasierten Methoden zur Erkennung böswilliger Payloads und zur Überprüfung der Protokolleinhaltung bei Web-Anfragen. Die betriebliche Komplexität bei der Verwaltung von WAF-Richtlinien hat zudem dazu geführt, dass viele Unternehmen einige Anwendungen nicht schützen. Bei zahlreichen spektakulären Angriffen wurde eine bekannte Anwendungsschwachstelle ausgenutzt, weil das betroffene Unternehmen die Anwendungsserver nicht patchen oder die WAF-Regel nicht schnell genug implementieren konnte.

Hinzu kommt, dass die Fortschritte bei den Automatisierungstechnologien und die einfache Verfügbarkeit von Botnets-for-Hire-Services die Erkennung von Bedrohungen deutlich erschweren. Durch Automatisierungstechnologien wie Headless Browser ist es schwierig, einen menschlichen Benutzer von einem Bot zu unterscheiden, selbst wenn CAPTCHA-Abfragen zum Einsatz kommen. Botnets bauen auf dem unerschöpflichen Fundus an einfach zu kompromittierenden IoT-Geräten, Kabelmodems und Browsern auf, wodurch die Quell-IP-Adresse für die Erkennung und Abwehr von Botnet-Angriffen nahezu nutzlos wird.

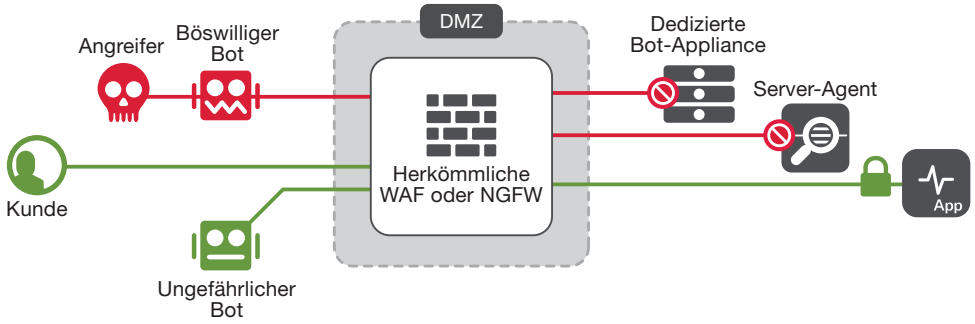

Abbildung 1: Automatisierte Bedrohungen umgehen die herkömmliche WAF und NGFW.

Hinter den Angriffen stecken heute automatisierte Bedrohungen.

Die Quelle der meisten Angriffe ist automatisiert, unabhängig von der Art der Attacken. Ob DDoS-Angriffe, Datenangriffe, Schwachstellen-Scans, Credential Stuffing, Brute Force, Resource Hoarding oder andere Angriffsarten – fast alle laufen automatisch ab. Angreifer nutzen Automatisierung, um groß angelegte Angriffe zu starten und Schwachstellen auszumachen. Dabei steht ihnen häufig weniger finanzielles Kapital und Personal zur Verfügung als den Unternehmen, die das Ziel ihrer Angriffe sind. Oft enthalten diese automatisierten Angriffe keine böswillige Payload und sind darauf ausgelegt, Abwehrmaßnahmen zu umgehen, indem sie legitimen Benutzerverkehr nachahmen.

DDoS-Angriffe auf Anwendungsebene (oder Layer 7) sind zu einem gängigeren Angriffsvektor geworden, weil sie eine ressourcenintensive URL mit legitimen Anfragen angreifen und damit ganz einfach die Anwendungsinfrastruktur überlasten können. Auf ähnliche Weise gestalten Angreifer Stuffing- (automatische Nutzung kompromittierter Benutzernamen und Passwörter) und Brute Force-Angriffe als legitime Anfragen, um die Anmeldeauthentifizierung zu umgehen. Diese Login-Attacken sind oftmals „Low-and-Slow"-Angriffe, um nicht als DoS-Angriffe erkannt zu werden.

Bei 30 bis 40 Prozent des Verkehrs auf einer normalen Website handelt es sich um böswilligen automatisierten Traffic und Bots. Wird eine Ressource auf der gleichen Seite angegriffen, sind es 90 Prozent des dortigen Verkehrs oder mehr. Das Ziel kann wie bei Brute Force oder Credential Stuffing eine Anmeldeseite oder bei einem Layer 7-DoS-Angriff eine Heavy URL sein. Bei einem Resource Hoarding-Angriff richtet der Angreifer seine Bemühungen möglicherweise auf Seiten aus, die stark nachgefragte Tickets, Turnschuhe oder andere Produkte verkaufen. Bei Scraping-Angriffen sind wiederum Daten das Ziel, die für die spätere Nutzung abgeschöpft werden. Diese gezielten Angriffe sind nicht nur schwer erkennbar, sondern verbrauchen auch unverhältnismäßig viele Infrastrukturressourcen.

Zu den Tools, die für die Automatisierung dieser Angriffe genutzt werden, zählen Headless Browser (z. B. Phantom.js und Selenium), Schwachstellen-Scanner, wie sie auch auch für Penetrationstests verwendet werden), Kommandozeilenskripte, Browser-Erweiterungen und sogar mit Malware infizierte Computer.

Das schwächste Glied in der Kette? Der Browser!

Browser sind häufig das schwächste Glied, was die Anwendungssicherheit betrifft. Angreifer versuchen, den Benutzer über gängige Phishing-Angriffe zu erreichen, die in E-Mails oder Social Media-Posts eingebettet sind. Wenn der Benutzer auf die böswilligen Links klickt, kann der Angreifer Malware auf dessen Computer/Gerät installieren. Diese Malware kann genutzt werden, um den infizierten Computer in eine Botnet-Armee aufzunehmen, in der er dann an einer der Angriffsformen beteiligt ist, die wir im vorigen Abschnitt beschrieben haben.

Häufiger kommt es jedoch vor, dass die Malware in Form eines RATs (Remote Access Trojan), eines Keyloggers oder einer anderen Methode der Datenerfassung auf den Computer gelangt. Mithilfe dieser Methoden kann der Angreifer sensible Daten wie Benutzernamen und Passwort, Kontaktlisten und andere Informationen erbeuten, die auf dem Schwarzmarkt potenziell wertvoll sind. Den Benutzer vor dem Diebstahl seiner Zugangsdaten zu schützen ist eine besonders schwierige Aufgabe, wenn der Client ein Browser oder eine mobile App ist. Diese Client-Arten bieten nur begrenzt Möglichkeiten, das gewünschte Sicherheitsniveau auf dem Endgerät durchzusetzen.

Benutzer bemerken häufig nicht, dass ihr Gerät kompromittiert ist und gehen immer noch davon aus, dass der Internetdienst ihre sensiblen Daten schützt. Die HTTPS-Verschlüsselung schützt Daten zwar bei der Übertragung, jedoch nicht, wenn sie auf dem Endgerät eingegeben werden.

Bessere Kontrollen für die Anwendungssicherheit müssen her.

Die WAF muss sich zu einer aktiven Sicherheitskontrolle entwickeln, die das Client-Endgerät überprüfen und den Sicherheitsstatus der Anwendung dynamisch verstärken kann. Wir haben gute Nachrichten: Die Advanced WAF von F5 verfügt über die geeigneten Gegenmaßnahmen, um neue Bedrohungen auf der Anwendungsebene aufzuhalten. Die Advanced WAF integriert auf hohem Niveau Verhaltensanalysen und dynamische Code Injections als ihre beiden Hauptmechanismen. Sie ermöglichen es, die Bedrohungen in Bezug auf eine vorhandene Client-Sitzung umfassender zu bewerten.

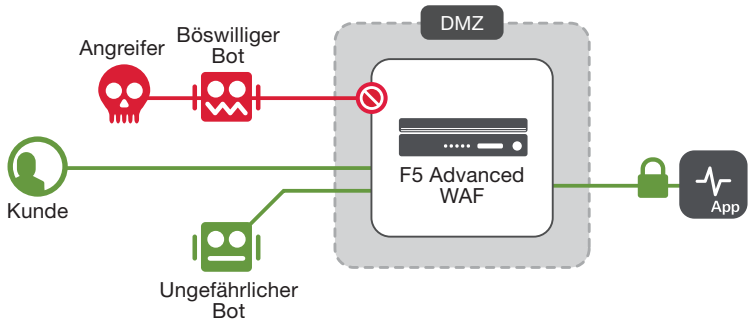

Abbildung 2: Die Advanced WAF erkennt Bots ohne Server-Agenten oder dedizierte Appliances.

Durch das Erstellen eines Basisprofils des normalen Verhaltens des Anwendungsverkehrs lassen sich anomale Traffic-Muster einfacher ermitteln. Die Automatisierung hat die Fähigkeiten der Angreifer verbessert. Diese Technologien setzen dem etwas entgegen, indem sie normalen von anomalem Verkehr so unterscheiden, wie es für einen menschlichen Sicherheitstechniker nie möglich wäre. Mittels hochentwickelter Analysefunktionen und maschinellem Lernen generiert F5 Advanced WAF dynamische Signaturen, die böswilligen Verkehr blockieren – ohne dass ein Administrator eingreifen muss.

Die Advanced WAF nutzt JavaScript Injections, um zu prüfen, ob ein Client ein Browser mit einem menschlichen Benutzer ist. Auf dieser Grundlage erstellt sie dann einen Client-Fingerabdruck, sodass Bots und andere automatisierte Tools einfacher erkennbar sind. Über einen Client-Fingerabdruck kann der Angreifer auch über die IP-Adresse hinaus verfolgt werden. Die proaktive Bot-Abwehr der Advanced WAF untersucht jede Client-Sitzung. Sie ermittelt die Art des Clients und unterscheidet ungefährliche von böswilligen Bots. Diese Vorgänge laufen für den Benutzer transparent ab, sodass die Auswirkungen auf den Benutzerkomfort, die sich durch CAPTCHA-Aufgaben ergeben, reduziert oder ganz vermieden werden.

Es kann auch Code injiziert werden, um die Tastatureingaben des Benutzers dynamisch zu verschlüsseln und ihn damit vor dem eigenen mit Malware infizierten Gerät zu schützen. Die DataSafe[1]-Technologie von F5 implementiert diesen Schutz für das Benutzernamen- und Passwortfeld und verhindert auf diese Weise den Diebstahl von Zugangsdaten. Dieser Schutz ist unverzichtbar, denn das Ziel von 86 Prozent der Angriffe auf Daten ist die Identität oder die Anwendung. Das haben Untersuchungen des F5 Labs ergeben.[2]

Da die API (d. h. die Programmierschnittstelle) sich bekanntlich oft nur schwer vor automatisierten Angriffen schützen lässt, sind die mobilen APIs verstärkt zum Angriffsziel geworden. Nur mit der Funktionalität der mobilen App anstelle eines Browsers stehen mobile App-Entwickler vor der Herausforderung, stabilere Sicherheitskontrollen zu implementieren. Mit dem neuen F5 Anti-Bot Mobile SDK[3] können Unternehmen hochentwickelte Sicherheitsfunktionen schnell mit wenigen Mausklicks in ihre vorhandenen mobilen Apps integrieren.

Das sind Ihre Vorteile, wenn Sie sich auf automatisierte Bedrohungen konzentrieren.

Wenn Unternehmen den Fokus auf automatisierte Bedrohungen richten und aktivere Gegenmaßnahmen ergreifen, können sie erhebliche Vorteile gegenüber herkömmlichen WAF-Methoden erzielen:

Verbesserungen im Betrieb

Alle Web-Anwendungen nutzen gemeinsam Browser und mobile Apps als Clients. Deshalb ist es einfacher, eine allgemeine WAF Policy für die meisten (im Idealfall alle) Web-Anwendungen einzusetzen. Web-Apps ohne WAF-Richtlinie oder auch aktives Patchen gehören der Vergangenheit an.

Geringeres Risiko

Wenn die Angreifer nicht mehr automatisch nach Schwachstellen scannen können, erhöht sich ihr Aufwand, wenn sie die neueste Schwachstelle in der Anwendungsstruktur finden wollen. Das Risiko, dass ein ungepatchter Server durch einen Zero-Day-Angriff kompromittiert wird, reduziert sich deutlich.

Bessere Nutzung der Ressourcen

Mit einer Traffic-Reduzierung um bis zu 40 Prozent werden die Betriebskosten der Anwendungsserver reduziert, insbesondere in Public Cloud-Umgebungen. Außerdem kann sich die Leistung von Anwendungsservern unter reduzierter Last verbessern, was sich wiederum positiv auf die Nutzererfahrung auswirkt. Die Reduzierung der Grundlast bedeutet auch, dass Web-Anwendungen für DDoS-Angriffe auf Anwendungsebene weniger anfällig sind.

Die hier beschriebenen Methoden sind ein Entwurf für eine neue Denkweise im Hinblick auf die Sicherheit von Web-Anwendungen. Er stellt dar, wie sich die Bedrohungslandschaft aus Sicht von F5 entwickelt. Durch einen aktiveren Sicherheitsansatz mit dem Einsatz von Tools wie der Advanced WAF können Sicherheitsverantwortliche effektivere Kontrollen einsetzen und mehr Anwendungen schützen. F5 übernimmt mit der Advanced WAF eine Vorreiterrolle, denn sie beinhaltet eine umfassende Bot-Abwehr für Web- und mobile Apps, den Schutz von Zugangsdaten im Browser und die automatische Verhaltensanalyse mittels maschinellem Lernen.

[1] https://www.f5.com/pdf/products/application-level_field_encryption_for_credential_and_data_protection.pdf

[2] https://f5.com/labs/articles/threat-intelligence/cyber-security/lessons-learned-from-a-decade-of-data-breaches

[3] https://www.f5.com/pdf/products/integrate_F5_anti-bot_mobile_SDK_with_any_mobile_app.pdf

DC0418 | WP-SEC-222132511