LÖSUNGSHINWEIS

BEHEBUNG UNBEABSICHTIGTER HERAUSFORDERUNGEN MIT DOT UND DOH

ZUSAMMENFASSUNG

Die Sicherung Ihrer DNS-Infrastruktur war noch nie so entscheidend: Über 90 % der Malware-Vorfälle und mehr als die Hälfte aller Ransomware- und Datendiebstahlangriffe nutzen den DNS-Vektor.

Die gute Nachricht? Zwei neue und sich weiterentwickelnde Technologien zur Verbesserung der DNS-Privatsphäre machen erhebliche Fortschritte.

Die schlechte Nachricht? Diese Technologien leiten Server und Anwendungen an externe DNS-Resolver weiter, wodurch die Geräte der Teilnehmer herkömmliche DNS-Mechanismen umgehen können, um auf DNS-Dienste außerhalb Ihrer Kontrolle zuzugreifen und das Unternehmen potenziellen Sicherheitsrisiken auszusetzen. Und diese Veränderungen geschehen gerade jetzt.

Infoblox bietet Organisationen Lösungen, die diese Herausforderungen im Bereich des DNS-Datenschutzes lösen. Durch die Möglichkeit, den Zugriff auf externe DNS-Resolver zu blockieren und eine interne verschlüsselte DNS-Auflösung bereitzustellen, können Organisationen die Kontrolle über DNS behalten.

VERBESSERUNGSMÖGLICHKEITEN

Das Konzept der Offenheit ist seit der Entstehung des Internets ein grundlegendes Merkmal. Obwohl Benutzer vertrauliche Informationen wie Kreditkartennummern, E-Mail-Adressen und Passwörter zwischen ihren Webbrowsern und Websites über das sichere HTTPS-Protokoll übertragen, werden anfängliche Anfragen nach Internetadressen und nachfolgende Antworten zu Website-Standorten im Klartext übertragen. Infolgedessen hat DNS traditionell unter einem von uns als „Last Mile“-Sicherheitsproblem bezeichneten Problem gelitten. Die Kommunikation zwischen einem DNS-Client und seinem lokalen DNS-Server ist fast immer unverschlüsselt und daher anfällig für Spoofing, Abfangen, Hijacking und weitere Probleme. Obwohl in der Vergangenheit Verbesserungen vorgenommen wurden, um eine größere End-to-End-Sicherheit zu integrieren, war der letzte Abschnitt der Kommunikation mit dem Webbrowser weiterhin anfällig für Spoofing.

EINFÜHRUNG VON DNS OVER TLS UND DOH

Branchenverbände, die innerhalb der Internet Engineering Task Force (IETF) arbeiten, haben zwei Mechanismen vorgeschlagen, um diese Probleme anzugehen. Diese Mechanismen verschlüsseln die DNS-Kommunikation zwischen dem Stub-Resolver Ihres Betriebssystems oder einer lokalen Anwendung und Ihrem rekursiven DNS-Resolver. Einer ist als DNS over TLS (Transportschicht-Sicherheit) oder DoT bekannt, der andere als DNS over HTTPS oder DoH. Obwohl DoT und DoH entwickelt wurden, um DNS-Datenschutzprobleme zu lösen, führen sie auch zu erheblichen Änderungen im DNS-Verhalten von Browsern und Anwendungen. Diese Änderungen schaffen zusätzliche Komplexität und unbeabsichtigte Folgen für die Netzwerksicherheit und beeinflussen direkt die Bereitstellung von Sicherheits- und Inhaltsfilterdiensten in Unternehmen. DoT und DoH können Server und Anwendungen zu externen DNS-Resolvern leiten, wodurch Client-Geräte traditionelle DNS-Mechanismen umgehen und DNS-Dienste außerhalb Ihrer Kontrolle nutzen können, was das Unternehmen potenziellen Sicherheitsrisiken aussetzt. Ein Beispiel: Die United States National Security Agency (NSA) hat kürzlich eine Empfehlung veröffentlicht, dass Organisationen ihre eigenen DoH-Resolver hosten und vermeiden sollten, internen DNS-Verkehr an externe Drittanbieter-Resolver zu senden.

DNS ÜBER TLS (DOT)

DNS over TLS ist ein IETF-Standard, der das Transmission Control Protocol (TCP) als Verbindungs-Protokoll verwendet, um TLS-Verschlüsselung und -Authentifizierung zwischen einem DNS-Client und einem DNS-Server zu schichten. Er funktioniert oft auf Betriebssystemebene und kommuniziert über Transmission Control Protocol-Port 853. Dieser bekannte Port wird für den gesamten verschlüsselten DNS-Datenverkehr verwendet und ist den Netzwerkadministratoren sehr vertraut. Der DNS over TLS-Datenverkehr ist verschlüsselt, jedoch erleichtert die Verwendung eines bekannten Ports Netzwerkadministratoren die Überwachung und Kontrolle verschlüsselter DNS, sobald diese auftreten. DNS over TLS ist außerdem ein ausgereifter Standard, der von etablierten Akteuren der DNS-Branche unterstützt wird.

DNS ÜBER HTTPS (DOH)

DoH wird von Apple, Microsoft, der Mozilla Foundation und Chromium Projects unterstützt und ist das andere IETF-Sicherheitsprotokoll, das sich mit der Kommunikationssicherheit von DNS-Clients und DNS-Servern befasst. Es nutzt die Sicherheitsprotokollerweiterung HTTPS zur Verschlüsselung und Authentifizierung zwischen einem DNS-Client und -Server.

Ein potenzielles Problem mit DoH ist, dass es denselben Transmission Control Protocol-Port (443) verwendet, den der gesamte HTTPS-Verkehr nutzt. Es könnte sich als schwierig erweisen, DoH-bezogene DNS-Probleme zu beheben, da DoH-basierte DNS-Anfragen nicht von regulären HTTPS-Anfragen unterschieden werden können. Ein Beispiel: Wenn ein Netzwerkadministrator DNS-Überwachung einsetzt, um DNS-Anfragen an bekannte bösartige Domains zu blockieren, würde er oder sie diese Anfragen im HTTPS-Protokoll nicht sehen. Daher würde dieser bösartige Datenverkehr unentdeckt bleiben.

Darüber hinaus wird DoH häufig auf der Anwendungsebene und nicht im Betriebssystem implementiert, wodurch die Möglichkeit besteht, dass Browserverkehr die DNS-Kontrollen des Unternehmens umgeht. Die Umgehung von DNS-Kontrollen könnte die Fähigkeit des Support-Teams beeinträchtigen, die von Unternehmen geforderte Netzwerkleistung, Sicherheit, Skalierbarkeit und Zuverlässigkeit des DNS aufrechtzuerhalten.

HERAUSFORDERUNGEN FÜR UNTERNEHMEN IM BEREICH DNS OVER TLS UND DOH

Netzwerk- und Sicherheitsadministratoren verlassen sich auf DNS als ein bedeutendes Element der Netzwerkkontrollebene, um schnellen Anwendungszugriff zu gewährleisten und Benutzer vor Malware und anderen internetbasierten Bedrohungen zu schützen. Zu den bemerkenswerten Herausforderungen, denen Netzwerk- und Sicherheitsteams aufgrund der neuen DNS over TLS- und DoH-Standards gegenüberstehen könnten, gehören:

- **Zentralisiertes DNS:** Die externe Kontrolle von DNS kann es Clients ermöglichen, zentralisierte DNS-Resolver zu verwenden, die von Dritten kontrolliert und nicht von der IT bereitgestellt werden, was Risiken einführt und die effektive Verwaltung und Sicherung von Netzwerkressourcen potenziell erschwert.
- **Umgehung von Unternehmenskontrollen:** DoH bietet speziell das Potenzial, dass Hunderte von Anwendungen und Websites, jede mit ihren eigenen DoH-Einstellungen, DNS-Kontrollen umgehen können. Abgesehen davon, dass die Überwachung von DNS-Exploits wie DNS-Hijacking durch DoH erschwert wird, könnte DoH auch die Umgehung von Unternehmensinhaltsfiltern wie für Erwachsene, Spiele, Streaming und Malware ermöglichen.
- **Gefährdung durch Datenexfiltration und Malware-Verbreitung:** Wenn unkontrolliert, kann DoH die Gefährdung durch Datenexfiltration und Malware-Verbreitung erhöhen, da es Hintertüren zu geschützten Netzwerken öffnen kann. Cyberkriminelle nutzen DNS oft als Hintertür, um geschäftskritische Informationen zu erlangen und zu exportieren sowie Malware über Command-and-Control-Kommunikation (C&C) mit Geräten zu verbreiten. Die DoH-DNS-Anfrage ist verschlüsselt und daher für Dritte unsichtbar, einschließlich Cybersicherheitssoftware, die möglicherweise auf passive DNS-Überwachung angewiesen ist, um Anfragen an bekannte bösartige Domänen zu blockieren. In der Regel können Sicherheitsteams diese Angriffe effektiv stoppen, indem sie Bedrohungsinformationen über die interne DNS-Infrastruktur in Kombination mit Analysen auf Basis künstlicher Intelligenz und maschinellem Lernen nutzen. Da DoH diese DNS-Sicherheitsmaßnahmen umgeht, besteht für Unternehmen ein neues Risiko, diesen und anderen DNS-basierten Bedrohungen ausgesetzt zu sein.

  Zum Beispiel verwenden neuere Versionen der PsiXBot-Malware DoH, um bösartige Kommunikation zu verschlüsseln, sodass sie sich im regulären HTTPS-Datenverkehr verstecken und Malware installieren kann, die Daten stehlen oder das Opfer zu einem Botnetz hinzufügen kann.

- **Erhöhter DNS-Server-Overhead/verminderte DNS-Server-Leistung:** DoH und DNS over TLS erhöhen die Belastung, die jede DNS-Abfrage auf einen DNS-Server ausübt, und können die Benutzererfahrung beeinträchtigen. Das herkömmliche DNS basiert auf dem User Datagram Protocol und verursacht nur minimalen Overhead. Sowohl DoH als auch DNS over TLS laufen über Transmission Control Protocol, das für einen DNS-Server ressourcenintensiver ist. Außerdem erfordern sowohl DoH als auch DNS over TLS, dass der DNS-Server die Anfrage entschlüsselt und die Antwort verschlüsselt, was den Overhead auf dem DNS-Server weiter erhöht. Administratoren von DNS-Servern sollten davon ausgehen, dass ihre Server nur einen Bruchteil der DoH- und DNS over TLS-basierten Abfragerate verarbeiten können, die sie mit herkömmlichen DNS-Anfragen bewältigen könnten.

ABWEICHENDER BROWSER UND BETRIEBSSYSTEM

Rollout-Pläne

Viele öffentliche rekursive DNS-Anbieter, wie Google DNS, Cloudflare und Quad9, bieten DNS over TLS und DoH in ihren Angeboten an. Viele Betriebssystem-Clients müssen sich für DNS over TLS entscheiden (obwohl viele Android-Clients standardmäßig für die Nutzung von DNS over TLS konfiguriert sind). Mit DoH benötigen Webbrowser wie Chromium und Mozilla jedoch jeweils eigene Methoden, damit sich Clients anschließen können.

Chromium

Die Chromium-Implementierung von DoH betrifft alle auf dem Chromium-Projekt basierenden Browser, einschließlich Google Chrome, Microsoft Edge und Opera. Chromium verwendet standardmäßig einen automatischen Modus, der eine unterstützte Liste von Betriebssystem-konfigurierten Resolvern auf DoH-Verfügbarkeit überprüft und dann den konfigurierten Resolver nur für DoH verwendet, wenn er verfügbar ist. Es ist außerdem geplant, die DNS over TLS-Client-Einstellungen in Android zu beobachten und sich auf eine kontrollierbare und vorhersehbare Weise zu verhalten. Für die meisten Infoblox-Kunden könnten die Änderungen von Chromium Sie möglicherweise nicht dazu verpflichten, Ihren Resolver oder Ihr Netzwerk zu ändern.

Mozilla

Mozilla bietet Cloudflare als standardmäßigen vertrauenswürdigen rekursiven Resolver unter Verwendung von DoH an. Mozilla wird versuchen, die Verwendung von DoH zu erkennen und zu deaktivieren, wenn es das für notwendig erachtet. Leider sind die Methoden, die für einen eleganten Rückgriff auf die traditionelle DNS-Auflösung verwendet werden, noch nicht bewährt und möglicherweise nicht für alle Situationen geeignet. Einige Unternehmen haben möglicherweise keine vollständige Kontrolle über die in ihrer Organisation installierten Browser. Zum Beispiel:

Es könnte sich als schwierig erweisen, die Einhaltung der Unternehmenspräferenzen für Browsereinstellungen über BYOD, Heimarbeit und andere mobile Szenarien hinweg sicherzustellen. Ebenso werden Kommunikationsdienstleister mit ihren vielfältigen Endbenutzern noch weniger Einfluss auf die Browsereinstellungen auf Netzwerkgeräten haben.

Apple

Die kürzlich von Apple veröffentlichten Versionen von iOS und macOS unterstützen sowohl DNS over TLS als auch DoH-Protokolle. Diese Einstellungen können selektiv angewendet werden – angefangen beim gesamten Betriebssystem über MDM-Profile oder Netzwerkerweiterungen bis hin zu einzelnen Anwendungen oder ausgewählten Netzwerkanfragen von Anwendungen.

Laut Apple gibt es drei Möglichkeiten, verschlüsseltes DNS zu aktivieren. Eine Option besteht darin, systemweite verschlüsselte DNS-Einstellungen anzuwenden, bei denen Benutzer oder Administratoren einen einzelnen verschlüsselten DNS-Server als Standardresolver für alle Anwendungen im Betriebssystem auswählen können. Entwickler können Netzwerkerweiterungsanwendungen schreiben, die das Betriebssystem so konfigurieren, dass es diesen Server verwendet, oder MDM-Profile können an Clients gesendet werden, die verschlüsselte DNS-Einstellungen konfigurieren. Wenn diese Option nicht verwendet wird, werden die beiden anderen Optionen automatisch aktiviert und der Gerätebesitzer kann sie nicht direkt deaktivieren.

Die zweite Option ist für Domäneninhaber. Sie können Einstellungen auf Domänenebene konfigurieren, die die Existenz eines verschlüsselten Resolvers für die Domäne anzeigen. Wenn diese Einstellungen erkannt und verifiziert werden, wird der DNS-Datenverkehr für diese Domäne an den von der Domäne bereitgestellten verschlüsselten Resolver umgeleitet.

Die letzte Option ist verschlüsseltes DNS auf der Anwendungsschicht. Hier können Entwickler Anwendungen erstellen, die es Anwendungen ermöglichen, DNS over TLS und DoH direkt aus einzelnen Apps heraus zu verwenden. Diese Option bedeutet, dass Entwickler einen bestimmten Server für einige oder alle ihrer Anwendungsverbindungen auswählen können, wenn das Betriebssystem nicht konfiguriert ist.

Apple plant, die Benutzer mit einer speziellen Meldung zu warnen, falls ein bestimmtes Netzwerk die verschlüsselte DNS-Kommunikation im Netzwerk aufgrund von Richtlinien blockiert. Bestimmte Netzwerke werden visuell mit einem Datenschutzhinweis gekennzeichnet, und Anwendungen, die für die Verwendung bestimmter DoH-Resolver konfiguriert sind, werden nicht ordnungsgemäß funktionieren.

Microsoft

Microsoft kündigte 2019 seine Absicht an, DoH zu unterstützen, und hat DoH im Windows-DNS-Client implementiert, mit der Möglichkeit, DNS over TLS in zukünftigen Versionen zu unterstützen. Microsoft entwickelte seinen Ansatz unter der Prämisse, dass Benutzer keine speziellen Kenntnisse für die Nutzung von DoH benötigen sollten, während Netzwerkadministratoren die Kontrolle behalten können, indem sie einen Rückfall auf das traditionelle DNS-Protokoll zulassen.

Wenn der DNS-Client konfiguriert ist, wird er im „opportunistischen Modus“ arbeiten, was bedeutet, dass er versuchen wird, das DoH-Protokoll anstelle des herkömmlichen DNS zu verwenden. Der Client kann jedoch so konfiguriert werden, dass er auf herkömmliches DNS zurückgreift, falls die DoH-Protokolle nicht verfügbar sind oder nicht reagieren. Die anfänglichen vertrauenswürdigen DoH-Resolver würden aus Cloudflare, Google und Quad9 bestehen.

INFOBLOX LÖST HERAUSFORDERUNGEN IM ZUSAMMENHANG MIT DNS OVER TLS UND DOH

Als Branchenführer im Bereich sicherer, Cloud-verwalteter Netzwerkdienste vertritt Infoblox die Auffassung, dass die Umgehung der bestehenden internen DNS-Infrastruktur die betriebliche Komplexität erhöht. Diese neuen DNS-Datenschutzoptionen entwickeln sich gerade erst. Organisationen sollten jetzt Maßnahmen ergreifen, um die Risiken dieser Technologien zu verringern. Ein hervorragender Ausgangspunkt ist es, mindestens den direkten DNS-Verkehr – einschließlich DNS over TLS und DoH – zwischen internen IP-Adressen und DNS-Servern im Internet zu blockieren (Abbildung 1). Dieser Schritt stellt sicher, dass Endbenutzer die interne DNS-Infrastruktur ihres Unternehmens nutzen, sodass ihre IT-Abteilung eine DNS-Auflösungsrichtlinie umfassend anwenden und Probleme beheben kann. Infoblox bietet Organisationen Lösungen, die diese Herausforderungen im Bereich des DNS-Datenschutzes lösen. Durch die Möglichkeit, den Zugriff auf externe DNS-Resolver zu blockieren und eine interne verschlüsselte DNS-Auflösung bereitzustellen, können Organisationen die Kontrolle über DNS behalten.

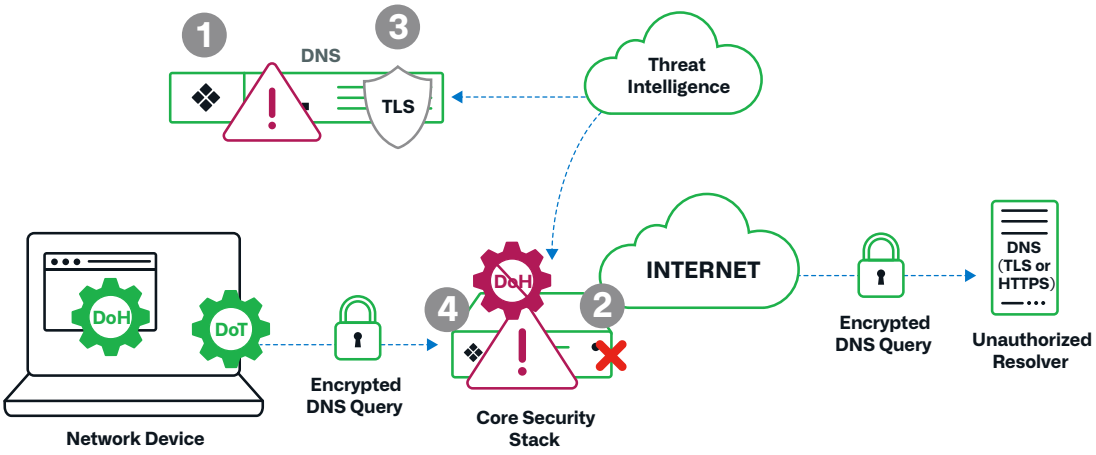

Abbildung 1: DoT/DoH-Best-Practices schützen Ihre Benutzer und Geräte

Blockauflösung für DoH-Domänen

BloxOne® Threat Defense, eine hybride grundlegende Sicherheitslösung von Infoblox, nutzt DNS als erste Verteidigungslinie. Sie blockiert die Auflösung von DoH-Domänen und ermöglicht einen reibungslosen Rückfall auf bestehendes internes DNS. Diese Funktionen helfen, den Missbrauch von DoH zu verhindern und Risiken zu mindern.

BloxOne Threat Defense umfasst mehrere Funktionen zur Verwaltung von DoH:

- Mit Policy Threat Intelligence-Feeds für DoH können Netzwerkadministratoren die DNS-Zugriffsmethode zur Erkennung und Abwehr von Bedrohungen steuern, indem sie DoH-basierte Sicherheitsrichtlinien deaktivieren. Browser greifen problemlos auf das verwaltete DNS der Organisation zurück, ohne die Benutzeraktivität zu unterbrechen.
- Ein DoH-Richtlinien-Feed für bekannte DoH-IPs und DoH-Domänen wurde zur Threat Intelligence Data Exchange, der Bedrohungsinformations-Aggregations- und -Verteilungsplattform von Infoblox, hinzugefügt. Andere Sicherheitstools, wie NGFWs, können diesen Datenfeed und die damit verbundenen Informationen verwenden, um den DoH-Datenverkehr zu externen Servern zu blockieren.
- Benutzer können DoH-bezogene Domänen und IPs innerhalb von Dossier, dem Bedrohungsuntersuchungstool von Infoblox, überprüfen.

Diese Funktionen sind für alle Abonnementstufen von BloxOne Threat Defense verfügbar.

Infoblox DNS-Verschlüsselung

Das Infoblox Network Identity Operating System (NIOS) ist das Betriebssystem, das die Infoblox-Kernnetzwerkdienste betreibt und den ununterbrochenen Betrieb der Netzwerkinfrastruktur sicherstellt.

Infoblox Encrypted DNS ist eine NIOS-Funktion, die eine effiziente Verschlüsselung bietet und gleichzeitig die erstklassigen DNS-Dienste von Infoblox bereitstellt. Zu den Startfunktionen gehört die Unterstützung von DOH und DNS over TLS.

Infoblox Encrypted DNS bietet einen einzigartigen Ansatz zur Verschlüsselung Ihres DNS-Verkehrs. Im Gegensatz zu Methoden, die auf Load-Balancer oder Überprovisionierung setzen, läuft Infoblox Encrypted DNS als ein einziger Dienst für all Ihre DNS-Anforderungen. Unsere Standardfunktionen, einschließlich erweiterter DNS-Schutz und DNS-Cache-Beschleunigung, sind alle über denselben hoch skalierbaren DNS-Dienst verfügbar.

ZUSAMMENFASSUNG

Infoblox ist bestrebt, Kunden dabei zu unterstützen, die Netzwerkleistung, Sicherheit, Skalierbarkeit und Zuverlässigkeit aufrechtzuerhalten, die moderne Unternehmensnetzwerke erfordern. Diese Veränderungen finden gerade statt, da die jüngsten Browser-Updates und Betriebssystemversionen diese Änderungen heute in Netzwerken implementieren. Die Lösung des „Last Mile“-Problems ist zwar unerlässlich und lohnenswert, wir sind uns jedoch auch bewusst, dass Unternehmen die Transparenz und Kontrolle über ihren DNS-Datenverkehr aufrechterhalten müssen. Renommierte Sicherheitsbehörden, darunter die NSA, empfehlen Unternehmen, Maßnahmen zu ergreifen, um die mit diesen Technologien verbundenen Risiken zu reduzieren. Kunden können Infoblox-Lösungen nutzen, um die Kontrolle über ihr DNS zu behalten und unvorhergesehene Probleme durch neue DNS-Datenschutzinitiativen zu minimieren. Weitere Informationen zu diesen sich weiterentwickelnden Technologien und Infoblox-Lösungen finden Sie in der Infoblox-Community.

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

+1.408.986.4000
www.infoblox.com/de

Version: 20230919v1