DATENBLATT

Stärkung der Cybersicherheit des Bundes mit verschlüsseltem DNS

Implementierung von verschlüsseltem DNS in Übereinstimmung mit der Executive Order des Weißen Hauses

ÜBERSICHT

In einer kürzlich veröffentlichten Leitlinie hat das Weiße Haus eine umfassende Durchführungsverordnung (Executive Order, EO) erlassen, die darauf abzielt, die Cybersicherheit der Nation zu stärken und zu fördern. Die EO zielt darauf ab, die Cybersicherheit zu verbessern, indem sie die Rechenschaftspflicht für Software- und Cloud-Service-Provider verbessert, die Kommunikations- und Identitätsmanagementsysteme in de USA stärkt und den Einsatz neuer Technologien in den Exekutivabteilungen und -behörden fördert. Bemerkenswert ist unter den eingeführten Schlüsselmaßnahmen die Anforderung nach verschlüsselten DNS-Protokollen, die die Vertraulichkeit und Integrität des DNS-Verkehrs sicherstellen. Dies erkennt DNS als eine wichtige Sicherheitskontrolle an vorderster Front an und unterstreicht dessen Bedeutung für eine umfassende Cybersicherheitsstrategie.

Im Einklang mit den aktuellen Cybersicherheitsvorgaben der US-Regierung bietet Infoblox Advanced DNS Protection (ADP) starke Unterstützung für verschlüsselten DNS-Verkehr und gewährleistet die Vertraulichkeit und Integrität der DNS-Kommunikation. Diese Fähigkeit ist für US-Bundesbehörden, die ihre Cybersicherheitsmaßnahmen verbessern und den neuesten Anordnungen des Weißen Hauses zur Verschlüsselung von DNS entsprechen möchten, unerlässlich.

Die Lösungen von Infoblox sind umfassend, skalierbar und einfach zu implementieren, was einen reibungslosen Übergang zu verschlüsseltem DNS mit minimalen Unterbrechungen ermöglicht. Mehr als 15 zivile US-Bundesbehörden nutzen die DNS-Verschlüsselung von Infoblox, die in Advanced DNS Protection enthalten ist. Dies hilft ihnen, Fortschritte bei der Umsetzung des Zero-Trust-Sicherheitsrichtlinienmandats zu machen, indem sie DNS-Verschlüsselung zur Unterstützung ihrer Zero-Trust-Initiativen ermöglicht.

HERAUSFORDERUNGEN DER AGENTUR

Verschlüsseltes DNS erfordert zusätzliche Rechenressourcen, insbesondere auf DNS-Servern, da beim Senden und Empfangen von DNS-Nachrichten eine Verschlüsselung und Entschlüsselung durchgeführt werden muss. Behörden sollten dies antizipieren und sicherstellen, dass ihre DNS-Server über ausreichende Ressourcen verfügen, um die Abfragelast zu bewältigen, bevor sie mit der flächendeckenden Bereitstellung von verschlüsseltem DNS beginnen. Das Versäumnis, verschlüsseltes DNS angemessen zu implementieren, könnte den gesamten Netzwerken, ihren Anwendungen und Benutzern schaden.

Verschlüsseltes DNS kann auch die Fehlerbehebung erschweren, da IT-Mitarbeiter, die Netzwerk-Fehlerbehebungstools verwenden, keinen direkten Zugriff auf die Inhalte von DNS-Abfragen oder -Antworten haben. Die Inhalte der DNS-Anfragen

WICHTIGE FÄHIGKEITEN

Unterstützt Cybersicherheitsmandate.
Stellt die Einhaltung der neuesten US-Cybersicherheitsrichtlinien sicher.

Unterstützung für verschlüsselten DNS-Verkehr
Unterstützt DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT) für sichere und authentifizierte DNS-Kommunikation.

Erweiterter Bedrohungsschutz
Definieren und verwalten Sie Adressblöcke und Routing-Bereiche für NIOS- und Cloud-Mandanten.

Hochgeschwindigkeits-Abfrageprotokollierung
Erfasst und protokolliert DNS-Datenverkehr in Echtzeit ohne signifikante Leistungseinbußen.

Skalierbar und zuverlässig
Gewährleistet eine effiziente Verwaltung großer Mengen an DNS- und DHCP-Verkehr mit außergewöhnlicher Skalierbarkeit und Zuverlässigkeit.

und -Antworten werden den IT-Mitarbeitern natürlich weiterhin auf den Nameservern selbst zur Verfügung stehen, da diese Nameserver die erforderliche Entschlüsselung durchgeführt haben.

Um diese Herausforderungen zu bewältigen und die Cyber-Resilienz sicherzustellen, sollten Behörden die Koexistenz mehrerer missionskritischer Dienste auf einem einzigen System einschränken. Angesichts der gestiegenen Rechenanforderungen gewährleistet diese Aufgabentrennung die höchstmögliche Ausfallsicherheit. Die Infrastruktur, die den DNS-Dienst hostet, sollte ausschließlich für diese Aufgabe vorgesehen und zu diesem Zweck abgesichert werden, um die Angriffsfläche zu reduzieren und sicherzustellen, dass dem DNS-Dienst ausreichende Systemressourcen zur Verfügung stehen. Die Infrastruktur sollte über ausreichende Kapazität für Elemente des DNS-Dienstes wie Protokollierung, Unterstützung von verschlüsselten DNS-Protokollen und Schutz-DNS verfügen, wo zutreffend. Dies lässt sich möglicherweise einfacher mit speziell entwickelten DNS-Diensten erreichen, entweder als Service oder über virtuelle oder physische Geräte.

INFOBLOX ADVANCED DNS PROTECTION

Als führender Anbieter von sicheren DNS-Lösungen ist Infoblox einzigartig positioniert, um Bundesbehörden bei der Erfüllung dieser neuen Anforderungen zu unterstützen. Infoblox Advanced DNS Protection (ADP) ist ein Software-Abonnement-Add-on für verschiedene Infoblox Trinzic Hardware- und Software-Appliances. Es unterstützt verschlüsselte DNS-Protokolle wie DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT) und eignet sich daher sowohl für lokale als auch für Cloud-Umgebungen. Darüber hinaus ist ADP eine umfassende Sicherheitslösung, die entwickelt wurde, um die DNS-Infrastruktur vor einer Vielzahl von Bedrohungen zu schützen, einschließlich DDoS-Angriffen, Malware und Datenexfiltration. Dies ermöglicht es Behörden, die DNS-Integrität zu schützen und sowohl externe als auch interne DNS-DDoS-Angriffe in lokalen, privaten und öffentlichen Cloud-Umgebungen zu verhindern.

Unterstützung für verschlüsselten DNS-Verkehr

- DNS-over-HTTPS (DoH): ADP unterstützt DoH, das den DNS-Verkehr über HTTPS leitet und dabei die weit verbreitete Akzeptanz und Sicherheit von HTTPS nutzt, um DNS-Anfragen und -Antworten zu schützen.
- DNS over TLS (DoT): ADP unterstützt auch DoT, das Transport Layer Security (TLS) zur Verschlüsselung des DNS-Verkehrs verwendet. Dieses Protokoll stellt sicher, dass die DNS-Kommunikation sicher und authentifiziert ist.

Erweiterter Schutz vor Bedrohungen

ADP bietet erweiterte Bedrohungsinformationen, automatisierte Bedrohungsabwehr und Echtzeit-Einblicke in den DNS-Verkehr, wodurch die Integrität und Verfügbarkeit von DNS-Diensten sichergestellt wird.

- Überwacht, erkennt und stoppt kontinuierlich alle Arten von DNS-Angriffen – einschließlich volumetrischer Angriffe und nicht-volumetrischer Angriffe, wie DNS-Exploits und DNS-Hijacking – und reagiert gleichzeitig auf legitime Anfragen.
- Wahrt die DNS-Integrität, die durch DNS-Hijacking-Angriffe gefährdet werden kann.
- Infoblox ADP nutzt die Threat Adapt™-Technologie, um den Schutz vor aufkommenden Bedrohungen mithilfe unabhängiger Analysen und Untersuchungen automatisch zu aktualisieren und sich an Änderungen der DNS-Konfiguration anzupassen.

Hochgeschwindigkeits-Abfrage- und Antwortprotokollierung

ADP umfasst eine Hochgeschwindigkeits-Protokollierung von DNS-Abfragen und -Antworten, die für die Erfassung und Analyse des DNS-Verkehrs in Echtzeit unerlässlich ist. Es wurde für Schnelligkeit und Leichtigkeit entwickelt und bietet eine schnelle, flexible Methode zur Erfassung und Protokollierung des DNS-Datenverkehrs ohne nennenswerte Leistungseinbußen.

- Im Gegensatz zur I/O-intensiven Abfrage- und Antwortprotokollierung arbeitet dnstap asynchron, was eine schnelle Abfrageprotokollierung mit minimalem Leistungsverlust ermöglicht.
- dnstap wird genutzt, um Informationen direkt vom DNS-Server in einem flexiblen binär strukturierten Protokollformat zu puffern und diese Daten dann an einen Empfangsserver zu streamen.
- Agenturen können Big-Data-Tools einsetzen, um diese Daten zu analysieren (und sogar mit anderen Quellen zu kombinieren), um ein umfassendes Bild der Netzwerk-Nutzungsmuster zu erstellen.

Skalierbarkeit und Zuverlässigkeit

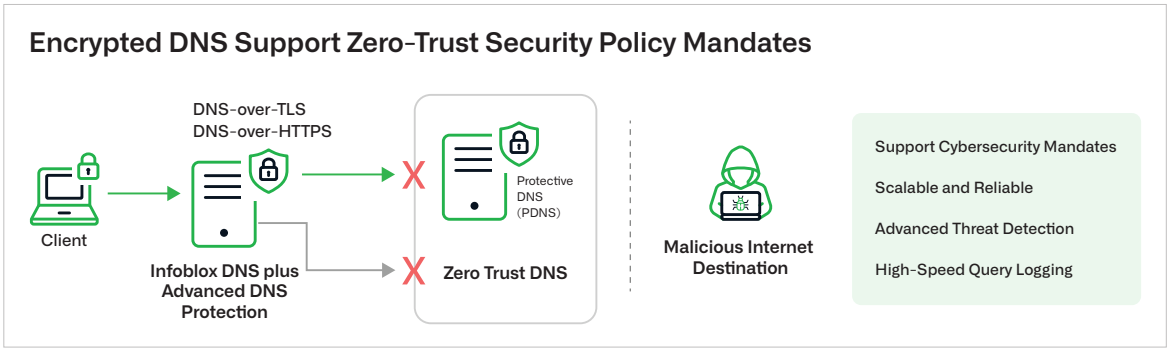
Die neuesten Infoblox Trinzic-Appliances wurden entwickelt, um außergewöhnliche Skalierbarkeit und Zuverlässigkeit zu bieten, was sie ideal für Behörden mit anspruchsvollen Netzwerkanforderungen macht.

- Entwickelt, um zukünftige Netzwerkanforderungen zu erfüllen und die neuesten Innovationen von Infoblox im Bereich Netzwerk- und Sicherheitsfortschritte zu nutzen.
- Eine Leistungssteigerung von 50 % bei DNS-Abfragen pro Sekunde (QPS) und DHCP-Leases pro Sekunde (LPS) gewährleistet eine effiziente Verwaltung großer Mengen an DNS- und DHCP-Verkehr.
- Einfacher in verteilten Architekturen bereitzustellen und zu verwalten, gewährleistet Netzwerkausfallsicherheit und Skalierbarkeit.
- Enthält zuvor lizenzierte Funktionen für die Infoblox Cloud Platform (CP) API, DNS-Firewall (DFW) RPZ-Unterstützung und DNS Traffic Control (DTC) für integrierten globalen Server-Lastausgleich.

Für weitere Informationen darüber, wie Infoblox Ihrer Organisation bei der Implementierung von verschlüsseltem DNS helfen kann, kontaktieren Sie das Infoblox-Team unter scsprogram@infobloxfederal.com oder wenden Sie sich direkt an die Kundenbetreuer.

Bereitstellungsoptionen

- ADP ist skalierbar, einfach bereitzustellen und hilft Behörden, ihre Cybersicherheitslage zu verbessern, indem ihre DNS-Infrastruktur geschützt wird. Behörden können Infoblox-DNS-Server mit aktivierter ADP-Funktion bereitstellen, um die Unterstützung für verschlüsselten DNS-Verkehr zu ermöglichen.
- Diese Bereitstellung kann vor Ort, in der Cloud oder in einer hybriden Umgebung erfolgen und bietet die Flexibilität, um verschiedene betriebliche Anforderungen zu erfüllen.



AUFRUF ZUM HANDELN

US-Behörden werden dringend aufgefordert, der DNS-Sicherheit Priorität zu geben, indem sie als Reaktion auf die jüngste Executive Order des Weißen Hauses Infoblox Advanced DNS Protection (ADP) einführen. Diese Anordnung schreibt die Verwendung verschlüsselter DNS-Protokolle vor und erkennt DNS als eine kritische Sicherheitskontrolle an der vordersten Front an. Durch die Implementierung von ADP können Behörden die Vertraulichkeit und Integrität ihres DNS-Verkehrs gewährleisten und sich so vor potenziellen Cyber-Bedrohungen schützen. Die umfassenden und skalierbaren Lösungen von Infoblox unterstützen DNS-over-HTTPS und DNS-over-TLS, wodurch der Übergang zu verschlüsseltem DNS nahtlos und effektiv wird.

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

Version: 20250203v1