infoblox.

DOCUMENTO TÉCNICO

PRÁCTICAS RECOMENDADAS DEL DNS

Autor:
Craig Sanderson,
Estratega principal de ciberseguridad
en Infoblox

ÍNDICE

1. INTRODUCCIÓN 3

2. IMPACTO DEL DNS EN LA RESILIENCIA CIBERNÉTICA, LA DEFENSA EN PROFUNDIDAD Y ZERO TRUST 3

3. VECTORES DE AMENAZAS DEL DNS 4

4. PRÁCTICAS DE SEGURIDAD RECOMENDADAS DEL DNS 4

4.1 DNS protector 5

4.2 Protección del protocolo del DNS 7

4.3 Protección del servicio y la infraestructura del DNS 7

5. RESUMEN Y RECOMENDACIONES..... 8

Este documento técnico tiene como objetivo proporcionar las prácticas de seguridad recomendadas del Domain Name System (DNS) para lograr dos objetivos: proteger el protocolo del DNS y su infraestructura para mitigar el uso indebido o la mala configuración, y utilizar el DNS para ofrecer una capa adicional de seguridad de red, como parte de un enfoque de gestión de riesgos de confianza cero o de defensa en profundidad.

1. INTRODUCCIÓN

Para acceder a los recursos de internet mediante nombres de dominio (p. ej., www.example.com) en lugar de direcciones IP (93.184.216.34), los usuarios necesitan un sistema que convierta estos nombres de dominio en direcciones IP y viceversa. Esta conversión es la tarea principal del Domain Name System (DNS). En las implementaciones de red de una organización moderna, la infraestructura del DNS es crucial para todas las comunicaciones de red, ya sea internas o externas. Si falla, redes enteras, junto con sus aplicaciones y usuarios, pueden verse afectadas. Por lo tanto, el DNS es un elemento crítico en la resiliencia digital de una organización y debe evaluarse o reevaluarse regularmente.

En dichas evaluaciones debe evaluarse si los servidores del DNS cuentan con la capacidad adecuada para cubrir las necesidades de la organización, especialmente al adoptar protocolos del DNS cifrados. Las evaluaciones también deben incluir una revisión del estado y la configuración de los servidores para garantizar que la infraestructura del DNS esté optimizada como parte de una arquitectura altamente resistente y redundante. Además, las organizaciones deben implementar controles en la plataforma del DNS para aprovechar su enorme potencial como capa fundamental de la arquitectura de ciberseguridad.

Clientes de todos los tipos en la red ya utilizan la plataforma del DNS, que incluye dispositivos IoT, además de in situ y en la nube. Por lo tanto, cualquier protección proporcionada por la infraestructura DNS beneficia a todos los clientes que utilizan esa infraestructura para la resolución de nombres, independientemente del tipo de dispositivo. Es por esta razón que las organizaciones y los gobiernos deben adoptar el DNS como un componente fundamental en su estrategia de ciberseguridad.

2. IMPACTO DEL DNS EN LA RESILIENCIA CIBERNÉTICA, LA DEFENSA EN PROFUNDIDAD Y ZERO TRUST

Los recientes avances en cuanto a prácticas de seguridad recomendadas para redes han impulsado un enfoque creciente en el concepto de «defensa en profundidad», la idea de que ninguna medida defensiva es infalible y que, por lo tanto, la mejor defensa proviene de múltiples capas de protección. Este estilo de ciberdefensa da lugar a un sistema más flexible, escalable y resiliente, más resistente a las vulneraciones y estrechamente alineado con los principios de confianza cero.

Los principios de confianza cero asumen que no se puede confiar implícitamente en ningún elemento, nodo o servicio. Sin embargo, el DNS a menudo sigue siendo un elemento que se omite en las estrategias de confianza cero, lo que crea una brecha significativa al confiar implícitamente en él.

Para alinear el DNS con los principios de confianza cero, las organizaciones no deben asumir, sino verificar sus fuentes de información, y aprovechar el DNS para aplicar políticas de seguridad, evitar que los usuarios finales y los sistemas accedan a recursos maliciosos o no autorizados, y proporcionar visibilidad de activos con fines de investigación forense digital y respuesta a incidentes.

Este paso supone un cambio en el papel del DNS, que deja de ser puramente operativo para convertirse en una herramienta de mayor escala con el fin de proporcionar una mayor seguridad en internet y fortalecer la resiliencia de la red.

La confianza cero presenta un cambio respecto del modelo centrado en la ubicación, que se sustituye por un enfoque centrado en la identidad, el contexto y los datos, con controles de seguridad detallados entre usuarios, sistemas, aplicaciones, datos y activos que cambian con el paso del tiempo. Dado que la resolución del DNS puede estar abierta a terminales que consultan cualquier nombre de dominio público, las organizaciones deben proteger el DNS para evitar que se utilice como ruta para eludir los controles de red de confianza cero, lo que puede requerir la implementación de servicios de DNS protectores o configuraciones específicas de resolución del DNS para ciertos tipos de terminales. La seguridad del DNS es particularmente útil para proteger dispositivos de IoT y la tecnología operativa presentes en la fabricación y las infraestructuras críticas, donde ha sido difícil implementar soluciones de seguridad de puntos finales.

3. VECTORES DE AMENAZAS DEL DNS

La infraestructura del DNS es un vector de amenaza común para las campañas de ataque.[1] Las amenazas al servicio del DNS pueden desencadenar fallos operativos significativos o pérdida de datos, integridad y confidencialidad. Además, muchos actores de amenazas, como ALPHV Blackcat, utilizan dominios maliciosos para lanzar ataques de ransomware a gran escala.[2] A continuación se presenta una lista no exhaustiva de ejemplos de compromisos que podrían poner en peligro no solo los servicios de DNS, sino también todos los sistemas de los que dependen las organizaciones:

a) **Denegación de servicio distribuida:** Un atacante malintencionado puede enviar un gran volumen de consultas para causar un ataque de denegación de servicio (DoS) contra un servidor o servicio del DNS. El atacante puede utilizar numerosos clientes del DNS externos como ayuda en el ataque (DoS distribuido o DDoS).

b) **Cambio de configuración no autorizado:** El archivo de configuración a nivel de plataforma que habilita la comunicación del DNS podría verse dañado o ser objeto de modificaciones no autorizadas debido a protecciones inadecuadas, lo que provocaría interrupciones que van desde la interrupción de la comunicación entre los hosts del DNS hasta el fallo completo del propio servicio del DNS.

c) **Explotaciones de CNAME colgantes:** Cuando un registro CNAME del DNS vincula dos nombres de dominio, existe el riesgo de que el dominio principal del nombre canónico al que apunta el registro ya no esté registrado por la organización objetivo. Como resultado, los actores de amenazas pueden registrar el dominio principal y, por tanto, las resoluciones del DNS apuntarán en última instancia al dominio que controla el actor de amenazas. Otra posible forma en que se pueden explotar los registros CNAME es que el nombre canónico apunte a una dirección IP que el propietario del dominio ya no utiliza y el atacante logre obtener el control de esa dirección IP, con lo que podrá aprovecharla para ejecutar ataques.

d) **Explotación de la delegación inválida:** Los dominios se delegan de un nivel de la jerarquía del DNS a otro, generalmente de un dominio de nivel superior a una organización que registra el dominio. Al establecer la delegación, es necesario especificar los servidores del DNS autoritativos para el dominio. Delegar una zona a cualquier servidor de nombres que no sea autoritativo para esa zona se conoce como delegación inválida o «lame». La delegación inválida puede dar lugar al secuestro del dominio en ciertas circunstancias. Cuando un subdominio se delega a un proveedor de alojamiento del DNS y caduca el contrato para proporcionar servicios del DNS para ese dominio, los actores malintencionados pueden secuestrar su resolución, contratando al proveedor que controla los servidores a los que se dirige la delegación para alojar ese subdominio bajo su control. De este modo, el actor malintencionado puede redirigir las solicitudes de resolución a su propia infraestructura y beneficiarse de la buena reputación del nombre de dominio.

e) **Explotación de dominios similares:** Los actores de amenazas aprovechan ampliamente los dominios similares o de tipo typosquat para hacerse pasar por organizaciones a las que atacan. Al utilizar la reputación positiva de organizaciones legítimas, los actores de amenazas incrementan significativamente la tasa de éxito de sus campañas de phishing y software malicioso. Estos dominios similares pueden incluir variaciones sutiles de dominios legítimos o sustituir texto o caracteres para registrar un dominio que un usuario pueda creer que pertenece a la organización legítima.

f) **DGA y Ransomware como servicio:** Los algoritmos de generación de dominios (DGA) permiten a los actores maliciosos generar numerosos nombres de dominio para la comunicación de comando y control (C2), lo que facilita la distribución de software malicioso y la evasión de la detección. El ransomware como servicio (RaaS), como Blackcat, utiliza el DNS para la comunicación C2.

4. MEJORES PRÁCTICAS DE SEGURIDAD DEL DNS

La función inicial del DNS era distribuir información, por ejemplo, asignaciones de direcciones IP y host, datos de enrutamiento de correo, etc., por lo que tradicionalmente no se consideraba una herramienta para proteger las comunicaciones de red. Sin embargo, el papel que desempeña el DNS para habilitar prácticamente todas las comunicaciones de red hoy en día lo convierte en una

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/

herramienta eficaz tanto para monitorizar como para gestionar esas comunicaciones. Por eso, la seguridad del DNS ha pasado de meramente proteger la infraestructura y los protocolos del DNS a convertirse en un punto de control crítico y un componente clave de la estrategia de seguridad de toda una organización. Hay que tener en cuenta que «DNSSEC» (protocolo llamado Extensión de Seguridad del DNS) es solo una parte de la idea más amplia de la «seguridad del DNS» y debe implementarse junto con otras prácticas recomendadas.

En las siguientes secciones, abordamos los tres componentes clave de las prácticas de seguridad recomendadas del DNS, tales como:

- Utilizar DNS protectores
- Protección del protocolo del DNS
- Protección del servicio y la infraestructura del DNS

4.1 DNS protector

El DNS protector es un servicio del DNS mejorado con capacidades de seguridad para analizar las consultas y respuestas de DNS y tomar medidas capaces de mitigar las amenazas. El DNS protector impide suministrar software malicioso, ransomware, ataques de phishing y otros a través de enlaces web que intentan transmitir spyware y virus, además de bloquear el acceso a sitios web malintencionados. El DNS protector puede proporcionarse como servicio de un proveedor, implementarse mediante una infraestructura del DNS interna o ser una combinación de ambas. Combinar un DNS protector de origen externo con un DNS protector interno aporta beneficios potenciales. Aunque es posible que este enfoque no sea aplicable en todos los casos, recomendamos utilizar el modelo híbrido combinado cuando sea posible. Como demuestran el despliegue de plataformas de DNS protector por parte de gobiernos de todo el mundo y la iniciativa DNS4EU en la Unión Europea,[3] el uso de DNS protector se ha convertido en una práctica recomendada del DNS.

Los resultados de emplear DNS de protección deberían incluir:

- 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 y telemetría

La superficie de ataque de las organizaciones está en constante evolución, por lo que es de suma importancia poder supervisar e interrumpir las comunicaciones maliciosas lo antes posible. El DNS es una constante, aun cuando surgen otras tecnologías de red, y está bien posicionado para proteger a los usuarios en todos los entornos, desde organizaciones hasta terminales móviles. Además, el DNS suele ser la primera conexión con las amenazas y puede detener ataques complejos multietapa antes de que avancen. El DNS, como punto de control de seguridad, no está limitado a un solo tipo de amenaza, a diferencia de otros mecanismos de la pila de seguridad. Puede proteger a los usuarios y las organizaciones frente a estafas, robo de credenciales, ransomware y exfiltración de datos.

Este enfoque requiere threat intelligence y la capacidad de integrarla en el sistema del DNS. La threat intelligence se utiliza en una infraestructura de DNS mediante mecanismos como las zonas de políticas de respuesta (RPZ) y se puede integrar sin problemas en la cadena de resolución del DNS a través de diversas arquitecturas.

b. Filtrado de resolución de nombres

El filtrado de resolución de nombres es un término utilizado para describir la infraestructura del DNS que aplica políticas a su resolución. Estas políticas suelen estar relacionadas con la seguridad: por ejemplo, una implementación de DNS protector puede rechazar resolver un conjunto de nombres de dominio que se sabe que se utilizan en campañas de phishing o que presentan la infraestructura de comando y control de software malicioso. En lugar de resolver estos nombres de dominio y proporcionar direcciones IP u otros tipos de datos, el DNS protector suele devolver otra forma de respuesta del DNS, como NXDOMAIN (que significa «dominio inexistente»), para indicar que el nombre de dominio consultado no existe. Las implementaciones de DNS protector también pueden registrar consultas para nombres de dominio que activan políticas, ya que esas consultas pueden indicar una infección por malware u otra actividad maliciosa.

El DNS protector suele implementarse mediante el uso de RPZ configuradas en un servicio de DNS in situ, un servicio de DNS recursivo seguro en la nube o una combinación de ambas opciones.

Los servicios de DNS recursivo seguro también están disponibles en internet. Los servicios suelen ofrecen un panel de control basado en la web, que permite a los administradores personalizar la política de resolución aplicada a las consultas de los clientes de la organización. El enfoque en la nube ofrece mayor escalabilidad, almacenamiento y potencia de cálculo, pero tiene desventajas, como la pérdida de confidencialidad, una mayor latencia y dificultades para atribuir las consultas al DNS de forma rápida y precisa a su origen. Las organizaciones pueden plantearse la opción de combinar los servicios de DNS seguro in situ con los basados en la nube para aprovechar los beneficios de cada uno de ellos. La mejor opción para una implementación concreta del DNS varía en función de las necesidades específicas de la red y sus usuarios.

c. DNS para la informática forense digital y la respuesta a incidentes

Las agencias gubernamentales y las empresas reguladas deben aplicar mecanismos robustos para registrar el tráfico del DNS a fin de cumplir los requisitos normativos. El registro debe capturar tanto el tráfico del DNS actual como el histórico para habilitar el análisis forense digital y la respuesta ante incidentes. Estos registros del DNS deben integrarse con otros registros del sistema para facilitar la correlación con la actividad de la red y así mejorar la visibilidad y la facilidad de auditoría.

En los casos en que se determine que el registro completo del tráfico del DNS consume demasiados recursos, las organizaciones pueden plantearse usar soluciones en la nube, métodos de registro eficientes (p. ej., DNSTAP) o un registro selectivo. Sin embargo, es imperativo que las consultas y respuestas del DNS asociadas con dominios clasificados como maliciosos o no autorizados por los servicios del DNS protector se registren siempre, para reforzar los principios de seguridad y cumplimiento. Para garantizar que se notifiquen rápidamente las consultas que puedan indicar una infección o actividad maliciosa, las organizaciones deben integrar los registros del DNS protector de sus servidores de nombres o su servicio de DNS recursivo seguro en su plataforma SIEM o de análisis de registros.

4.2 Protección del protocolo del DNS

El protocolo del DNS es fundamental para localizar servicios que posibiliten la navegación web, el correo electrónico y otras aplicaciones críticas para la misión. Como resultado, las plataformas de seguridad tradicionales, como los firewalls de última generación, a menudo dejan pasar el tráfico del DNS sin obstáculos ni inspección. Los actores de amenazas recurren cada vez más al DNS como vector de exfiltración. Según la Agencia de Ciberseguridad y Seguridad de las Infraestructuras de Estados Unidos (CISA), «la infraestructura del DNS es un vector de amenazas común en campañas de ataque».[4] Los actores de amenazas incrustan con frecuencia datos robados en paquetes DNS, confiando en que la infraestructura del DNS envíe los datos robados a servidores DNS controlados por los actores de amenazas. Las plataformas DNS están idealmente posicionadas para evaluar las solicitudes recursivas al DNS que tratan de exfiltrar datos.

a. Protección de la integridad de los servicios DNS

Proteger la integridad del protocolo del DNS es crucial para garantizar la seguridad y la fiabilidad de las comunicaciones en internet. Las extensiones de seguridad del DNS (DNSSEC) desempeñan un papel crucial, al utilizar firmas criptográficas para autenticar las respuestas del DNS y prevenir ataques como el envenenamiento de la caché e intercepciones con intermediarios (man in the middle). Además, el protocolo Transaction Signature (TSIG) mejora la seguridad del DNS, puesto que permite la autenticación mutua y la verificación de la integridad entre los servidores del DNS y utiliza claves secretas compartidas para proteger las transferencias de zona y las actualizaciones dinámicas frente a cambios no autorizados. Implementar estos mecanismos, junto con buenas prácticas como la limitación de la velocidad, la supervisión de anomalías y la aplicación de controles de acceso estrictos, permite mantener la confianza y la resiliencia de la infraestructura del DNS frente a ciberamenazas en continua evolución. Además, las organizaciones deben asegurarse de que los usuarios no utilicen, deliberada o accidentalmente, servicios de DNS públicos no autorizados y basados en internet.

b. Uso de DNS cifrado y autenticaciones para proteger el protocolo

Tradicionalmente, la comunicación entre los sistemas de resolución y los servidores recursivos del DNS que consultan no se cifraba. Los mensajes del DNS intercambiados entre los sistemas de resolución y los servidores del DNS son en código binario, código ampliamente comprendido y fácil de decodificar. Por lo tanto, estas comunicaciones han sido objeto de interceptación y suplantación, lo que revela información sensible y permite a los atacantes redirigir usuarios desprevenidos hacia sitios maliciosos.

Para abordar estas amenazas, el Grupo de Trabajo de Ingeniería de Internet (IETF) ha desarrollado varias mejoras para el DNS, comúnmente conocidas como DNS cifrado. Todos estos protocolos cifran las comunicaciones entre los sistemas de resolución y los servidores recursivos del DNS y, como opción, permiten que los servidores recursivos del DNS se autentiquen ante los sistemas de resolución para contrarrestar amenazas de interceptación y suplantación.

c. Higiene y prácticas recomendadas del DNS

La explotación de errores de configuración y el registro de dominios/sistemas de resolución del DNS caducados es relativamente sencillo para los actores de amenazas y puede dar lugar a problemas graves en cuanto a la integridad del DNS.

Los actores de amenazas han demostrado que ataques como el phishing tienen muchas más probabilidades de tener éxito si están vinculados a dominios propiedad de organizaciones de confianza. Como resultado, a menudo registran dominios similares que se asemejan a los de la organización objetivo, pero que no son de su propiedad. Lo que resulta aún más inquietante es que una mala gestión de los dominios autorizados puede permitir que actores de amenazas tomen control de dominios pertenecientes a organizaciones que se consideran fiables.

4.3 Protección del servicio y la infraestructura del DNS

Los dispositivos del DNS, al igual que otros dispositivos de red, están diseñados específicamente para optimizar la facilidad de gestión, seguridad y rendimiento. Los servidores de propósito general no pueden igualar la configuración que ofrecen estos dispositivos y, como tales, exponen a las organizaciones a riesgos significativos, dada la importancia del DNS como servicio de red.

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

Las organizaciones suelen utilizar servidores Windows que alojan DNS y DHCP junto con Active Directory (AD), otra infraestructura de identidad esencial para el funcionamiento de una organización. AD administra el acceso y los permisos de los usuarios y almacena información relevante, lo que genera una amplia superficie de ataque vulnerable a ataques cibernéticos.

Sin esta separación de funciones, si un atacante siguiera una ruta de escalada común y se dirigiera a Active Directory, esto pondría en riesgo el servicio DNS y la red de la que depende. A medida que el DNS adquiere un papel más importante en la estrategia de ciberseguridad de una organización, será esencial contar con un servidor DNS dedicado para mitigar estos riesgos.

Del mismo modo, los actores de amenazas suelen tratar de aprovechar las vulnerabilidades detectadas en el DNS que pueden afectar a la integridad del sistema del DNS o dar lugar a una denegación de servicio.

Para obtener más orientación sobre DNS seguro, consulte la versión más reciente de la guía NIST SP 800-81: Secure Domain Name System (DNS) Deployment Guide.

5. RESUMEN Y RECOMENDACIONES

Este documento técnico analiza la importancia crítica de la infraestructura del DNS para mantener la resiliencia digital y la ciberseguridad de una organización. Destaca la necesidad de efectuar evaluaciones periódicas de los servidores del DNS para garantizar que tienen capacidad suficiente y están configurados de manera óptima. También hace hincapié en el papel del DNS como capa fundamental en la arquitectura de la ciberseguridad, que beneficia a todos los clientes que utilizan su infraestructura.

Para hacer frente a las amenazas a la seguridad del DNS en constante evolución, presentamos las siguientes recomendaciones generales, dirigidas a responsables de redes y seguridad:

- Utilice el DNS protector siempre que sea técnicamente factible, para proporcionar opciones de seguridad adicionales a toda la red, como:
  - » Bloqueo de tráfico dañino o malicioso en tiempo real,
  - » El filtrado de categorías de tráfico que no cumplen las políticas de la organización,
  - » Datos de consulta y respuesta del DNS en tiempo real e históricos para facilitar la investigación forense digital y la respuesta ante incidentes,
  - » La integración con el ecosistema de seguridad más amplio como parte de un enfoque de defensa en profundidad o de confianza cero, y
  - » La facilitación de la responsabilidad de una organización para cumplir los requisitos reglamentarios o contractuales en cuanto a bloquear el tráfico a sitios no permitidos (violaciones de derechos de autor, restricciones legales, etc.).
- Cifre el tráfico del DNS, tanto interno como externo, siempre que sea factible.
- Implemente servidores del DNS específicos para reducir la superficie de ataque.
- Siga todas las guías técnicas para que sus implementaciones del DNS y el protocolo del DNS sean lo más seguros y resilientes posible.

Para obtener más información, póngase en contacto con el equipo de Infoblox en ga@infoblox.com.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com

Versión: 20250131v3