SOLUTION NOTE

MODERNES ZERO TRUST MIT INFOBLOX ERMÖGLICHEN

EINLEITUNG

In der heutigen digitalen Landschaft wird die Einführung von Zero-Trust-Sicherheitsmodellen immer wichtiger. Laut einer Umfrage von Gartner haben 63 % der Unternehmen weltweit Zero-Trust-Strategien vollständig oder teilweise implementiert, um komplexen Cyberbedrohungen entgegenzuwirken und/oder die Best Practices der Branche einzuhalten. Allerdings gibt es in einer typischen Zero-Trust-Strategie Lücken. Viele Organisationen vertrauen implizit den Domänen, auf die Benutzer im Internet zugreifen. Dadurch ist das Unternehmen anfällig für verdächtige, bösartige und ähnliche Domänen, die sich im Besitz von Angreifern befinden und zu Sicherheitsverletzungen führen können. Ohne Verständnis des Datenverkehrsflusses in einem Netzwerk ist Zero Trust nicht umsetzbar. Infoblox bietet einen modernen Ansatz für Zero Trust und betont die entscheidende Rolle von DNS bei der Sicherung von Hybrid- und Multi-Cloud-Umgebungen.

> *Für die meisten Organisationen deckt eine Zero-Trust-Strategie typischerweise die Hälfte oder weniger der Umgebung einer Organisation ab und mindert ein Viertel oder weniger des gesamten Unternehmensrisikos. “*
>
> **Gartner**

WARUM ZERO TRUST?

Zero Trust ist ein Sicherheitsframework, das davon ausgeht, dass Sicherheitsverletzungen unvermeidbar sind und sich darauf konzentriert, die Auswirkungen solcher Verletzungen zu minimieren. Zu den wichtigsten Treibern für die Einführung von Zero Trust gehören:

- Bedrohungsakteure, die immer raffinierter werden
  - » Ransomware und Lookalike-Spear-Phishing-Domains
  - » Systeme mit verteiltem Datenverkehr (Traffic Distribution System, TDS)
- Hyperkonnektivität und digitale Initiativen
  - » Hybride Multi-Cloud-Umgebungen
  - » IoT/OT und Fernarbeit

Mit Hyperkonnektivität und allgegenwärtigen digitalen Transformationen, wie der Einführung von Multi-Cloud- und Hybrid-Netzwerken, werden Sicherheitsverletzungen immer häufiger. Nach einem ersten Sicherheitsverstoß können sich Bedrohungen sehr schnell lateral ausbreiten. Ein Zero-Trust-Ansatz kann den Umfang, die Auswirkungen und die Kosten einer Sicherheitsverletzung begrenzen, sodass Unternehmen schnell auf Vorfälle reagieren und Betriebsunterbrechungen minimieren können.

Zu den Zero Trust-Prinzipien gehören die Annahme von Sicherheitsverletzungen, das Prinzip „Niemals vertrauen, immer überprüfen“, die Verwendung von Zugriffsrechten mit geringsten Privilegien, ständige Überwachung sowie Segmentierung, um die laterale Ausbreitung von Bedrohungen zu begrenzen.

DNS-ÜBERLEGUNGEN IM ZERO TRUST

DNS spielt eine entscheidende Rolle in Zero-Trust-Strategien. Traditionelle Zero-Trust-Modelle übersehen oft DNS und vertrauen ihm implizit, was eine erhebliche Lücke darstellen kann. Das ermöglicht es Benutzern und Geräten, auf bösartige Domänen zuzugreifen, die mit Bedrohungen wie Ransomware, Phishing, Lookalike-Domänen und Zero-Day-DNS verbunden sind, wodurch das Netzwerk Sicherheitsverletzungen ausgesetzt wird. Infoblox betont, dass eine Zero-Trust-Strategie DNS nicht implizit vertrauen, sondern Folgendes sicherstellen sollte:

- **Verschlüsselte und authentifizierte DNS-Verbindungen**
- **Überwachung auf Datenexfiltration und Zero-Day-DNS-Bedrohungen**
- **Protective DNS (PDNS) zur Verhinderung des Zugriffs auf bösartige Domänen**

Der Ansatz von Infoblox umfasst verschlüsseltes DNS aus Datenschutzgründen sowie aktuelle Bestandsdaten für Zugriffsentscheidungen und PDNS zur Blockierung von Domänen mit hohem Risiko, Command and Control (C2)-Kommunikation und Datenexfiltration.

DNS-VERSCHLÜSSELUNG FÜR UNTERNEHMEN

NIST SP 800-207 besagt: „Alle Kommunikation sollte auf die sicherste verfügbare Weise erfolgen, Vertraulichkeit und Integrität schützen und eine Quellenauthentifizierung bieten.“ Das sollte die Aktivierung des Datenschutzes (Anti-Snooping) für die rekursive DNS-Auflösung umfassen. Die Verschlüsselung umfasst DNS over TLS (DoT), das den bekannten designierten Port 853 verwendet, und DoH (DNS over HTTP), das Port 443 verwendet, durchsetzt mit Internet-Traffic.

SCHÜTZENDES DNS FÜR DAS UNTERNEHMEN

Die Protective DNS (PDNS)-Lösung von Infoblox für Unternehmen bietet proaktive Sicherheit durch:

- **Verhinderung von Erstinfektionen durch die Verweigerung der Auflösung hochriskanter Domänen**
- **Stoppen der laufenden C2-Kommunikation**
- **Blockieren der Datenexfiltration**

Infoblox PDNS integriert Bedrohungsinformationen, KI/ML-Engines und die Durchsetzung von DNS-Richtlinien, um umfassenden Schutz vor Cyberbedrohungen zu bieten. Zu den Komponenten gehören:

- **Rekursiver DNS-Server:** Findet IP-Adressen für Domänen und gibt sie an den Client zurück
- **DNS Threat Intel:** Identifiziert hochriskante und bösartige Domänen, die sich im Besitz von Bedrohungsakteuren befinden
- **KI/ML-Lern-Engine:** Identifiziert fortgeschrittene Bedrohungen, indem sie den DNS-Datenverkehr eines Unternehmens in Echtzeit überprüft und Verhaltensanalysen durchführt
- **DNS-Richtlinien-Engine/RPZ:** Erlaubt oder verweigert die DNS-Auflösung basierend auf dem Richtliniensatz

DURCHSETZUNG AUF GERÄTEEBENE

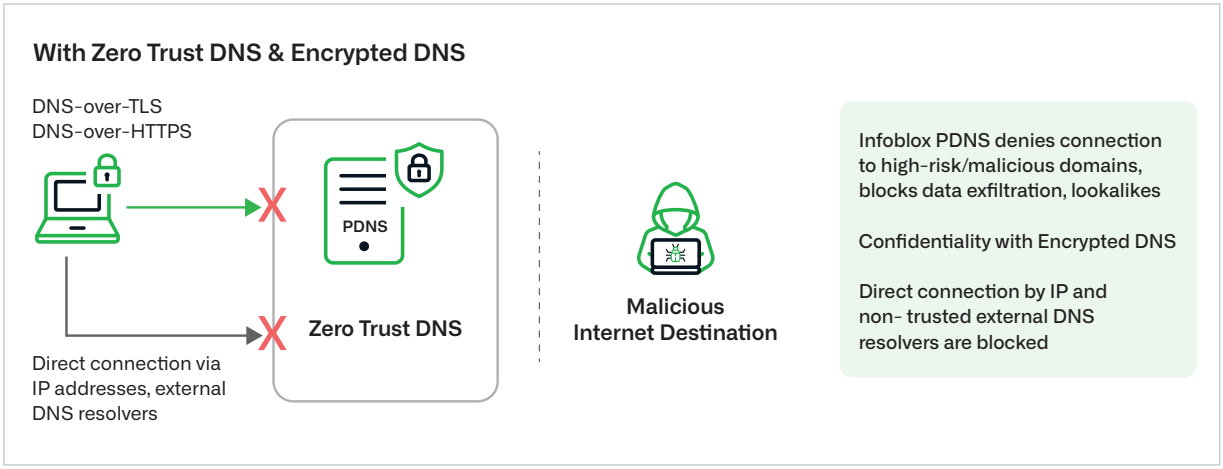
Das Zero Trust DNS-Modell von Infoblox umfasst eine Durchsetzung auf Geräteebene, um DNS-Umgehung zu verhindern und ausgehenden IP-Verkehr einzuschränken. Dadurch wird sichergestellt, dass Geräte nur mit zugelassenen PDNS-Servern verbunden werden, was die allgemeine Netzwerksicherheit erhöht.

ASSET-ERKENNUNG UND DATEN ALS EINGABE FÜR ZERO-TRUST-SYSTEME, UM ENTSCHEIDUNGEN ÜBER DEN ZUGRIFF ZU TREFFEN

Transparenz über alle Netzwerkressourcen ist entscheidend für Zero Trust. Universal Asset Insights von Infoblox bietet eine einheitliche Ansicht von Assets in hybriden Multi-Cloud-Umgebungen und automatisiert die Erkennung und Analyse. Das hilft, ein aktuelles Asset-Inventar zu pflegen, nicht autorisierte Geräte zu erkennen und Geräteaktivitäten mit Identitäten zu korrelieren. DNS- und IPAM-Metadaten sind wichtige Telemetriequellen, die detaillierte Kundeninformationen und Netzwerkverhalten als Input für Zero-Trust-Systeme liefern. Sie können verwendet werden, um bessere Entscheidungen über den Zugriff und die Zuweisung von Richtlinien zu treffen, aber der Zugriff kann je nach Geolokalisierung des Benutzers/Geräts, des Netzwerk-Switch-Ports usw. gewährt oder verweigert werden. Infoblox kann Ihnen beispielsweise mitteilen, dass ein Gerät ein Drucker ist und dass es nur auf bestimmte Domänen zugreifen kann. Ein weiteres Beispiel ist, dass Infoblox IoT-/OT-Geräte (z. B. Kameras) identifizieren kann und feststellen kann, dass sie in der letzten Woche nur bestimmte DNS-Aufrufe getätigt haben. Der Administrator kann dann entscheiden, eine Zero-Trust-Richtlinie für diese Kameras zu erstellen.

AUTOMATISIERUNG UND ORCHESTRIERUNG

Zero Trust stützt sich stark auf Automatisierung und Orchestrierung, um Sicherheitsreaktionsfunktionen zu unterstützen. Infoblox lässt sich in verschiedene Sicherheitstools und Plattformen integrieren, um die Durchsetzung von Richtlinien, die Erkennung von Bedrohungen und die Reaktion auf Vorfälle zu automatisieren und Kontextinformationen bereitzustellen.



ZUSAMMENFASSUNG

Die Zero-Trust-Lösungen von Infoblox bieten ein robustes Framework zur Sicherung moderner Netzwerke. Durch die Integration von DNS-basierter Sicherheit, Asset-Transparenz und Automatisierung unterstützt Infoblox Unternehmen bei der Implementierung effektiver Zero-Trust-Strategien, wodurch das Risiko von Cyberbedrohungen reduziert und die allgemeine Sicherheitslage verbessert wird.

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

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

Version: 20241205v1