infoblox.

WHITEPAPER

DNS BEST PRACTICES

Autor:
Craig Sanderson,
Principal Cyber Security Strategist
bei Infoblox

INHALTSVERZEICHNIS

In diesem Whitepaper werden Best Practices für die Sicherheit des Domain Name Systems (DNS) vorgestellt, mit denen zwei Ziele erreicht werden sollen: die Sicherung des DNS-Protokolls und der DNS-Infrastruktur zur Eindämmung von Missbrauch oder Fehlkonfigurationen und die Nutzung von DNS als zusätzliche Ebene der Netzwerksicherheit im Rahmen eines Zero-Trust- und/oder Defense-in-Depth-Ansatzes zur Verwaltung von Sicherheitsrisiken.

1. EINLEITUNG

Um auf Internetressourcen über Domainnamen (z. B. www.example.com) und nicht über diese IP-Adressen (93.184.216.34) zuzugreifen, benötigen Benutzer ein System, das diese Domainnamen in IP-Adressen und zurück übersetzt. Diese Übersetzung ist die Hauptaufgabe des Domain Name System (DNS). In den Netzwerken moderner Unternehmen ist die DNS-Infrastruktur für die gesamte interne Netzwerkkommunikation und die Kommunikation mit dem Internet von entscheidender Bedeutung. Wenn sie ausfällt, können ganze Netzwerke mitsamt ihren Anwendungen und Benutzern zum Erliegen kommen. Daher ist das DNS ein entscheidendes Element für die digitale Ausfallsicherheit eines Unternehmens und sollte regelmäßig überprüft oder neu bewertet werden.

Bei solchen Beurteilungen sollte auch festgestellt werden, ob die DNS-Server über ausreichend Kapazität verfügen, um die Anforderungen des Unternehmens zu erfüllen, insbesondere bei der Einführung verschlüsselter DNS-Protokolle. Die Bewertungen sollten auch eine Überprüfung des Zustands und der Konfiguration der Server umfassen, um sicherzustellen, dass die DNS-Infrastruktur als Teil einer äußerst belastbaren und redundanten Architektur optimiert ist. Darüber hinaus sollten Unternehmen Kontrollen innerhalb der DNS-Plattform implementieren, um das enorme Potenzial von DNS als grundlegende Ebene einer Cybersicherheitsarchitektur zu nutzen.

Die DNS-Plattform wird bereits von allen Arten von Clients im Netzwerk verwendet, einschließlich On-Premises, in der Cloud und in sämtlichen IoT-Geräten. Daher kommt jeder Schutz, den die DNS-Infrastruktur bietet, allen Clients zugute, die diese Infrastruktur für die Namensauflösung nutzen, unabhängig von der Art des Geräts. Aus diesem Grund sollten Unternehmen und Regierungen DNS als grundlegende Komponente in ihre Cybersicherheitsstrategie aufnehmen.

2. AUSWIRKUNGEN VON DNS AUF DIE CYBER-RESILIENZ, DEFENSE-IN-DEPTH UND ZERO TRUST

Die jüngsten Entwicklungen bei den Best Practices für die Netzwerksicherheit haben dazu geführt, dass das Konzept der „Defense-in-Depth“ (Verteidigung in der Tiefe) immer mehr in den Vordergrund rückt. Dabei handelt es sich um die Idee, dass keine Verteidigungsmaßnahme unfehlbar ist und dass die beste Verteidigung daher aus mehreren Schutzebenen besteht. Diese Art der Cyber-Verteidigung führt zu einem flexibleren, skalierbaren und widerstandsfähigeren System, das widerstandsfähiger gegen Kompromittierungen ist und sich stärker an Zero-Trust-Prinzipien orientiert.

Zero-Trust-Prinzipien basieren auf der Annahme, dass keinem Element, Knoten oder Dienst implizit vertraut werden kann. Das DNS wird jedoch bei den Zero-Trust-Strategien häufig übersehen, wodurch eine erhebliche Lücke entsteht, wenn ihm implizit vertraut wird.

Um DNS an Zero-Trust-Prinzipien auszurichten, sollten Unternehmen keine Annahmen treffen, sondern ihre Informationsquellen überprüfen, indem sie DNS zur Durchsetzung von Sicherheitsrichtlinien einsetzen, Endbenutzer und Systeme am Zugriff auf schädliche oder nicht autorisierte Ressourcen hindern und für die digitale Forensik und die Reaktion auf Vorfälle eine vollständige Transparenz der Ressourcen gewährleisten.

Dies markiert eine Verschiebung der Rolle des DNS von einer rein operativen zu einem umfassenderen Werkzeug zur Gewährleistung der Internetsicherheit und zur Stärkung der Netzwerkresilienz.

Zero Trust stellt einen Wechsel von einem ortsbezogenen Modell zu einem identitäts-, kontext- und datenorientierten Ansatz dar, mit fein abgestuften Sicherheitskontrollen zwischen Benutzern, Systemen, Anwendungen, Daten und Assets, die sich im Laufe der Zeit ändern. Die DNS-Auflösung könnte für Endpunkte offen sein, die beliebige öffentliche Domainnamen abfragen. Daher sollten Unternehmen das DNS sichern, um zu verhindern, dass es als Kanal zur Umgehung von Zero-Trust-Netzwerkkontrollen verwendet wird. Dies könnte die Implementierung von schützenden DNS-Diensten und/oder spezifischen DNS-Resolver-Konfigurationen für bestimmte Klassen von Endpoints beinhalten. DNS-Sicherheit ist besonders für den Schutz von IoT-Geräten und Betriebstechnologien in der Fertigung und in kritischen Infrastrukturen nützlich, bei denen der Einsatz von Endpunkt-Sicherheitslösungen eine Herausforderung darstellt.

3. DNS-BEDROHUNGSVEKTOREN

Die DNS-Infrastruktur ist ein häufiger Bedrohungsvektor für Angriffskampagnen.[1] Bedrohungen des DNS-Dienstes können kaskadenartig zu erheblichen Betriebsausfällen oder zum Verlust von Daten, Integrität und Vertraulichkeit führen. Darüber hinaus nutzen viele Bedrohungsakteure, wie beispielsweise ALPHV Blackcat, bösartige Domains zur Durchführung von umfangreichen Lösegeldangriffen.[2] Nachfolgend finden Sie eine nicht erschöpfende Liste von Beispielen für Kompromisse, die nicht nur die DNS-Dienste gefährden könnten, sondern auch alle Systeme, auf die sich Organisationen verlassen:

a) Distributed Denial of Service: Ein böswilliger Angreifer könnte eine große Anzahl von Anfragen senden, um einen Denial-of-Service-Angriff (DoS) auf einen DNS-Server/-Dienst durchzuführen. Der Angreifer könnte zahlreiche DNS-Clients von Drittanbietern zur Unterstützung des Angriffs einsetzen (verteilter DoS oder DDoS).

b) Nicht autorisierte Konfigurationsänderung: Die Konfigurationsdatei auf Plattformebene, welche die DNS-Kommunikation ermöglicht, könnte aufgrund unzureichender Schutzmaßnahmen beschädigt oder unbefugten Änderungen ausgesetzt sein. Dies kann zu Störungen führen, die von einer Unterbrechung der Kommunikation zwischen DNS-Hosts bis hin zum vollständigen Ausfall des DNS-Dienstes selbst reichen können.

c) Ausnutzung von nicht genutzten CNAMEs: Wenn ein DNS-CNAME-Eintrag zwei Domainnamen miteinander verknüpft, besteht das Risiko, dass die übergeordnete Domain des kanonischen Namens, auf den der Eintrag verweist, nicht von der Zielorganisation registriert bleibt. Infolgedessen können Angreifer die übergeordnete Domain registrieren, sodass DNS-Auflösungen letztendlich zu der vom Angreifer kontrollierten Domain führen. Eine weitere Möglichkeit zur Ausnutzung von CNAME-Einträgen besteht in der Auflösung des kanonischen Names zu einer IP-Adresse, die vom Domaininhaber nicht mehr verwendet wird. In einem solchen Fall könnte der Angreifer dann die Kontrolle über diese IP-Adresse erlangen, um Angriffe durchzuführen.

d) Ausnutzung einer unzulässigen Delegierung: Domains werden von einer Ebene der DNS-Hierarchie an eine andere delegiert, meist von einer Top-Level-Domain an eine Organisation, die die Domain registriert hat. Bei der Einrichtung der Delegierung müssen die autoritativen DNS-Server für die Domain angegeben werden. Die Delegierung einer Zone an einen Nameserver, der für diese Zone nicht autoritativ ist, wird als unzulässige Delegierung bezeichnet. Eine unzulässige Delegierung (auch „Lame Delegation“) kann unter bestimmten Umständen zu einem Domain-Hijacking führen. Wenn eine Subdomain an einen DNS-Hosting-Anbieter delegiert wird und der Vertrag über die Bereitstellung von DNS-Diensten für diese Domain ausläuft, können Angreifer die Auflösung für diese Subdomain kapern, indem sie mit dem Anbieter, der die von der Delegierung betroffenen Server kontrolliert, einen Vertrag über das Hosting dieser Subdomain unter ihrer Kontrolle abschließen. Auf diese Weise kann der Angreifer Auflösungsanfragen an seine eigene Infrastruktur umleiten und so von der positiven Reputation des Domainnamens profitieren.

e) Ausnutzung von Lookalike-Domains: Bedrohungsakteure nutzen in großem Umfang Lookalike- oder Typosquat-Domains, um sich als Zielunternehmen auszugeben. Indem sie den guten Ruf legitimer Organisationen ausnutzen, erhöhen sie die Erfolgsquote ihrer Phishing- und Malware-Kampagnen erheblich. Diese Lookalike-Domains können subtile Variationen legitimer Domains enthalten oder Text- oder Zeichenersetzungen zur Registrierung einer Domain verwenden, von der Benutzer annehmen würden, dass sie sich im Besitz der legitimen Organisation befindet.

f) DGAs und Ransomware-as-a-Service: Domain Generation Algorithms (DGAs) ermöglichen es böswilligen Akteuren, zahlreiche Domainnamen für die C2-Kommunikation (Command-and-Control) zu generieren, was die Verbreitung von Malware und die Umgehung der Entdeckung erleichtert. Ransomware-as-a-Service (RaaS) wie Blackcat verwenden DNS für die C2-Kommunikation.

4. BEST PRACTICES FÜR DIE DNS-SICHERHEIT

Der ursprüngliche Zweck von DNS war die Verteilung von Informationen wie Zuordnungen von Host- und IP-Adressen, Mail-Routing-Informationen und mehr. Aus diesem Grund wurde DNS traditionell nicht als ein Tool zur Sicherung der Netzwerkkommunikation angesehen. Die Rolle, die DNS heute

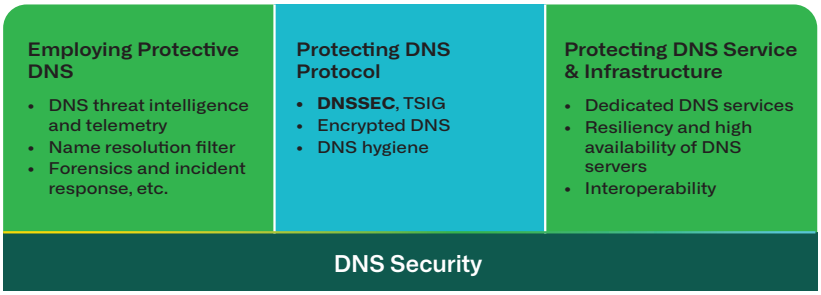
1 https://www.cisa.gov/news-events/news/cisa-launches-its-protective-dns-resolver-general-availability-federal-agencies

2 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
https://blogs.infoblox.com/threat-intelligence/dns-early-detection-breaking-the-blackcat-ransomware-kill-chain/

bei der Ermöglichung fast aller Netzwerkkommunikationen spielt, macht es jedoch zu einem effektiven Werkzeug für die Überwachung und Verwaltung dieser Kommunikationen. Aus diesem Grund hat sich die DNS-Sicherheit von einem reinen Schutz der DNS-Infrastruktur und -Protokolle zu einer kritischen Sicherheitskontrolle und einer zentralen Komponente der Sicherheitsstrategie des gesamten Unternehmens entwickelt. Es sei darauf hingewiesen, dass „DNSSEC“ (das für ein spezielles Protokoll namens DNS Security Extension steht) nur ein Teil des umfassenderen Konzepts der „DNS-Sicherheit“ ist und zusammen mit anderen bewährten Verfahren umgesetzt werden muss.

In den folgenden Abschnitten erörtern wir die drei wichtigsten Komponenten bewährter Verfahren für die DNS-Sicherheit, die berücksichtigt werden sollten:

- Einsatz von Schutz-DNS
- Schutz des DNS-Protokolls
- Schutz des DNS-Service und der DNS-Infrastruktur



4.1 Protective DNS

Protective DNS ist ein DNS-Dienst, der mit Sicherheitsfunktionen ausgestattet ist, um DNS-Anfragen und -Antworten zu analysieren und Maßnahmen zur Bedrohungsabwehr zu ergreifen. Protective DNS verhindert die Zustellung von Malware, Ransomware, Phishing und anderen auf Weblinks ausgerichteten Angriffen, die versuchen, Spyware und Viren zu liefern, und blockiert den Zugriff auf bösartige Websites. Protective DNS kann als Dienst von einem Anbieter bereitgestellt werden, auf einer internen DNS-Infrastruktur implementiert werden oder als Kombination aus beidem genutzt werden. Eine Kombination aus extern bereitgestelltem Protective DNS und intern eingesetztem Protective DNS bietet potenzielle Vorteile. Auch wenn dieser Ansatz nicht in allen Fällen anwendbar ist, empfehlen wir, dieses kombinierte hybride Schema zu nutzen, wo es machbar ist. Wie der Einsatz von Protective DNS-Plattformen durch Regierungen weltweit und die DNS4EU-Initiative in der Europäischen Union zeigt,[3] ist die Verwendung von Protective DNS ist zu einer bewährten DNS-Praxis geworden.

Die Ergebnisse des Einsatzes von Protective DNS sollten Folgendes umfassen:

Blocking or redirecting harmful traffic in real time before malicious activity starts.

Blocking categories of traffic. This is typically traffic that doesn't conform to an organizations policies.

Visibility into real-time DNS query and response history for digital forensics.

Integration with an organization's wider security ecosystem.

Facilitating an organizations responsibility to comply with regulatory or contractual requirements for blocking traffic to disallowed sites.

3 https://www.joindns4.eu/
https://www.ncsc.gov.uk/information/pdns
https://www.forgov.qld.gov.au/information-and-communication-technology/cyber-security/cyber-security-services/system-and-email-hardening/protective-dns-service/implement-a-protective-dns-service
https://www.cisa.gov/resources-tools/services/protective-domain-name-system-resolver

a. Threat Intelligence und Telemetrie.

Die Angriffsfläche von Unternehmen entwickelt sich ständig weiter. Daher ist es von größter Bedeutung, bösartige Kommunikation so früh wie möglich zu überwachen und zu unterbrechen. DNS ist trotz des Aufkommens anderer Netzwerktechnologien eine Konstante und ist gut positioniert, um Benutzer in allen Umgebungen zu schützen – von Unternehmen bis hin zu mobilen Endgeräten. Darüber hinaus ist DNS oft die erste Verbindung zu Bedrohungen und kann komplexe, mehrstufige Angriffe stoppen, bevor sie fortschreiten. DNS als Sicherheitskontrollpunkt ist im Gegensatz zu anderen Mechanismen im Sicherheits-Stack nicht auf eine bestimmte Art von Bedrohung beschränkt. Es kann Benutzer und Unternehmen vor Betrug, Diebstahl von Zugangsdaten, Ransomware und Datenexfiltration schützen.

Dieser Ansatz erfordert Threat Intelligence und die Fähigkeit, diese in den DNS-Resolver zu integrieren. Bedrohungsdaten werden in einer DNS-Infrastruktur über Mechanismen wie Response Policy Zones (RPZs) genutzt und können über eine Reihe von Architekturen nahtlos in die DNS-Auflösungskette integriert werden.

b. Filterung der Namensauflösung

Filterung der Namensauflösung ist ein Begriff, der sich auf eine DNS-Infrastruktur bezieht, die Richtlinien auf die DNS-Auflösung anwendet. Diese Richtlinien beziehen sich in der Regel auf die Sicherheit: Eine Protective-DNS-Implementierung könnte beispielsweise die Auflösung einer Reihe von Domainnamen verweigern, von denen bekannt ist, dass sie in Phishing-Kampagnen verwendet werden oder die eine Malware-Befehls- und Kontrollinfrastruktur identifizieren. Anstatt diese Domainnamen in IP-Adressen oder andere Datentypen aufzulösen, gibt Protective DNS in der Regel eine andere Form der DNS-Antwort zurück, z. B. NXDOMAIN (was „Non-existent Domain“ bedeutet), was wiederum anzeigt, dass der gesuchte Domainname nicht existiert. Protective-DNS-Implementierungen protokollieren auch Abfragen nach Domainnamen, die eine Richtlinie auslösen, da diese Abfragen auf eine Infektion durch Malware oder andere bösartige Aktivitäten hinweisen können.

Protective DNS wird in der Regel entweder mit RPZs implementiert, die auf einem lokalen DNS-Dienst, einem cloudbasierten, sicheren rekursiven DNS-Dienst oder mit einer Kombination aus beidem konfiguriert sind.

Im Internet sind auch sichere rekursive DNS-Dienste verfügbar. Diese Dienste bieten in der Regel ein webbasiertes Kontrollpanel, mit dem Administratoren die Auflösungsrichtlinie für Anfragen von Kunden des Unternehmens anpassen können. Der Cloud-Ansatz bietet mehr Skalierbarkeit, Speicherplatz und Rechenleistung, hat aber auch Nachteile, wie z. B. den Verlust der Vertraulichkeit, höhere Latenzzeiten und Probleme bei der schnellen und genauen Zuordnung von DNS-Anfragen zu ihrer Quelle. Unternehmen können eine Kombination aus lokalen und cloudbasierten sicheren DNS-Diensten in Erwägung ziehen, um sich die Vorteile beider Systeme zu sichern. Die beste Wahl für einen bestimmten DNS-Einsatz hängt von den spezifischen Anforderungen des Netzwerks und seiner Benutzer ab.

c. DNS für digitale Forensik und Vorfallsreaktion

Regierungsbehörden und regulierte Unternehmen sollten zuverlässige Mechanismen zur Protokollierung des DNS-Traffics implementieren, um entsprechende Compliance-Anforderungen zu erfüllen. Die Protokollierung sollte sowohl aktuellen als auch historischen DNS-Traffic erfassen, um digitale Forensik und die Reaktion auf Vorfälle zu ermöglichen.
Diese DNS-Protokolle sollten mit anderen Systemprotokollen integriert werden, um die Korrelation mit anderen Protokollen von Netzwerkaktivitäten zu erleichtern und so die Transparenz und Nachvollziehbarkeit zu verbessern.

In Fällen, in denen eine vollständige Protokollierung des DNS-Traffics zu ressourcenintensiv ist, können Unternehmen cloudbasierte Lösungen, effiziente Protokollierungsmethoden (z. B. DNSTAP) oder eine selektive Protokollierung in Betracht ziehen. Allerdings müssen DNS-Anfragen und -Antworten, die mit Domains in Verbindung stehen, die von den Protective-DNS-Diensten als bösartig oder nicht autorisiert eingestuft wurden, zur Unterstützung der Sicherheits- und Compliance-Ziele unbedingt protokolliert werden. Um eine schnelle Benachrichtigung über Abfragen zu gewährleisten, die auf eine Infektion oder bösartige Aktivitäten hindeuten könnten, sollten Unternehmen die Protective-DNS-Protokolle von ihren Nameservern oder ihrem sicheren rekursiven DNS-Dienst in ihre SIEM- oder Protokollanalyseplattform integrieren.

4.2 Schutz des DNS-Protokolls

Das DNS-Protokoll ist unerlässlich für das Auffinden von Diensten, die das Surfen im Internet, E-Mail und andere geschäftskritische Anwendungen ermöglichen. Infolgedessen lassen herkömmliche Sicherheitsplattformen, wie Firewalls der nächsten Generation, DNS-Traffic oft ungehindert und unkontrolliert passieren. Bedrohungsakteure nutzen DNS zunehmend als Vektor für die Exfiltration. Laut der U.S. Cybersecurity and Infrastructure Security Agency (CISA) ist die DNS-Infrastruktur ein häufiger Bedrohungsvektor für Angriffskampagnen.[4] Bedrohungsakteure betten gestohlene Daten oft in DNS-Pakete ein und verlassen sich darauf, dass die DNS-Infrastruktur die gestohlenen Daten an die von den Bedrohungsakteuren kontrollierten DNS-Server weiterleitet. DNS-Plattformen sind ideal positioniert, um rekursive DNS-Anfragen, die sie erhalten, auf Versuche zur Datenexfiltration zu bewerten.

a. Schutz der Integrität von DNS-Diensten

Der Schutz der Integrität des DNS-Protokolls ist für die Sicherheit und Zuverlässigkeit der Internetkommunikation entscheidend. DNS Security Extensions (DNSSEC) spielen eine entscheidende Rolle, indem sie kryptografische Signaturen zur Authentifizierung von DNS-Antworten verwenden und so Angriffe wie Cache Poisoning und Man-in-the-Middle-Abfragen verhindern. Darüber hinaus erhöht die Transaktionssignatur (TSIG) die DNS-Sicherheit, indem sie die gegenseitige Authentifizierung und Integritätsprüfung zwischen DNS-Servern ermöglicht. Dabei werden gemeinsam genutzte geheime Schlüssel verwendet, um Zonentransfers und dynamische Updates vor unbefugten Änderungen zu schützen. Die Implementierung dieser Mechanismen zusammen mit Best Practices wie Ratenbegrenzung, Überwachung auf Anomalien und Durchsetzung strenger Zugriffskontrollen trägt dazu bei, das Vertrauen in die DNS-Infrastruktur und ihre Widerstandsfähigkeit gegenüber sich entwickelnden Cyber-Bedrohungen zu erhalten. Darüber hinaus sollten Unternehmen sicherstellen, dass Benutzer weder absichtlich noch versehentlich nicht autorisierte öffentliche, internetbasierte DNS-Dienste nutzen.

b. Verwendung von verschlüsseltem DNS und Authentifizierungen zum Schutz des Protokolls.

Die Kommunikation zwischen Stub-Resolvern und den rekursiven DNS-Servern, die sie abfragen, ist traditionell unverschlüsselt. Die DNS-Nachrichten, die zwischen Stub-Resolvern und DNS-Servern ausgetauscht werden, sind binär kodiert, wobei diese Kodierung allgemein bekannt und leicht zu entschlüsseln ist. Diese Kommunikation war daher sowohl dem Abfangen als auch dem Spoofing ausgesetzt, wodurch sensible Informationen preisgegeben werden konnten oder ein Angreifer ahnungslose Benutzer auf bösartige Websites umleiten konnte.

Um diesen Bedrohungen zu begegnen, hat die Internet Engineering Task Force (IETF) mehrere Verbesserungen für DNS entwickelt, die allgemein als „Verschlüsseltes DNS“ bekannt sind. Alle diese Protokolle verschlüsseln die Kommunikation zwischen Stub-Resolvern und rekursiven DNS-Servern und ermöglichen es rekursiven DNS-Servern optional, sich bei Stub-Resolvern zu authentifizieren, um den Bedrohungen durch Abfangen und Spoofing entgegenzuwirken.

c. DNS-Hygiene und Best Practices

Die Ausnutzung von Fehlkonfigurationen und abgelaufenen Domain-/DNS-Resolver-Registrierungen ist für Bedrohungsakteure relativ einfach und kann zu einer ernsthaften Beeinträchtigung der DNS-Integrität führen.

Bedrohungsakteure haben bewiesen, dass Phishing-Angriffe viel häufiger erfolgreich sind, wenn sie mit Domains vertrauenswürdiger Organisationen in Verbindung stehen. Infolgedessen registrieren sie häufig Domains, die dem Zielunternehmen ähneln, aber nicht zu ihm gehören. Noch bedenklicher ist, dass eine mangelhafte Domain-Hygiene es Bedrohungsakteuren ermöglichen kann, die Kontrolle über Domains zu übernehmen, die einem vertrauenswürdigen Unternehmen gehören.

4.3 Schutz des DNS-Service und der DNS-Infrastruktur

DNS-Geräte, wie andere Netzwerkgeräte, sind speziell für eine einfache Verwaltung, Sicherheit und Leistung entwickelt und optimiert. Allzweck-Server können nicht mit der Feinabstimmung mithalten, die diese Geräte bieten, und setzen Organisationen angesichts der kritischen Bedeutung von DNS als Netzwerkdienst einem erheblichen Risiko aus.

4 https://www.cisa.gov/news-events/news/cisa-launches-its-protective-dns-resolver-general-availability-federal-agencies

Unternehmen verwenden üblicherweise Windows-Server, die neben Active Directory (AD), einer weiteren unternehmenskritischen Identitätsinfrastruktur, auch DNS und DHCP hosten. AD verwaltet den Benutzerzugriff und die Berechtigungen und speichert kritische Informationen, wodurch eine große Angriffsfläche entsteht, die anfällig für Cyberangriffe ist.

Wenn ein Angreifer ohne diese Aufgabentrennung einem gemeinsamen Eskalationspfad folgt und Active Directory ins Visier nimmt, sind der DNS-Dienst und das Netzwerk, auf das er sich stützt, gefährdet. Da DNS in der Cybersicherheitsstrategie eines Unternehmens eine immer bedeutendere Rolle spielt, wird ein dedizierter DNS-Server unerlässlich sein, um diese Risiken zu mindern.

Ebenso versuchen Bedrohungsakteure häufig, die in DNS entdeckten Schwachstellen auszunutzen, die sich auf die Integrität des DNS-Systems auswirken oder zu einem Denial-of-Service führen können.

Weitere Hinweise zum Thema sicheres DNS finden Sie in der neuesten Version von NIST SP 800-81: Leitfaden für die Bereitstellung eines sicheren Domain Name Systems (DNS).

5. ZUSAMMENFASSUNG UND EMPFEHLUNGEN

In diesem Whitepaper wird die entscheidende Bedeutung der DNS-Infrastruktur für die Aufrechterhaltung der digitalen Widerstandsfähigkeit und Cybersicherheit eines Unternehmens erörtert. Es unterstreicht die Notwendigkeit, DNS-Server regelmäßig zu überprüfen, um sicherzustellen, dass sie über ausreichende Kapazitäten verfügen und optimal konfiguriert sind. Außerdem wird die Rolle von DNS als grundlegende Ebene in der Cybersicherheitsarchitektur hervorgehoben, von der alle Clients profitieren, die die Infrastruktur nutzen.

Um den sich entwickelnden DNS-Sicherheitsbedrohungen zu begegnen, geben wir den Netzwerk- und Sicherheitsverantwortlichen die folgenden übergeordneten Empfehlungen:

- Setzen Sie Protective DNS ein, wo immer dies technisch möglich ist, um zusätzliche netzwerkweite Sicherheitsfunktionen bereitzustellen, die Folgendes umfassen:
  - » Blockierung von schädlichem oder bösartigem Datenverkehr in Echtzeit,
  - » Das Ausfiltern von Verkehrskategorien, die nicht den Richtlinien einer Organisation entsprechen,
  - » Echtzeit- und historische DNS-Abfrage- und Antwortdaten zur Unterstützung der digitalen Forensik und der Vorfallsreaktion.
  - » Integration in das breitere Sicherheitsökosystem als Teil eines Defense-in-Depth- oder Zero-Trust-Ansatzes und
  - » Erleichterung der Verantwortung eines Unternehmens für die Einhaltung gesetzlicher oder vertraglicher Bestimmungen zur Blockierung des Datenverkehrs zu nicht zugelassenen Websites (Urheberrechtsverletzungen, rechtliche Einschränkungen usw.).
- Verschlüsseln Sie den DNS-Traffic, sowohl intern als auch extern, wo immer es möglich ist.
- Setzen Sie dedizierte DNS-Server ein, um die Angriffsfläche zu verringern.
- Befolgen Sie alle technischen Anleitungen, um sicherzustellen, dass Ihre DNS-Bereitstellungen und das DNS-Protokoll so sicher und widerstandsfähig wie möglich sind.

Weitere Informationen erhalten Sie vom Infoblox-Team unter ga@infoblox.com.

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

+1 408 986 4000
www.infoblox.com

Version: 20250131v3