DATENBLATT

Infoblox DNS Infrastructure Protection

Minimieren Sie durch DNS-basierte Angriffe verursachte Geschäftsunterbrechungen

HERAUSFORDERUNG: UNTERBRECHUNGEN DES DIENSTES

DNS ist das verborgene Backbone digitaler Operationen. Jede Website, App und jeder Benutzer verlässt sich darauf, um verbunden zu bleiben. Wenn DNS-Dienste ausfallen, kann das Millionen an Umsatzeinbußen und verlorenem Kundenvertrauen kosten. Das gilt insbesondere für die externen DNS-Dienste, die Ihre Websites, E-Mails und andere öffentlich zugängliche Anwendungen online halten. Gleichzeitig müssen externe DNS-Server dem öffentlichen Internet ausgesetzt sein, was sie zu einem ständigen Ziel von Cyberangriffen macht, darunter:

- **DDoS-Angriffe**, die Server mit massivem Datenverkehr aus mehreren Quellen überlasten und so zum Absturz von Websites führen
- **DNS-Hijacking**, bei dem Angreifer DNS-Einträge manipulieren, um den Datenverkehr auf eine bösartige Website umzuleiten
- **Cache-Poisoning**, bei dem Angreifer bösartige oder ungültige Daten in den Cache eines Netzwerks injizieren, entweder um bösartige Inhalte bereitzustellen oder Benutzer auf bösartige Websites umzuleiten
- **NXDOMAIN-Exploits**, die DNS-Server mit Abfragen für nicht existierende Domains überfluten und zu Serviceunterbrechungen führen

Darüber hinaus werden externe autoritative DNS-Einträge weltweit auf Internetservern verteilt. Wenn es einem Angreifer gelingt, sie zu ändern, kann es Stunden oder sogar Tage dauern, alle fehlerhaften Daten zu korrigieren, während dieser Zeit sind Ihre Websites und andere Online-Apps möglicherweise überhaupt nicht erreichbar.

Infoblox DNS Infrastructure Protection (früher Advanced DNS Protection) stoppt DDoS- und andere Angriffe auf DNS-Server. Dieses NIOS-Software-Add-on sorgt dafür, dass Ihre geschäftskritischen, mit dem Internet verbundenen Anwendungen am Laufen bleiben – selbst wenn die DNS-Infrastruktur stark angegriffen wird.

LÖSUNG: SCHÜTZEN SIE IHR UNTERNEHMEN VOR STÖRUNGEN DURCH DNS-BASIERTE ANGRIFFE

DNS Infrastructure Protection erkennt und blockiert kontinuierlich eine Vielzahl von Bedrohungen, die auf kritische DNS-Dienste abzielen, und verhindert, dass Angreifer die DNS-Integrität manipulieren. Es blockiert sowohl volumetrische Angriffe wie DDoS und NXDOMAIN als auch nicht-volumetrische Exploits wie DNS-Hijacking, Cache-Poisoning und andere Bedrohungen, die auf externe und interne DNS-Server abzielen.

Im Gegensatz zu Standardmethoden, die legitimen Datenverkehr blockieren können, verwendet DNS Infrastructure Protection kontinuierlich aktualisierte Informationen, um echte Bedrohungen zu identifizieren. In der Zwischenzeit wird der reale Datenverkehr aufrechterhalten, sodass Ihr Unternehmen auch bei einem Angriff auf die DNS-Infrastruktur weiterläuft.

WICHTIGE FUNKTIONEN

Reduzieren Sie Geschäftsunterbrechungen: Infoblox DNS Infrastructure Protection überwacht, erkennt und stoppt kontinuierlich alle Arten von DNS-Angriffen – einschließlich volumetrischer und nicht-volumetrischer Angriffe wie DNS-Exploits und DNS-Hijacking – und reagiert gleichzeitig auf legitime Anfragen. Es gewährleistet außerdem die DNS-Integrität, die durch DNS-Hijacking-Angriffe gefährdet werden kann. Infoblox trägt dazu bei, dass geschäftskritische Websites und Apps online und verfügbar bleiben.

Anpassung an sich entwickelnde Bedrohungen: Infoblox DNS Infrastructure Protection nutzt die Infoblox Threat Adapt™-Technologie, um den Schutz vor neuen und sich weiterentwickelnden Bedrohungen automatisch zu aktualisieren, sobald diese auftauchen. Threat Adapt wendet unabhängige Analysen und Forschungen zu sich entwickelnden Angriffstechniken an, einschließlich dessen, was die Bedrohungsspezialisten von Infoblox in Kundennetzwerken gesehen haben, um den Schutz zu aktualisieren. Es passt den Schutz automatisch an DNS-Konfigurationsänderungen an.

AKTIVIERUNG VON VERSCHLÜSSELTEM DNS (DoH UND DoT)

Die Kommunikation zwischen dem DNS-Client (Stub-Resolver) und dem lokalen DNS-Server (rekursiver Resolver) ist nicht verschlüsselt. Unverschlüsselte Kommunikation ist anfällig für das Ausspähen, Abfangen und Weiterleiten von Daten - auch bekannt als das DNS-Sicherheitsproblem der „letzten Meile". Als Reaktion darauf hat die Branche DNS over TLS (DoT) und DNS over HTTPS (DoH) eingeführt, um Datenschutz und Verschlüsselung zwischen DNS-Clients und externen Internet-DNS-Servern zu gewährleisten. Durch die Implementierung der Verschlüsselung über den DNS-Resolver in Ihrem Netzwerk behalten Sie die Kontrolle über die Netzwerkerfahrung Ihrer Benutzer und bieten gleichzeitig Sicherheit und Inhaltsfilterung gemäß Ihren Sicherheitsrichtlinien. DNS Infrastructure Protection optimiert die DNS-Verschlüsselung, sodass Sie verschlüsselte DNS over TLS- und DoH-Verbindungen in Ihrem Netzwerk beenden können.

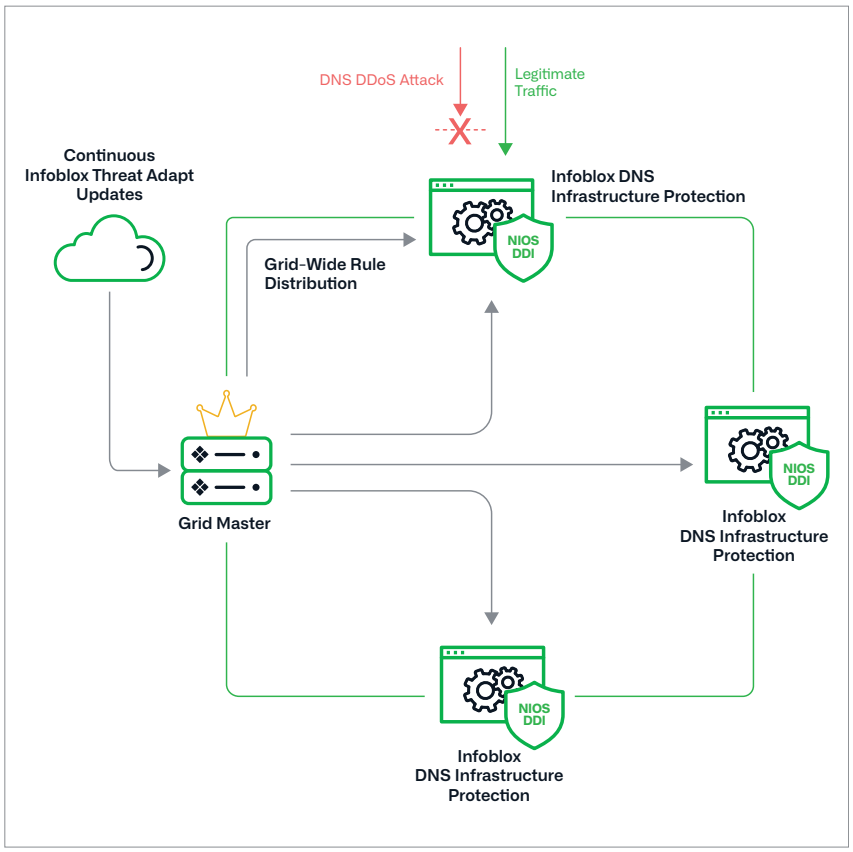

Abbildung 1: Infoblox DNS Infrastructure Protection bietet einen einzigartigen Schutz gegen DNS-basierte Angriffe

Erhalten Sie umfassende Transparenz: DNS Infrastructure Protection bietet umfassende, zentrale Transparenz in DNS-Angriffsmustern – sowohl in Echtzeit als auch im Verlauf. NetOps- und SecOps-Teams können Bedrohungsquellen verfolgen und Angriffspunkte in der gesamten Umgebung einsehen, um die Schadensbegrenzung zu beschleunigen und die Abwehr kontinuierlich zu verbessern.

Verfügbar auf physischen, virtuellen und Cloud-Plattformen: Mit Infoblox haben Sie die Möglichkeit, es als Software-Abonnement-Add-on auf virtuellen und physischen Trinzic-Geräten bereitzustellen, wodurch Dienste auf einem gemeinsamen Modell ausgeführt werden können und lokale, private sowie öffentliche Cloud-Umgebungen unterstützt werden.

WAS UNSERE KUNDEN SAGEN

„Servicevorfälle aufgrund von DDoS-Angriffen haben sich halbiert, und Kundenbeschwerden über lange Ladezeiten von Seiten sind deutlich zurückgegangen."

Vice President für Kundensupport,
Großer Dienstanbieter

„Ich verwende Infoblox seit vier Jahren für die Verwaltung von DNS, DHCP und IP-Adressen. Es ist ein solides Produkt. Wir konnten Ressourcen umverteilen, weil das Produkt so gut funktioniert. Lediglich eineinhalb Vollzeitbeschäftigte kümmern sich um die Verwaltung unserer globalen Präsenz – und das sind immerhin 65 Geräte."

Manager für globale Infrastruktur,
Adobe

TABELLE 1:
ZUSAMMENFASSUNG DER ANGRIFFSARTEN, VOR DENEN DNS INFRASTRUCTURE PROTECTION SCHÜTZT

Name des Angriffs	Typ	Wie es funktioniert
DNS-Reflexion/DDoS-Angriffe	Volumetrisch	Verwendung von DNS-Servern von Drittanbietern (offene Resolver) zur Propagierung eines DoS- oder DDoS-Angriffs
DNS-Verstärkung	Volumetrisch	Verwendung einer speziell gestalteten Abfrage zur Erstellung einer verstärkten Antwort, um das Opfer mit Datenverkehr zu überfluten
Transmission Control Protocol/ UDP/ICMP-Floods	Volumetrisch	Denial-of-Service auf Layer 3, indem ein Netzwerk oder ein Dienst durch Überflutung mit großen Datenmengen zum Absturz gebracht wird
NXDOMAIN	Volumetrisch	Überflutung des DNS-Servers mit Anfragen für nicht existierende Domänen, was zu einer Sättigung des Caches und einer langsameren Reaktionszeit führt
Zufällige Subdomain-Angriffe (Slow-Drip-Angriffe), Domain-Lock-up-Angriffe, Phantom-Domain-Angriffe	Stealth mit geringem Umfang	Überflutung des DNS-Servers mit Anfragen für Phantom-Domains oder Domains mit schlechtem Verhalten, die als Teil des Angriffs eingerichtet wurden, wodurch die Ressourcen erschöpft werden, der Cache gesättigt wird, das Limit für ausgehende Abfragen erschöpft wird und die Leistung beeinträchtigt wird
DNS-basierte Exploits	Exploits	Angriffe, die Schwachstellen in der DNS-Software ausnutzen
DNS-Cache-Poisoning	Exploits	Beschädigung der DNS-Cache-Daten durch eine betrügerische Adresse
Anomalien des Protokolls	Exploits	Verursachen eines Serverabsturzes durch das Senden fehlerhafter Pakete und Abfragen
Auskundschaftungsmaßnahmen	Exploits	Versuche von Hackern, Informationen über die Netzwerkumgebung zu erhalten, bevor sie einen großen DDoS-Angriff oder eine andere Art von Angriff starten
DNS-Hijacking	Exploits	Angriffe, die Domain-Registrierungsinformationen außer Kraft setzen, um auf einen betrügerischen DNS-Server zu verweisen
Datenexfiltration (mit bekannten Tunneln)	Exploits	Der Angriff beinhaltet das Tunneln eines anderen Protokolls durch DNS-Port 53, was erlaubt ist, wenn die Firewall so konfiguriert ist, dass sie nicht-DNS-Verkehr durchlässt—für die Zwecke der Datenexfiltration

ANWENDUNGSOPTIONEN

DNS Infrastructure Protection: Verfügbar auf physischen und virtuellen Plattformen

Infoblox DNS Infrastructure Protection verteidigt gegen ein breites Spektrum von DNS-DDoS-Angriffen und gewährleistet einen unterbrechungsfreien Dienst für Ihr Unternehmen. Es ist ein Software-Abonnement-Add-on für eine Vielzahl von Trinzic Hardware- und Software-Appliances, das Ihnen ermöglicht, die DNS-Integrität zu schützen und sowohl externe als auch interne DNS-DDoS-Angriffe zu verhindern, die Ihren Geschäftsbetrieb in lokalen, privaten und öffentlichen Cloud-Umgebungen stören könnten.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1 408 986 4000
www.infoblox.com/de

Version: 20251007v3