DATENBLATT

Infoblox advanced DNS protection

Minimieren Sie durch DNS-basierte Angriffe verursachte Geschäftsunterbrechungen

HERAUSFORDERUNG: UNTERBRECHUNGEN DES DIENSTES

Das DNS ist für jedes Unternehmen von grundlegender Bedeutung, da es die geschäftskritische Netzwerkkonnektivität bereitstellt, die für den Betrieb eines Unternehmens notwendig ist. Wenn Ihr externer DNS-Server ausfällt, ist Ihr gesamtes Netzwerk vom Internet abgeschnitten. DNS-Störungen beeinträchtigen Ihre kritischen IT-Anwendungen wie E-Mail, Websites, VoIP und Software as a Service (SaaS) oder legen sie lahm. Da ein großer Teil der Belegschaft ab 2020 aus der Ferne arbeitet, kam es zu einem enormen Anstieg der DDoS-Angriffe. DNS ist nach wie vor einer der wichtigsten Angriffsziele für DDoS, denn es ist entscheidend dafür, dass ein Unternehmen online bleibt. Neben dem Verlust des Vertrauens der Kunden können erfolgreiche DDoS-Angriffe ein Unternehmen Hunderttausende von Dollar an entgangenen Einnahmen pro Monat kosten.

Infoblox bietet den umfassendsten Schutz auf dem Markt, um Ihre lebenswichtigen DNS-Dienste vor Angriffen zu schützen, und gewährleistet so die tagtägliche Verfügbarkeit, auf die Ihr Unternehmen angewiesen ist. Es bietet einen zentralen Überblick darüber, wer das Netzwerk nutzt, auf welchen Geräten sie sich befinden und Details über den Angriff, um eine schnelle Reaktion zu gewährleisten.

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

Mit Infoblox Advanced DNS Protection (ADP) ist Ihr Unternehmen selbst bei einem DNS-basierten Angriff immer betriebsbereit. Infoblox blockiert ein breites Spektrum von Angriffen, wie z. B. volumetrische Angriffe, NXDOMAIN, Exploits und DNS-Hijacking. Im Gegensatz zu Ansätzen, die sich auf eine Überbelegung der Infrastruktur oder eine einfache Begrenzung der Antwortrate verlassen, erkennt Advanced DNS Protection auf intelligente Weise und entschärft DNS-Angriffe, indem es nur auf legitime Anfragen antwortet, indem es ständig aktualisierte Bedrohungsdaten verwendet, ohne dass Sicherheits-Patches installiert werden müssen. Mit Infoblox können Sie die Zuverlässigkeit Ihres Netzwerks auf die nächste Stufe heben, indem Sie sicherstellen, dass Ihre kritische Infrastruktur—und Ihr Unternehmen—weiterhin funktioniert, jederzeit.

WICHTIGE FUNKTIONEN

Reduzieren Sie Geschäftsunterbrechungen: Infoblox Advanced DNS Protection (ADP) überwacht, erkennt und stoppt kontinuierlich alle Arten von DNS-Angriffen - einschließlich nicht-volumetrischer Angriffe wie DNS-Exploits und DNS-Hijacking - während es auf legitime Anfragen reagiert. Außerdem wird die DNS-Integrität gewahrt, die durch DNS-Hijacking-Angriffe gefährdet werden kann. Infoblox bietet eine solide Grundlage für Sicherheit, die eine ganztägige Verfügbarkeit für Ihr Netzwerk ermöglicht.

Anpassen an sich entwickelnde Bedrohungen: Infoblox ADP 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. Dieser wird automatisch an DNS-Konfigurationsänderungen angepasst.

DOT UND DOH AKTIVIEREN

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. ADP optimiert die DNS-Verschlüsselung für unsere Hochleistungs-Paket-Engine namens Fast Path, so dass Sie verschlüsselte DoT- und DoH-Verbindungen in Ihrem Netzwerk beenden können.

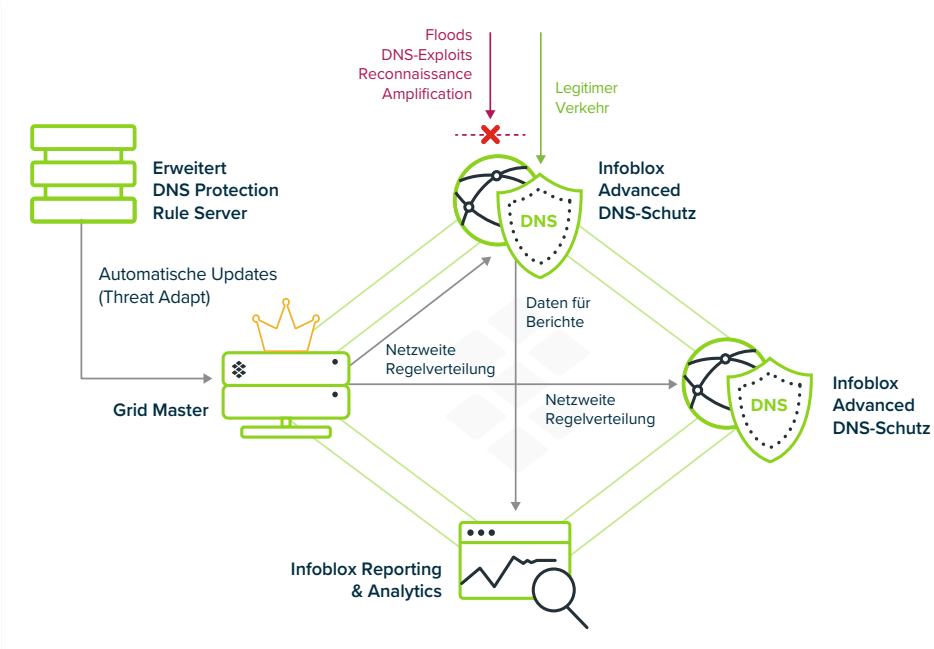

Abbildung 1: Infoblox Advanced DNS Protection bietet einen einzigartigen Schutz gegen DNS-basierte Angriffe.

HAUPTMERKMALE (FORTSETZUNG)

Gewinnen Sie Sichtbarkeit aus einem Blickwinkel:
Mit Infoblox kann Ihr Unternehmen frühere oder aktuelle DNS-Angriffe einfach einsehen und die betriebliche Effizienz durch unsere schnelle Bedrohungsbeseitigung verbessern. Infoblox Advanced DNS Protection bietet außerdem einen Überblick über die Angriffspunkte im gesamten Netzwerk und die Angriffsquellen und liefert die Informationen, die für das Bedrohungsmanagement erforderlich sind. Es ist in unsere DNS-Lösung integriert.

Flexible Bereitstellung:
Mit Infoblox haben Sie die Möglichkeit, virtuelle und physische Trinzic-Appliances im Rahmen eines Abonnements zu implementieren.

WAS UNSERE KUNDEN SAGEN

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

—VP für Kundensupport, großer Dienstleister

„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. Unsere globale Präsenz wird von 1,5 FTE verwaltet – und das sind 65 Geräte.“

—Manager of Global Infrastructure, Adobe

TABELLE 1:
ZUSAMMENFASSUNG DER ANGRIFFSARTEN, GEGEN DIE SICH ADVANCED DNS PROTECTION (ADP) VERTEIDIGT

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
TCP/UDP/ICMP Überflutung	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
Auskundschaftungs-maßnahmen	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

Software ADP: Verfügbar auf physischen und virtuellen Plattformen

Software ADP ist ein Software-Add-on für Trinzic TE-815/825/1415/1425/2215/2225/4015/4025 Appliances.

TE - 4015/4025

TE - 1415/1425

TE - 2215/2225

TE - 815/TE 825

Beginnen Sie mit einer Evaluierung

60 Tage frei Software ADP Auswertung mit temporärer Lizenz für Kunden werden über Ihre Account Manager/SEs zur Verfügung gestellt.

infoblox.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Hauptsitz der Gesellschaft
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com