DATENBLATT

Infoblox Erweiterter DNS-Schutz für Dienstanbieter

HERAUSFORDERUNG: UNTERBRECHUNGEN DES DIENSTES

CSPs, Mobilfunkbetreiber und Cloud-Anbieter verlassen sich alle in hohem Maße auf DNS, zum Teil als wesentliche Konnektivitätskomponente und zum Teil als Service, den sie ihren Kunden implizit oder explizit anbieten. CSPs müssen dieses lebenswichtige Gut schützen – für ihren Ruf und für ihre Kunden, die auf eine stabile, immer verfügbare Internetverbindung angewiesen sind. Wenn die DNS-Server ausfallen, sind Ihre Abonnenten 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.

Führenden Sicherheitsberichten zufolge ist DNS der am zweithäufigsten attackierte Dienst bei Angriffen auf der Anwendungsebene. 72 Prozent der Unternehmen waren 2018 davon betroffen. Neustar schätzt die Kosten eines über DNS durchgeführten DDoS-Angriffs (Distributed Denial of Service) auf mehr als 220.000 Dollar pro Stunde, wobei der Verlust von Abonnenten und die Schädigung von Marken nicht berücksichtigt sind. Angreifer suchen nach den schwächsten Gliedern (Angriffsvektoren) in Ihrem Netzwerk, und das DNS-Protokoll lässt sich leicht für DDoS oder DNS-Hijacking ausnutzen; solche Angriffe gefährden die Integrität des DNS.

EINE VIELZAHL VON ABWEHRMASSNAHMEN – ABER IMMER NOCH IM BLINDFLUG

Viele CSP-Netzwerke setzen eine Reihe von Tools ein, darunter Intrusion-Prevention-Systeme (IPS), Firewalls und Loadbalancing-Systeme, die verschiedene Aspekte der Infrastruktur des Anbieters schützen können. Bei DNS sind diese Tools jedoch ineffektiv, da sie nicht mit DNS-Servern integriert sind und DNS nicht beherrschen oder einsehen können.

Trotz des umfassenden Einsatzes dieser Tools beklagen viele CSPs, dass sie erst dann von Angriffen auf DNS erfahren, wenn Kunden über langsame Netzwerkleistung oder andere Beeinträchtigungen berichten. Die meisten Unternehmen haben kaum oder gar keine Frühwarnung vor Angriffen auf DNS-Systeme. Viele Betriebsteams greifen sogar auf die manuelle Analyse von DNS-Server-Protokolldaten zurück, um festzustellen, ob das Trafficaufkommen gestiegen ist und ob Server überlastet oder kompromittiert sind.

KRITISCHE BEREICHE, DIE SCHUTZ ERFORDERN

Zwei kritische Bereiche, die im Netzwerk des Providers geschützt werden müssen, sind die autoritativen DNS-Server und die DNS-Caching-Server. Autoritative DNS-Server an verschiedenen Standorten innerhalb des Netzwerks des Anbieters beantworten DNS-Anfragen und Konnektivitätsanfragen ihrer Abonnentenbasis. Autoritative DNS-Server ermöglichen Webpräsenz, E-Commerce-Funktionen und den Standort mehrerer Netzwerkkomponenten für mobile IP-Konnektivität, insbesondere Roaming und Gateway-Standort in LTE- und 5G-Netzwerken. Um ein reibungsloses Internet-Erlebnis für die

VORTEILE UND MERKMALE

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.

Anpassung 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 beobachtet haben, um den Schutz zu aktualisieren. Es passt den Schutz automatisch an Änderungen der DNS-Konfiguration an.

Teilnehmer zu gewährleisten, ist die DNS-Caching-Schicht der Schlüssel für eine schnelle Antwort auf DNS-Anfragen. Daher ist es wichtig, Abfrageantworten für häufig aufgerufene Websites und andere URLs im Cache zu halten, um akzeptable Antwortzeiten zu erreichen.

EINE NEUE VARIABLE: VERSCHLÜSSELTES DNS

Es haben sich neue verschlüsselte DNS-Standards herausgebildet, die auf der einen Seite die Privatsphäre von DNS-Anfragen und die Integrität von Antworten schützen. Auf der anderen Seite können CSPs hierbei einen Teil der Kontrolle über die DNS-Nutzung in ihren Netzwerken verlieren, wenn sie nicht ihre verschlüsselten DNS-Dienste anbieten. DNS über TLS (Transport Layer Security) oder DoT und DNS über HTTPS oder DoH verschlüsseln die DNS-Kommunikation zwischen dem Stub-Resolver Ihres Betriebssystems oder einer lokalen Anwendung und Ihrem rekursiven DNS-Resolver. Beide Technologien gewährleisten Datenschutz und Authentifizierung, indem sie die Kommunikation zwischen DNS-Clients und -Servern verschlüsseln. Dabei werden jedoch viele Lösungen dahingehend geändert, dass sie auf externe DNS-Resolver verweisen. Dadurch können Client-Geräte auf DNS-Dienste zugreifen, die sich der Kontrolle des Anbieters entziehen, und setzen den Abonnenten potenziellen Sicherheitsrisiken und negativen Kundenerfahrungen aus. Anbieter sollten jetzt Maßnahmen ergreifen, um die Risiken zu verringern, die diese Technologien darstellen. Durch die Implementierung der Verschlüsselung über den DNS-Resolver in Ihrem Netzwerk behalten Sie die Kontrolle über die Netzwerkerfahrung Ihrer Kunden. Sie ermöglicht es den Anbietern, weiterhin Sicherheit, Inhaltsfilterung und andere wichtige Dienste im Netz anzubieten.

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-Angriffe, Exploits und DNS-Hijacking. Anders als bei Methoden, die sich auf eine Überbereitstellung der Infrastruktur oder eine einfache Begrenzung der Antwortrate stützen, erkennt und entschärft ADP DNS-Angriffe auf intelligente Weise und reagiert nur auf legitime Anfragen, 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 Netzwerkinfrastruktur (und Ihr Unternehmen) zu jedem Zeitpunkt funktioniert.

UNTERSTÜTZT VERSCHLÜSSELTE DNS-STANDARDS

Infoblox Network Identity Operating System (NIOS) ist das Betriebssystem, das die zentralen Netzwerkdienste von Infoblox betreibt und den kontinuierlichen Betrieb der Netzwerkinfrastruktur gewährleistet. Infoblox Encrypted DNS for Service Providers ist eine NIOS-Funktion, die eine effiziente Verschlüsselung bietet und gleichzeitig die besten DNS- und Mehrwertdienste von Infoblox bereitstellt. Mit Unterstützung für DoT und DoH bietet Infoblox Encrypted DNS einen einzigartigen Ansatz zur Verschlüsselung Ihres DNS-Datenverkehrs. Im Gegensatz zu Methoden, die auf Load-Balancer oder Überprovisionierung setzen, läuft Infoblox Encrypted DNS als ein einziger Dienst für alle Ihre DNS-Anforderungen. Infoblox Encrypted DNS ist über virtualisierte Instanzen von ADP verfügbar und ermöglicht es Infoblox, die Last-Mile-DNS-Kommunikation zwischen seinen Endpunkten und DNS-Servern zu verschlüsseln, unabhängig davon, welches Protokoll der Endpunkt unterstützt. Es unterstützt diese Funktionalität und löst gleichzeitig Leistungsprobleme, die mit dem zusätzlichen Overhead im Zusammenhang mit verschlüsselten DNS-Kommunikationen verbunden sind. Vom selben Dienst aus ermöglichen wir CSPs, verschlüsseltes DNS mit Mikrosekunden-Latenz zu unterstützen, wenn die Verbindung bereits hergestellt ist, während alle anderen DNS-Funktionen ausgeführt werden.

VORTEILE UND MERKMALE

Einheitliche Sichtbarkeit auf einen Blick: Mit Infoblox können Kommunikationsdienstleister (CSPs) frühere oder aktuelle DNS-Angriffe problemlos einsehen und die betriebliche Effizienz durch unsere schnelle Bedrohungsbehebung verbessern. Infoblox Advanced DNS Protection bietet zudem eine einheitliche Betrachtung der Angriffsvektoren im gesamten Netzwerk und der Angriffsquellen und liefert die notwendigen Daten für das Bedrohungsmanagement. Es ist in unsere DNS-Lösung integriert.

Flexible Bereitstellung: Netzbetreiber können Infoblox Trinzic Flex virtuelle Appliances einsetzen, mit denen sie spezifische Funktionen für ihren gesamten Infoblox-Footprint hinzufügen und dabei die elastischen Skalierungsfunktionen und die anbieterspezifischen, kapazitätsbasierten Preise nutzen können.

Kostensenkung: Infoblox Software ADP nutzt vorhandene Hardware, was bedeutet, dass Kunden nur die Software aktualisieren müssen, die auf der Hardware läuft, was zu minimalen zusätzlichen Upgrade-Kosten führt.

FLEXIBLE DEPLOYMENT-OPTIONEN

Infoblox Advanced DNS Protection ist für CSP-Umgebungen konzipiert, die skalierbare Edge-Bereitstellungen erfordern. Es ist in mehreren Carrier-Grade-Optionen verfügbar, darunter orchestrierte virtualisierte Netzwerkfunktionen (VNF) und cloudnative Lösungen.

- Infoblox Trinzic Flex: eine skalierbare virtuelle Plattform, die auf den der virtuellen Maschine zugewiesenen Ressourcen basiert. Das Infoblox Network Identity Operating System (NIOS) erkennt automatisch die Kapazität der virtuellen Maschine und skaliert sie auf die entsprechende Plattform. Außerdem sind die Trinzic Flex Appliances durch das Service Provider License Agreement Program (SPLA) abgedeckt.
- Verfügbar auf physischen und virtuellen Plattformen: Software ADP ist ein Software-Abonnement-Add-on für Trinzic TE-815/825/1415/1425/ 2215/2225/4015/4025-Appliances.

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

Tabelle 1: Übersicht der Angriffstypen, gegen die Advanced DNS Protection (ADP) verteidigt

SCHUTZ VON ABONNENTEN UND IHRER MARKE

Die Lösungen auf Netzbetreiberniveau von Infoblox für Service Provider schützen Abonnenten durch den Einsatz globaler Bedrohungsdaten und automatisierter Schutzpakete. Die Lösungen gewährleisten die Verfügbarkeit kritischer DNS-Dienste in sich schnell entwickelnden Netzwerken, bei wachsendem Datenaufkommen und sogar während eines bösartigen DDoS-Angriffs.

- Infoblox Advanced DNS Protection ist die umfassendste und am besten integrierte DNS-Schutzlösung der Branche für die DNS-Infrastruktur von Dienstanbietern.
- Erweiterte, automatisierte Erkennungs- und Abwehrfunktionen für DNS-basierte Angriffe wie Amplifikation, Reflexion, Protokoll-Anomalien und Tunneling – alles in den DNS-Server integriert.
- Die Lösung auf Netzbetreiberniveau ist in verschiedenen Formfaktoren erhältlich, einschließlich orchestrierter virtualisierter Netzwerkfunktionen (VNF) und cloudnativer Lösungen. Sie bietet den weltweit schnellsten DNS-Caching-Server sowie Unterstützung für DNS-Caching und autoritative DNS-Implementierungen.
- Regeln zur Bedrohungsanalyse und Schadensbegrenzung mit automatischen Updates von Infoblox.
- Die patentierte Infoblox Grid™-Technologie bietet umfassende Kontrolle, Automatisierung und Verbreitung von Updates, um die Betriebskosten für den Support zu senken und das Risiko von Ausfällen durch manuelle Konfigurationsfehler zu eliminieren.
- Unterstützt verschlüsselte DNS-Protokolle, einschließlich DNS over TLS (DoT) und DNS over HTTPS (DoH).

Um mehr zu erfahren, besuchen Sie www.infoblox.com/sp oder kontaktieren Sie noch heute Ihren lokalen Infoblox-Vertreter.

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.

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

+1.408.986.4000
www.infoblox.com/de

© 2023 Infoblox, Inc. Alle Rechte vorbehalten. Das Infoblox-Logo und andere hier dargestellte Marken sind Eigentum von Infoblox, Inc. Alle anderen Marken sind Eigentum ihrer jeweiligen Besitzer.