MYRA

THREAT FACT SHEET DNS ATTACKS

Alles, was Sie über DNS-Attacken wissen müssen

Angriffe auf das Domain Name System (DNS) zählen zu den größten Bedrohungen in der modernen Internet-Landschaft. Insbesondere Organisationen mit geschäftskritischen Online-Prozessen sind durch DNS-Angriffe gefährdet.

Die Technologie zur Namensauflösung ordnet Domains den zugehörigen IP-Adressen zu – etwa für Webseiten, VoIP-, E-Mail- oder Streaming-Dienste. Erst durch eine erfolgreiche Namensauflösung wissen Webbrowser auf Smartphones oder PCs, welche Webserver die Inhalte für eine spezifische Webseite bereithalten.

Das Konzept des DNS als Telefonbuch des Web stammt noch aus den Anfangstagen des Internets, als es weder Cyberkriminalität noch Tracking oder digitale Zensur gab. Daher wurde damals auf Verschlüsselungsmethoden bei der Übertragung von DNS-Anfragen verzichtet. Standardmäßig erfolgt die Übertragung ungesichert im Klartext. Diese Schwachstelle macht die Technologie zu einem mächtigen Werkzeug für Angreifer.

Durch Manipulationen an der Delegationsstruktur von Domainnamen können Kriminelle die IP-Adressen von Webservern austauschen, um Traffic gezielt auf andere Systeme umzuleiten. Somit lassen sich User etwa auf gefälschte Webseiten führen, um ihre Logindaten abzugreifen, Malware zu verbreiten oder Desinformationen zu streuen. Hierbei handelt es sich um unterschiedlichste Formen des DNS Spoofing. Darüber hinaus können Angreifer auch das DNS als Werkzeug missbrauchen, um massive DDoS-Attacken (Distributed Denial of Service) auf Webseiten, Online-Portale oder Web-APIs zu starten.

Welches Bedrohungspotenzial Angriffe auf das DNS besitzen, zeigte sich etwa 2019. Damals warnte die Internetverwaltung ICANN (Internet Corporation for Assigned Names and Numbers) eindringlich vor einer globalen DNS-Hijacking-Kampagne, die dutzende Domains von Regierungs-, Telekommunikations- und Internet-Infrastruktur-Organisationen in Europa, Nordamerika, Nordafrika sowie im Nahen Osten betraf. Verantwortlich für die Angriffe sollen Akteure mit staatlichem Hintergrund gewesen sein, die primär politische Ziele verfolgten.

Durch den Einsatz einer abgesicherten DNS-Infrastruktur (Secure DNS) schützen sich Unternehmen vor solcherlei Attacken, welche die Verfügbarkeit, Integrität und Vertraulichkeit von betroffenen Geschäftsprozessen massiv gefährden.

Das folgende Threat Fact Sheet liefert einen Überblick über DNS-basierte Cyberbedrohungen und stellt effektive Möglichkeiten zur Verteidigung vor.

Inhalt

Was ist das DNS und wo liegen die Schwachstellen? 3
Wie funktioniert eine DNS-Abfrage? 3

Cyberrisiken rund um DNS 4
DNS Cache Poisoning 5
DNS Hijacking 6
DNS Reflection & Amplification 7

Schutzmaßnahmen für und vor DNS 8

Vorzüge von Security-as-a-Service-Lösungen für den DNS-Schutz 9

Schutzbedarf und Compliance-Vorgaben bei der Dienstleisterwahl 9

Myra Secure DNS sichert Verfügbarkeit und globale Performance 10

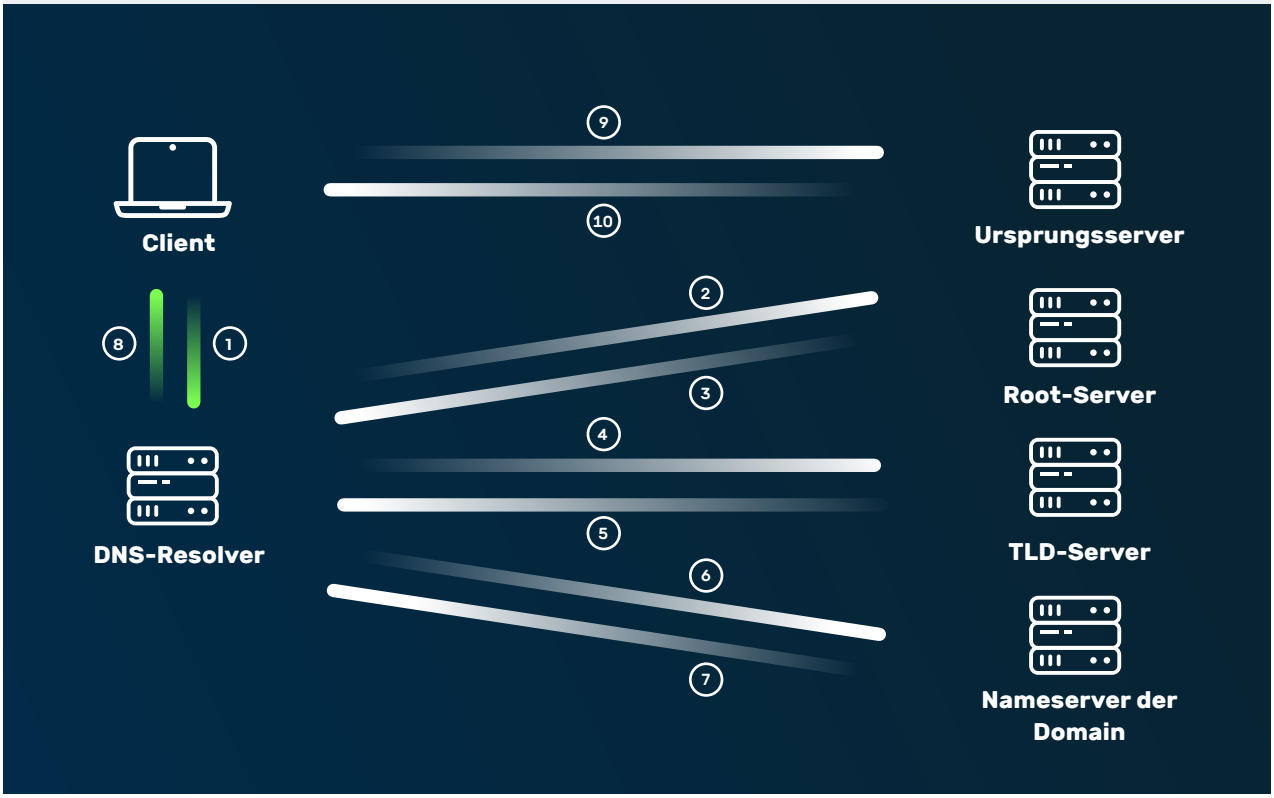
Was ist das DNS und wo liegen die Schwachstellen?

Das DNS ist ein weltweit verteilter hierarchischer Verzeichnisdienst, welcher der Zuordnung von Domains zu den dazugehörigen IP-Adressen im Internet dient. Über das DNS können damit Domainnamen wie myrasecurity.com einer konkreten IP-Adresse des Webservers zugewiesen werden.

Wie funktioniert eine DNS-Abfrage?

Eine DNS-Abfrage ist immer dann erforderlich, wenn der Computer die für einen Webseitenaufruf benötigten Adressinformationen nicht im Cache vorliegen hat und der vorkonfigurierte DNS-Dienst des Internetdienstanbieters die Namensauflösung ebenfalls nicht bewerkstelligen kann. Im Detail läuft eine DNS-Anfrage nach folgendem Muster ab:

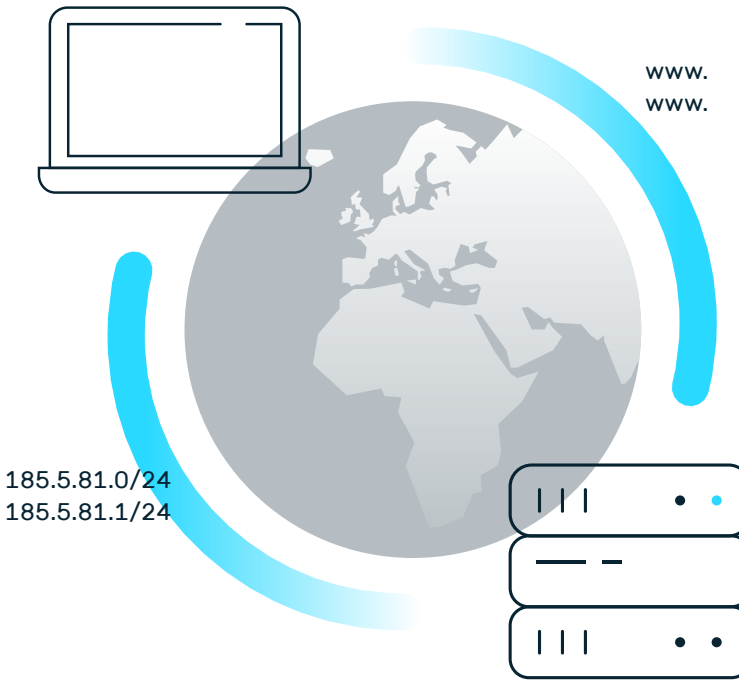
1. Eingabe der URL einer Website im Browser (z. B. www.myrasecurity.com). Das Betriebssystem überprüft den DNS-Cache anhand der Anfrage. Falls die Adresse nicht im Cache liegt, wird die Anfrage an den DNS-Resolver geleitet.
2. Der DNS-Resolver kontaktiert darauf den DNS-Root-Server.
3. Der Root-Server gibt dem Resolver an, unter welcher Top-Level-Domain die Information für die Website zu finden ist. Im Fall von www.myrasecurity.com handelt es sich um die Top Level Domain (TLD) .com
4. Der Resolver schickt eine Anfrage an den entsprechenden TLD-Server.
5. Der TLD-Server gibt die IP-Adresse des entsprechenden autoritativen DNS-Servers der gesuchten Domain an.
6. Der DNS-Resolver erfragt beim autoritativen DNS-Server die IP-Adresse des Ursprungsservers, auf dem die Website gehostet ist.
7. Der Nameserver gibt die Adresse des Ursprungsservers an den DNS-Resolver weiter.
8. Der Resolver leitet die IP-Adresse an den Browser des Clients weiter.
9. Der Browser ruft nun die Website auf, indem er eine HTTP-Anfrage an die IP-Adresse schickt.
10. Der so angesprochene Server schickt die Dateien der Website an den Browser, sodass der Content angezeigt wird.



Die Delegierung der Anfragen über das User Datagram Protocol (UDP) erfolgt im DNS unverschlüsselt im Klartext, eine Verifizierung der DNS-Einträge findet nicht statt. Das macht die Namenszuordnung grundsätzlich anfällig für externe Angriffe, Manipulation, Überwachung oder Zensur. Betroffen von diesen Risiken sind sowohl die auf das DNS zugreifenden Clients und DNS-Infrastrukturen als auch Organisationen, die Ziel einer DNS-basierten Überlastungsattacke werden.

Manipulationen an der DNS-Delegationsstruktur erlauben es Angreifern etwa, Datentraffic auf andere IP-Adressen umzuleiten. So lassen sich Internetanwender:innen unbemerkt auf gefälschte Plattformen locken, um deren Account-Daten zu stehlen, Schadsoftware zu verbreiten oder Fake News zu streuen. Solche Angriffsmethoden auf das DNS werden als Spoofing-Attacken beziehungsweise DNS Cache Poisoning oder auch DNS Hijacking bezeichnet.

Ebenso sind Zensur- und Blockademaßnahmen gegen einzelne Webseiten über das DNS möglich. So greifen etwa autokratische Staaten oftmals auf DNS-Blockaden zurück, um unliebsame Social-Media-Plattformen oder die Webpräsenz der politischen Opposition zu zensieren. Dabei werden DNS-Anfragen mit einer Blocklist abgeglichen und bei Treffern mit einer spezifischen IP-Adresse beantwortet. Auf dieselbe Weise blockieren auch Netzbetreiber illegale Plattformen im Netz.



Cyberrisiken rund um DNS

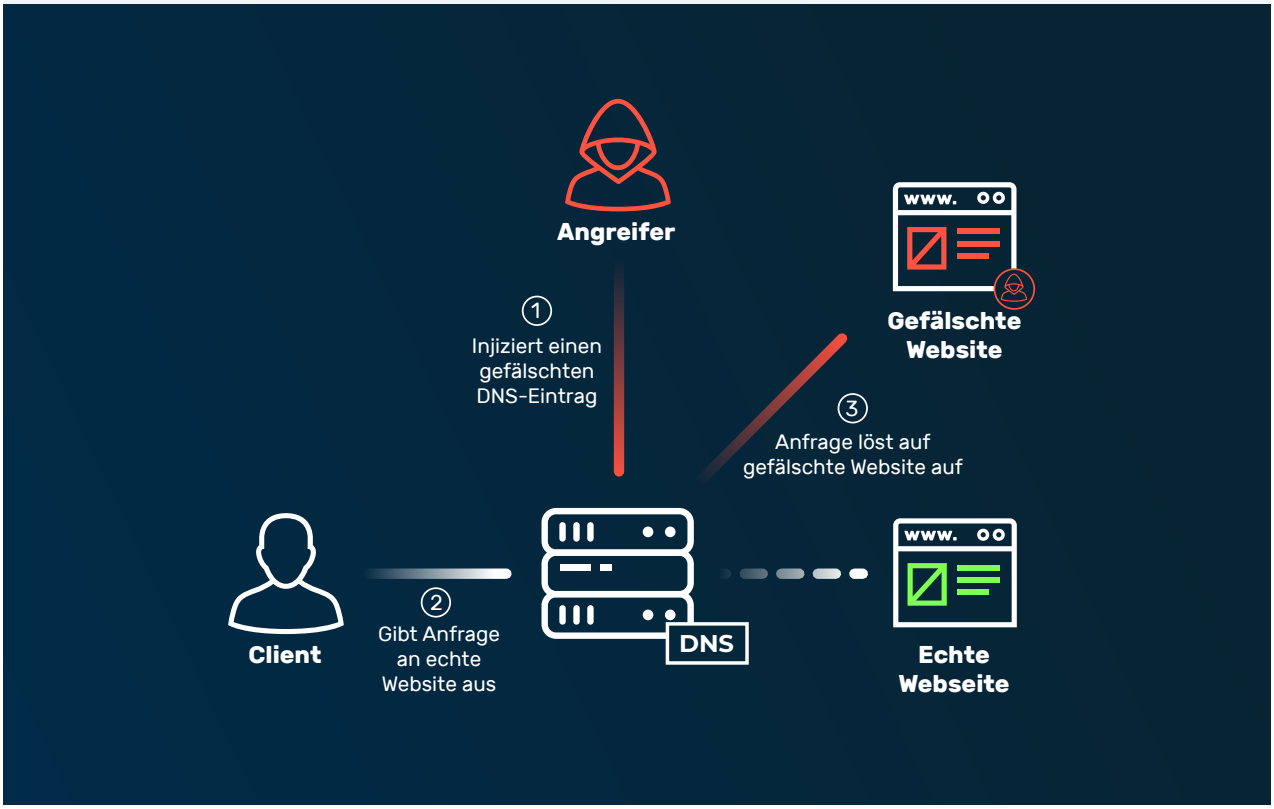
Zu den geläufigsten DNS-basierten Cyber-angriffsmethoden zählt das DNS Spoofing. Hierbei handelt es sich um einen Sammelbegriff für schädliche DNS-Manipulationen, die auf eine Umleitung von Internetnutzer:innen auf eine bestimmte Ressource abzielen. Zu DNS Spoofing gehören etwa Attacken mittels DNS Cache Poisoning, bei dem manipulierte Einträge in den DNS Cache von Nameservern geschmuggelt werden, oder DNS Hijacking, bei dem Cyberkriminelle darauf abzielen, mittels Schadsoftware oder durch die Ausnutzung von Sicherheitslücken die Kontrolle über DNS-Einstellungen auf Clints, Servern und DNS-Infrastruktur zu übernehmen.

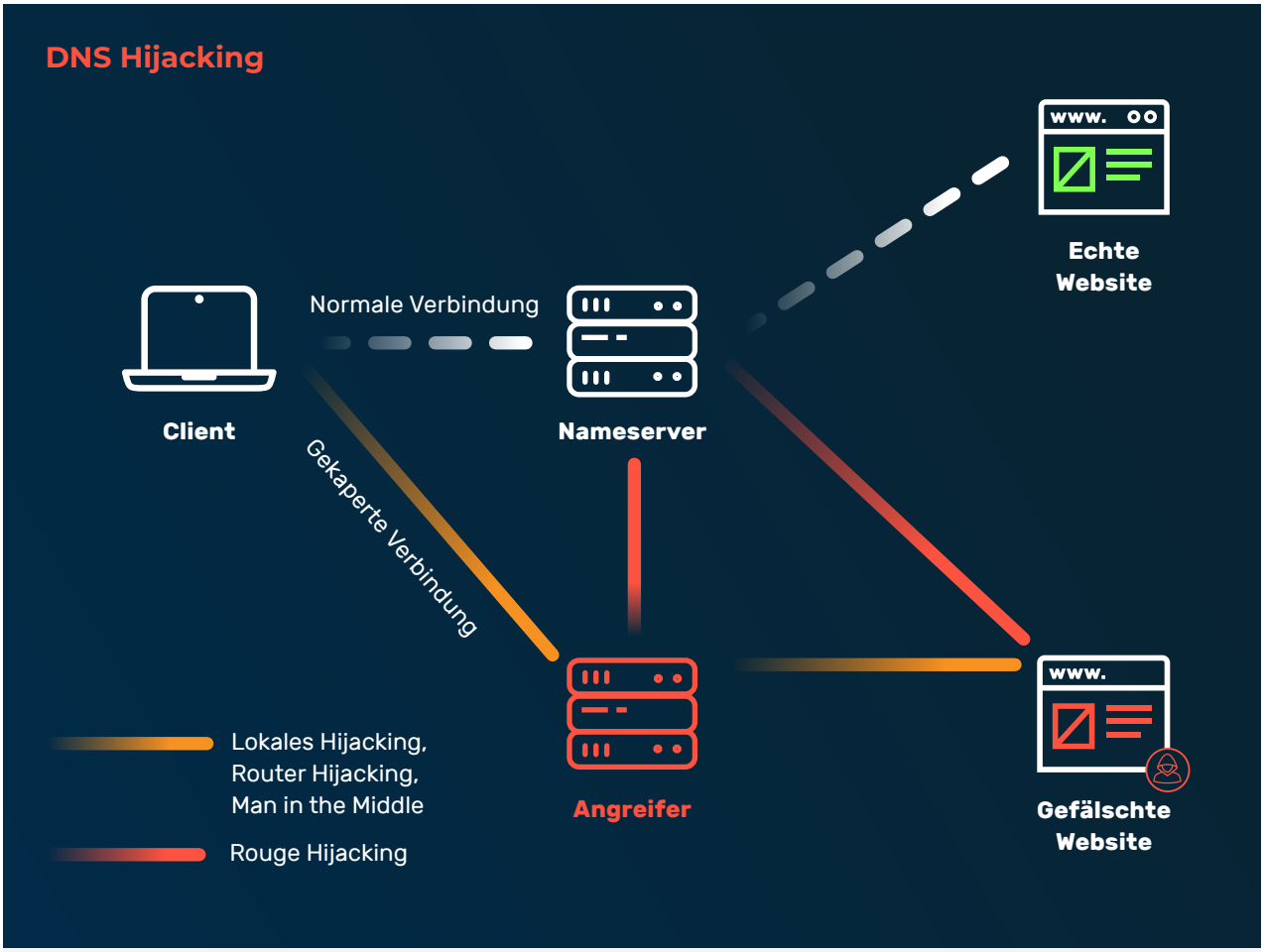
Kriminelle nutzen die gezielte Traffic-Umleitung über das DNS aber nicht nur für Spoofing-Angriffe, auch DDoS-Attacken sind über DNS-Server möglich. Hierbei handelt es sich um sogenannte DNS Reflection & Amplification Attacks. Angreifer senden bei dieser Methode die schädlichen Anfragen „über Bande" zu einem DNS-Server, der diese mit höherer Traffic-Last an den Webserver des anvisierten Unternehmens weiterleitet. Ungeschützte Server-Instanzen gehen bei solchen Anfragen meist in die Knie oder arbeiten zumindest stark verzögert aufgrund der hohen Auslastung.

Darüber hinaus sind Nameserver oft auch selbst das Ziel von DDoS-Attacken. Wenn Cyberkriminelle mit ihren Überlastungsangriffen auf die Webserver einer Organisation keinen Erfolg haben, schwenken sie den schädlichen Traffic meist auf die DNS-Infrastruktur um und versuchen, diese lahmzulegen. Geht der für die Namensauflösung verantwortliche Nameserver in die Knie, ist auch die dahinterliegende Webressource nicht mehr erreichbar.

DNS Cache Poisoning

Beim Cache Poisoning missbrauchen Cyberkriminelle die Funktionsweise des DNS, um Internetnutzer:innen unbemerkt auf gefälschte Webseiten zu locken und dort deren Zugangsdaten und andere sensible Informationen zu stehlen. Gelingt es Angreifern, einen Nameserver über Sicherheitslücken zu korrumpieren und gefälschte Einträge in die Delegationsstruktur einzuschleusen, gelangen die manipulierten Einträge auch in den Cache anfragender Server, Router und Endgeräte, die die betroffene Domain auf dem Nameserver anfragen. Der DNS Cache ist nun „vergiftet“ und leitet User auf die von den Angreifern festgelegte Webseite um. Letztere ist zumeist darauf ausgelegt, Logindaten zu stehlen oder Schadsoftware zu verbreiten.





DNS-Hijacking beschreibt eine Angriffstechnik, bei der Angreifer DNS-Einträge manipulieren, um Anfragen auf betrügerische Websites umzuleiten. Dies kann durch die Kompromittierung von Client-PCs, Routern, DNS-Servern oder durch das Abfangen von DNS-Anfragen erfolgen. Abhängig vom jeweils betroffenen System unterscheidet die IT-Sicherheit hier zwischen „lokalem Hijacking", „Router Hijacking", „Rogue-DNS-Server-Angriffen" und „Man-in-the-Middle-Angriffen".

Lokales Hijacking findet direkt auf dem Client-PC von Anwender:innen statt. Über Trojaner wie Win32/DNSChanger werden hierbei lokal die DNS-Einstellungen im Betriebssystem verändert, um Anfragen im Webbrowser umzuleiten.

Router Hijacking erfolgt auf dem Router im Heim- oder Unternehmensnetzwerk. Insbesondere auf preiswerten Consumer-Lösungen kommen oftmals Standardpasswörter zum Einsatz. Werden diese Logindaten nicht manuell angepasst, können Cyberkriminelle mittels Credential Stuffing die Zugänge zu den Administrationsportalen kapern und die DNS-Einstellungen des Routers manipulieren. Die Webanfragen der verbundenen Geräte werden nach der Manipulation auf die von den Cyberkriminellen definierten, meist schädlichen Webseiten geleitet.

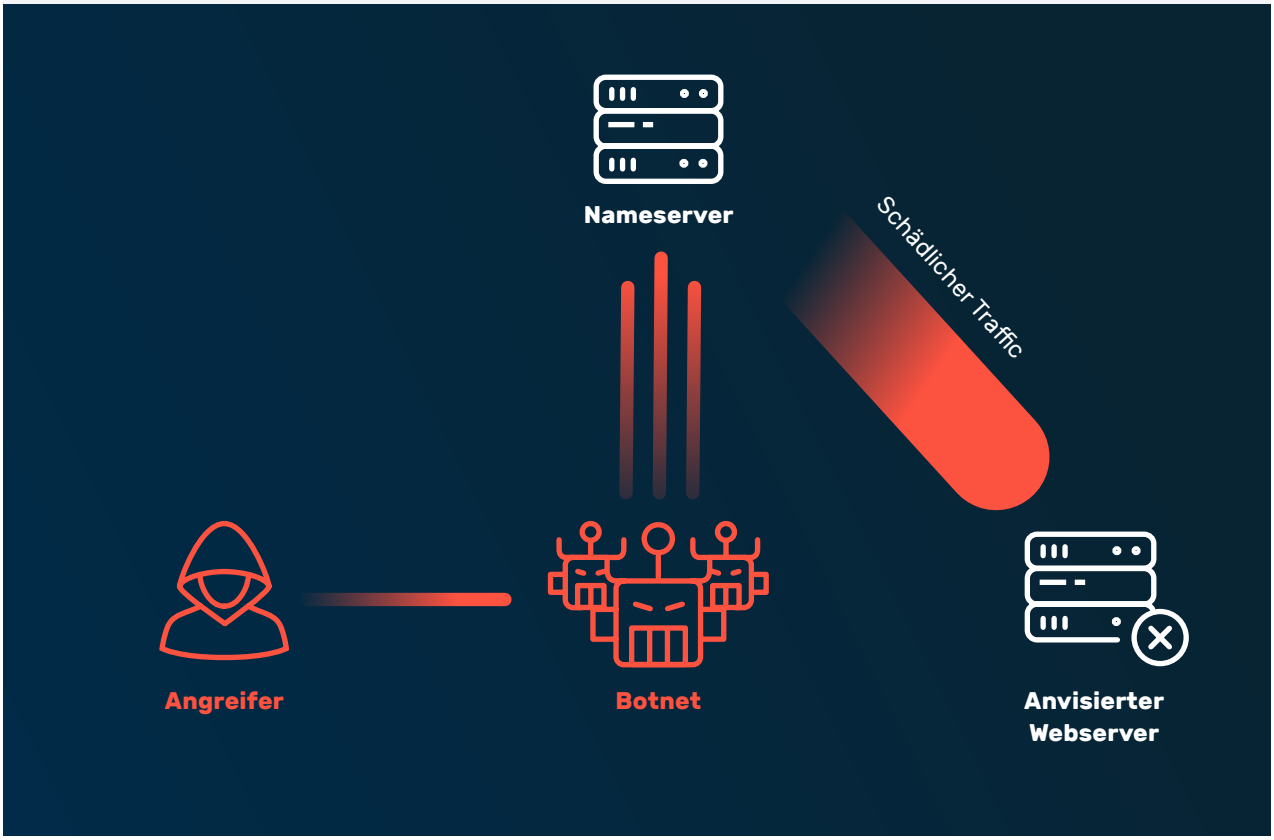
Rouge Hijacking beschreibt einen direkten Angriff auf die DNS-Infrastruktur. Durch den Einsatz von Malware oder unter Ausnutzung von Software-Schwachstellen kompromittieren Cyberkriminelle bei Rouge Hijacking beispielsweise die Nameserver von Internetdienstanbietern (ISPs). In der Folge erhalten alle bei diesem Nameserver anfragenden Geräte die manipulierten Einträge geliefert.

Man-in-the-Middle-Attacken nutzen Cyberkriminelle, um Datenpakete während der Kommunikation zwischen Client und Server abzugreifen und zu manipulieren. Bei solchen Attacken machen es sich Angreifer zunutze, dass die allermeisten DNS-Anfragen unverschlüsselt und ohne Verifizierung gesendet werden.

DNS Reflection & Amplification

Nameserver kommunizieren standardmäßig über UDP. Im Gegensatz zum Transmission Control Protocol (TCP) ist UDP ein verbindungsloses Protokoll. Das DNS-Protokoll per se bietet keine Möglichkeit für den Empfänger von Paketen, die Integrität des Senders zu prüfen. Daher liefern DNS-Server die Antworten strikt an die IP-Adresse, die im Anfragen-Paket hinterlegt ist. Diesen Fakt machen sich Cyberkriminelle zunutze. Sie platzieren bei ihren Angriffen mittels IP-Spoofing die IP-Adresse des Ziels als Quelladresse. Dadurch leitet der DNS-Server die Antwort an die Webserver der betroffenen Organisation um (Reflection). Dies geschieht in der Regel aber nicht nur von einem einzigen Rechner aus, sondern parallel durch Tausende Systeme, die in einem Botnetz organisiert sind.

Die UDP-Pakete von DNS-Abfragen sind typischerweise sehr klein. Deutlich größer fallen hingegen die Antwortpakete aus. Bei Unterstützung von DNSSEC fallen die Antworten nochmals deutlich größer aus. Angreifer können diese Eigenschaften missbrauchen, um das Volumen ihrer Attacken massiv zu steigern (Amplification). Laut US-CERT liegt der Amplifizierungsfaktor bei DNS zwischen 28 und 54.



Schutzmaßnahmen für und vor DNS

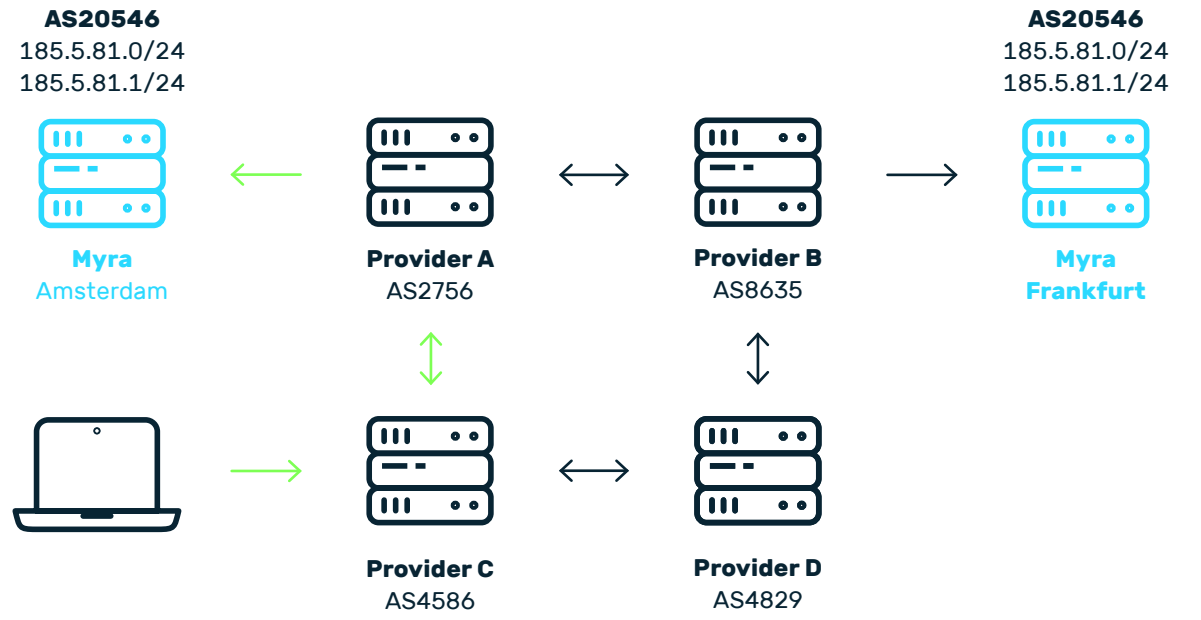
Eine abgesicherte DNS-Infrastruktur setzt auf verschiedene Schutz- und Performance-Systeme, die zur Aufrechterhaltung von Integrität, Vertraulichkeit und Verfügbarkeit dienen. Hierzu zählt die Unterstützung für DNS-Erweiterungen wie DNSSEC, die zur Validierung von DNS-Anfragen zum Einsatz kommen und schädliche Manipulationen durch DNS Spoofing in der Delegation verhindern. Indessen ist durch die Implementierung von verschlüsselten Protokollen wie DNS over HTTPS (DoH), DNS over TLS (DoT) oder DNSCrypt eine Absicherung der Namensauflösung vor Man-in-the-Middle-Attacken und DNS-basierten Zensurmaßnahmen möglich.

Der Einsatz von Verschlüsselungstechnologien kann aber auch zu Kompatiblitätsproblemen führen. Vor allem die Kommunikation im IoT (Internet of Things) oder IIoT (Industrial Internet of Things) lässt sich nicht ohne Weiteres auf verschlüsselte DNS-Übertragungen umstellen. Viele vernetzte Sensoranlagen in der Produktion oder auch andere IoT-Geräte sind softwareseitig nicht erweiterbar.

Darüber hinaus ist insbesondere beim Einsatz von DoH ein zentraler Provider erforderlich, bei dem alle Fäden zusammenlaufen – das Tracking-Potenzial besteht also weiterhin. Vor diesem Hintergrund ist eine individuelle Evaluierung der Technologie für den jeweiligen Einsatzzweck unbedingt erforderlich.

Darüber hinaus bietet der Einsatz von gehärteten DNS-Serverinstanzen im georedundanten Anycast-Betrieb Schutz vor DDoS-Angriffen. Für das Anycast-Routing wird das Border Gateway Protocol (BGP) genutzt, das auch standardmäßig bei allen Internet Service Providern (ISP) für den Aufbau ihrer Netze zum Einsatz kommt. Einzelne Server können dabei nicht gezielt von Angreifern angegangen werden, da allen Server-Instanzen dieselbe IP-Adresse zugeordnet ist und eingehende Anfragen über BGP-Peering immer vom schnellsten erreichbaren Server beantwortet werden. So verteilt sich die Last flexibel auf das gesamte Servernetzwerk. Nach demselben Prinzip arbeiten auch die 13 Root-Nameserver, die sich aus mehr als 1.600 Serverinstanzen zusammensetzen.

Beispiel für Anycast Routing



BGP-Routingtabelle für 185.5.81.0/24

AS path1:	4586	2765*		
AS path2:	4586	4829	8635	
AS path3:	4586	4829	8635	2756

*Aktive Route

Vorzüge von Security-as-a-Service-Lösungen für den DNS-Schutz

Das DNS ist ein weltweit verteilter hierarchischer Verzeichnisdienst, welcher der Zuordnung von Domains zu den dazugehörigen IP-Adressen im Internet dient. Über das DNS können damit Domainnamen wie myrasecurity.com einer konkreten IP-Adresse des Webservers zugewiesen werden.

Die oben genannten Sicherheitslösungen gegen schädliche Manipulationen in der DNS-Delegation und gegen Überlastungsangriffe auf Webserver bilden einen holistischen Schutz für die DNS-Infrastruktur. Während jedoch die Unterstützung von DNS-Erweiterungen wie DNSSEC oder verschlüsselten Protokollen noch in den meisten Organisationen inhouse abzubilden ist, schließt der Anycast-Betrieb die eigene Bereitstellung von Nameservern in den allermeisten Fällen aus. Der Aufwand für Aufbau, Betrieb und Wartung eines ganzen Netzwerks an Serverinstanzen ist massiv. Für eine dedizierte Absicherung von DNS-Servern ist das Outsourcing an einen Security-as-a-Service-Dienstleister daher die beste Wahl.

In der Praxis ergeben sich durch das Outsourcing mehrheitlich Vorteile, denn die erforderliche Konfigurationsfreiheit besteht auch beim Dienstleister. Unterstützt der Schutzanbieter Hidden-Primary-Konfigurationen, ist auch der Umzug der Namensauflösung samt zugehöriger Konfigurationen schnell und einfach umzusetzen.

Schutzbedarf und Compliance-Vorgaben bei der Dienstleisterwahl

Zur Auswahl eines passenden Schutzanbieters für eine abgesicherte DNS-Infrastruktur müssen Unternehmen zunächst die individuellen Anforderungen definieren. Schutzfunktionalität, Bereitstellungsart, Performance und Compliance-Vorgaben zählen dabei zu den zentralen Kriterien.

Führende Anbieter bieten holistische Schutzsysteme, die Unternehmen einerseits vor einem Missbrauch von DNS-Servern schützen sowie andererseits direkte Angriffe auf die Namensauflösung selbst verhindern. Hierzu zählen eine gehärtete DNS-Serverinfrastruktur, Anycast-Routing sowie DNSSEC-Support.

Daneben müssen bei der Dienstleisterwahl die geltenden regulatorischen Anforderungen beachtet werden. Internationale Compliance-Regelwerke wie die Datenschutz-Grundverordnung (DSGVO), die NIS-2-Richtlinie (NIS-2) oder den Cyber Resilience Act (CRA) gilt es hierbei zu adressieren – insbesondere, wenn Unternehmen in hochregulierten Sektoren wie der Finanz- und Versicherungsindustrie, dem Gesundheitswesen oder der öffentlichen Verwaltung tätig sind. Spezialanbieter sind mit diesen Vorgaben vertraut und besitzen im Idealfall die erforderlichen Zertifizierungen und Prozesse, um selbst hohe regulatorische Herausforderungen zu bewältigen. Zu den relevantesten Zertifizierungen und Audits zählen etwa ISO 27001 (auf Basis von BSI IT-Grundschutz), BSI C5 (Typ 2) oder eine KRITIS-Qualifikation nach §8a Absatz 3 BSI-Gesetz.

Myra Secure DNS sichert Verfügbarkeit und globale Performance

Secure DNS von Myra Security umfasst eine globale DNS-Serverinfrastruktur, bei der die Namensauflösung mittels Anycast-Routing erfolgt. Secure DNS wird auf speziell gehärteten Serverinstanzen betrieben und durch dieselbe BSI-zertifizierte Schutztechnologie abgesichert, die zahlreiche deutsche Behörden auf Bundes-, Landes- und Kommunalebene zur Verteidigung ihrer Domains vor Cyberangriffen einsetzen.

Als Security-as-a-Service-Lösung ist Secure DNS von Myra in kurzer Zeit implementiert und einsatzbereit. Zusätzliche Software oder Hardware sind für den Betrieb nicht erforderlich. Myra ist langjähriger Service-Partner diverser Bundes-, Landes- und Kommunalbehörden, namhafter Banken und Versicherungen sowie von Betreibern kritischer Infrastrukturen (KRITIS).

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021

PCI DSS Certified

BSIG KRITIS-qualifiziert

BSI C5 TESTAT TYP 2

Trusted Cloud

ISAE 3402 IDW PS 951 TYPE 2

DIN EN 50600 zertifiziert BETRIEBSSICHERES RECHENZENTRUM

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard (PCI DSS) | KRITIS-qualifiziert nach §3 BSI-Gesetz | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600

Made in Germany

Myra Security ist der neue Maßstab für globale IT-Sicherheit.

Sie wollen mehr darüber erfahren, wie Sie mit unseren Lösungen Ihren Umsatz steigern, Ihre Kosten minimieren und Ihre Anwendungen vor bösartigen Angriffen schützen? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihr Unternehmen. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.

Kostenlose Demo anfordern →

Myra Security GmbH

+49 89 414141 - 345
www.myrasecurity.com
info@myrasecurity.com