IP Intelligence-Dienst

DATENBLATT

Inhalt

Schutz vor schädlichem Datenverkehr

Unternehmen sind heute vielen potenziell schädlichen Angriffen von schnell wechselnden IP-Adressen ausgesetzt. Eingehender und ausgehender Datenverkehr aus Botnets, wie DDoS- (Distributed Denial-of-Service) und Malware-Angriffe, können Sicherheitsvorrichtungen überwinden und wertvolle Prozessorleistung verbrauchen.

F5® IP Intelligence nutzt externe, intelligente Dienste zur Verbesserung der automatisierten Anwendungsbereitstellung mit optimierter IP-Erkennung und stärkerem, kontextorientiertem Schutz. Durch die Erfassung von IP-Adressen und Sicherheitskategorien, die mit schädlichen Aktivitäten in Beziehung stehen, kann der IP Intelligence-Dienst dynamische Listen gefährlicher IP-Adressen für die F5 BIG-IP®-Plattform zur Verfügung stellen. Damit werden Richtlinienentscheidungen um ein kontextuelles Kriterium ergänzt. Der IP Intelligence-Dienst mindert Risiken und steigert die Effizienz von Rechenzentren, da schädlicher Datenverkehr nicht mehr verarbeitet wird.

Wichtige Vorteile

Schutz vor IP-Bedrohungen

Blockieren Sie mit Kontextsensitivität und Analysefunktionen Bedrohungen aus einer dynamischen Datenbank von IP-Adressen mit hohem Gefährdungspotenzial.

Verbesserte Transparenz bei Bedrohungen aus mehreren Quellen

Erkennen Sie schädliche Aktivitäten und IP-Adressen dank eines globalen Netzwerks aus Bedrohungssensoren und einer IP-Erkennungs-Datenbank.

Detaillierte Bedrohungsberichte und automatisierte Blockierung

Erkennen Sie die Kommunikation mit schädlichen IP-Adressen zur Erstellung effektiverer Sicherheitsrichtlinien.

Optimierung von Schutz mit Echtzeitaktualisierungen

Aktualisieren Sie die Bedrohungsdatenbank automatisch in Intervallen von fünf Minuten, um die Sicherheit des Unternehmens zu gewährleisten.

Kontextsensitivität und Schutz vor IP-Bedrohungen

Mithilfe einer regelmäßig aktualisierten Datenbank von Bedrohungsquellen und IP-Adressen mit hohem Risikopotenzial bietet IP Intelligence Kontextsensitivität. Damit und mit der Analyse von IP-Anfragen können Bedrohungen aus vielen verschiedenen Quellen im Internet erkannt werden. Der Dienst nutzt ein globales Netzwerk von Bedrohungssensoren, um schädliche Aktivitäten und IP-Adressen zu erkennen. Selbst wenn sich das BIG-IP-Gerät hinter einem Content Delivery Network (CDN) oder anderen Proxys befindet, bietet der IP Intelligence-Dienst Schutz, indem er die tatsächliche Client-IP-Adresse erkennt, die im Header „X-Forwarded-For“ (XFF) verzeichnet ist. Sie können ganz einfach Warnmeldungen konfigurieren oder Datenverkehr aus einem CDN mit gefährlichen IP-Adressen blockieren.

Schlüsselfaktor Kontextsensitivität

IP Intelligence:

- Aktualisierung der Datenbank gefährlicher IP-Adressen in Abständen von fünf Minuten
- Erkennung und Blockierung bekannter schädlicher IP-Adressen
- Erkennung und Blockierung der Kommunikation mit neuen gefährlichen IP-Adressen

Schutzkategorien

Der IP Intelligence-Dienst erfasst und sperrt IP-Adressen, die mit unterschiedlichen Bedrohungsquellen in Verbindung stehen, unter anderem in folgenden Kategorien:

Windows-Exploits: Aktive IP-Adressen, die Schadsoftware, Shell-Code, Rootkits, Würmer oder Viren anbieten oder verteilen.

Webangriffe: Cross-Site-Scripting, iFrame Injection, SQL Injection, Cross-Domain Injection oder Brute-Force-Angriffe auf Domänenkennwörter.

Botnets: Command-and-Control-Kanäle von Botnets und infizierte Zombie-Computer, die vom Bot-Master gesteuert werden.

Scanner: Ausspähen des Netzwerks durch Probes, Scannen von Hosts, Scannen von Domänen und Brute-Force-Angriffe auf Kennwörter.

Denial of Service: DoS, DDoS, SYN-Flooding und Erkennung von Anomalien im Datenverkehr.

Reputation: Verweigert bei Aktivierung den Zugriff auf IP-Adressen, die bekanntermaßen mit Malware infiziert sind oder Verteilungspunkte für Schadsoftware kontaktieren.

Phishing: IP-Adressen, auf denen Phishing-Websites oder andere Betrugsaktivitäten wie Klickbetrug oder Gaming-Betrug gehostet werden.

Proxy: IP-Adressen, die Proxy- oder Anonymisierungsdienste bereitstellen, sowie Anonymisierungsadressen von The Onion Router (TOR).

Detaillierte Bedrohungsberichte und automatisierte Blockierung

Dank aktueller Bedrohungsdaten und prädiktiver Risikoanalyse erkennt IP Intelligence eingehende und ausgehende Kommunikation mit gefährlichen IP-Adressen und ermöglicht detaillierte Bedrohungsberichte sowie automatisierte Blockierung. Mit dieser erhöhten Transparenz lassen sich verschiedene IP-Bedrohungen aufdecken, zum Beispiel Phishing-Angriffe, Attacken über anonyme Proxys, Missbrauch des TOR-Netzwerks für anonyme Online-Angriffe und sogar die ausgehende Kommunikation mit Command-and-Control-Servern von Botnets. So wird Schadsoftware in Unternehmen frühzeitig erkannt. Sind die Bedrohungen erkannt, können Sie wirksam abgewehrt werden, indem der Datenverkehr mit ausgewählten IP-Kategorien automatisch blockiert wird.

Hoch entwickelte Erkennung und Analyse von Bedrohungen

IP Intelligence nutzt eine Datenbank gefährlicher IP-Adressen und weist Bedrohungskategorien zu. Außerdem werden Netzwerkverkehr und Verhaltensdaten aller IP-Adressen gesammelt, analysiert und Bedrohungskategorien zugewiesen. So werden Bedrohungen schon in der Frühphase anhand von IP-Adressen erkannt.

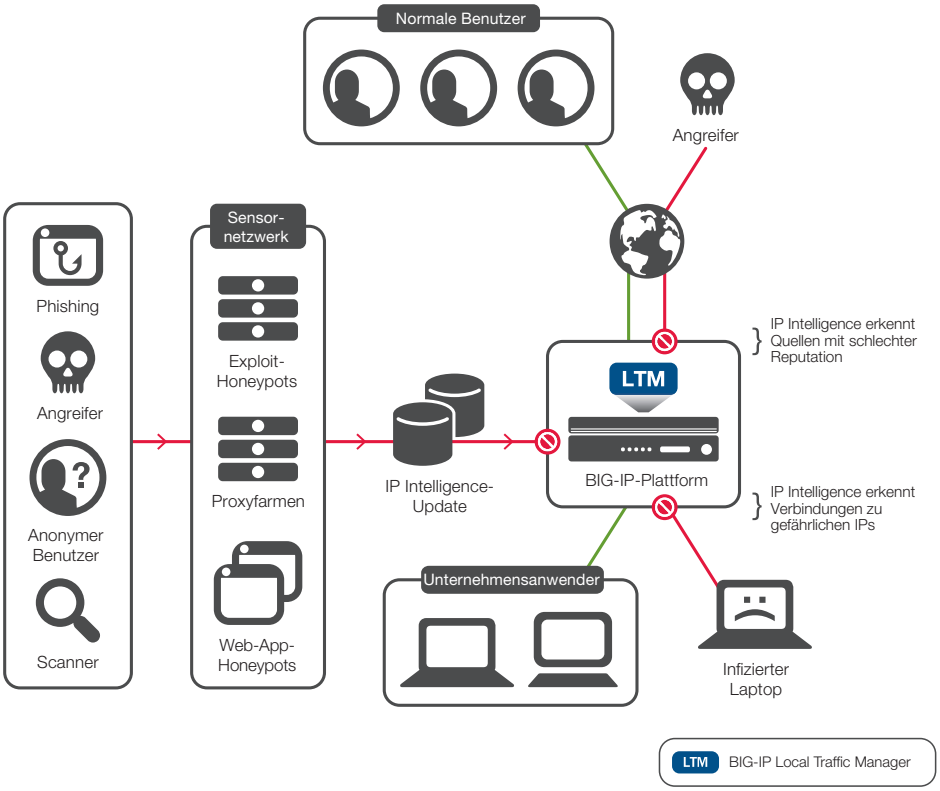

Abbildung 1: IP Intelligence erfasst IP-Adressen, vergleicht sie mit der globalen IP Intelligence-Datenbank und lässt Verbindungen zu oder blockiert diese je nach Risiko.

Bedrohungsdaten aus einer dynamischen IP Intelligence-Datenbank

IP Intelligence greift auf eine Datenbank zu, in der IP-Adressen mit hohem Risikopotenzial verzeichnet sind. Auf einem F5 BIG-IP-System kann IP Intelligence Verbindungen zu diesen Adressen entsprechend blockieren. Diese dynamische Datenbank wird in Abständen von fünf Minuten mit der Cloud synchronisiert. Dadurch sind die Bedrohungsdaten immer aktuell, das Zeitfenster für Bedrohung wird minimiert und das Unternehmen sowie dessen Reputation werden geschützt.

Durch das Erfassen und Blockieren von unerwünschtem Datenverkehr beseitigt IP Intelligence zudem einen wesentlichen Teil der Serverlast. Neu auftretende Bedrohungen werden kontinuierlich erfasst und veröffentlicht. IP-Adressen, die keine Bedrohung mehr darstellen, werden aus der Bedrohungsdatenbank entfernt. IP Intelligence sorgt für mehr Transparenz für alle Big-IP-Plattformen, ohne den Zugriff auf unbedenkliche IP-Adressen zu behindern.

Echtzeitaktualisierung für kontinuierlichen Schutz

Dank authentifiziertem Zugriff auf globale Bedrohungsdaten in der Cloud kann IP Intelligence das BIG-IP-System in Abständen von nur fünf Minuten aktualisieren. BIG-IP-Produkte können Sie ganz einfach für diese Echtzeitaktualisierungen konfigurieren. So profitieren Sie von bequemem Sicherheitsmanagement und zusätzlichen Kontextinformationen bei IP-Anfragen.

BIG-IP-Plattformen für flexible Bereitstellung

IP Intelligence ist ein Abonnementdienst, der mit der Benutzeroberfläche von BIG-IP® Application Security Manager™ (ASM) konfiguriert oder mit der Skriptsprache F5 iRules® in jede beliebige BIG-IP-Plattform integriert werden kann. Beispielsweise kann IP Intelligence mit BIG-IP® Local Traffic Manager™ (LTM) als Schutz vor einer E-Commerce- oder Finanzwebsite angeordnet werden, um Phishing-Angriffe abzuwehren. Nutzen Sie IP Intelligence zusammen mit BIG-IP ASM, um die Kontextsensitivität von Websites zu erhöhen und Anwendungen zu schützen, die Anfragen von IP-Adressen mit bekannter Schadsoftware oder Viren erhalten. Detaillierte Informationen zur Hardware finden Sie im Datenblatt zur BIG-IP-Plattform.

VIPRION-Plattformen

Der IP Intelligence-Dienst ist auch für das modulare System F5 VIPRION® verfügbar. IP Intelligence kann mit der Benutzeroberfläche von BIG-IP ASM konfiguriert oder mit iRules in jedes beliebige BIG-IP-Produkt auf der VIPRION-Plattform integriert werden. Detaillierte Informationen zur Hardware finden Sie im VIPRION-Datenblatt.

F5 Services

F5 Services bietet Support, Schulungen und Consulting der Spitzenklasse. So holen Sie das Maximum aus Ihrer Investition in F5 heraus. Sie benötigen schnell eine Antwort auf eine dringende Frage? Sie müssen interne Teams schulen? Oder Sie benötigen Unterstützung bei der Implementierung? Mit F5 Services erreichen Sie eine agile IT. Weitere Informationen zu F5 Services erhalten Sie unter f5.com/services. Persönlich erreichen Sie uns unter der Adresse consulting@f5.com.

Weitere Informationen

Besuchen Sie unsere Website f5.com und nutzen Sie die Suchfunktion, um mehr über IP Intelligence zu erfahren. Dort können unter anderem folgende Ressourcen abgerufen werden (in englischer Sprache):

Datenblätter

BIG-IP Platform

VIPRION

Whitepaper

IP Intelligence

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119, USA; Tel. (+1) 888-882-4447 www.f5.com

F5 Networks, Inc.
Unternehmenszentrale
info@f5.com

F5 Networks Ltd.
Europa/Naher Osten/Afrika
emeainfo@f5.com

F5 Networks GmbH
Lehrer-Wirth-Straße 2
81829 München
Tel. 089 94 383-0
germanyinfo@f5.com

Solutions for an application world.