Domain Name System

What happens when you make a DNS request?

Schritt 1: Der Computer schaut im lokalen cache, ob die Adresse schonmal gesucht wurde. Wenn ja, endet die Request. Wenn nicht wird der Recursive Server requested

Schritt 2: Der Recursive Server wird vom Internetanbieter (ISP) vorgegeben, man kann aber auch ein eigenen wählen. Dieser schaut ebenfalls im lokalen Cache, ob die Adresse schonmal gesucht wurde. Wenn ja endet die Request. Wenn nicht wird der Root Server requested.

Schritt 3: Der Rootserver ist das Rückgrat des Internets und leitet die Anfrage zum richtigen TLD Server.

Schritt 4: Der TLD Server hat Informationen darüber wo man den authoritative server findet. Dort endet die Anfrage.

Schritt 5: Für eine Domain gibt es oft mehrere authoritative server/nameserver, die als backup dienen, falls eine down ist.

Schritt 6: Ein authoritative server ist der Server, der für die Speicherung von DNS Records für einen bestimmten Domainnamen verantwortlich ist und auf dem alle Updates der DNS-Records des Domainnamens vorgenommen werden. Der DNS-Record wird dann zum Recursive Server gesendet um dort eine Kopie im cache zu speichern, welche dann an den Client weitergeleitet wird, der die Anfrage gestellt hat. Alle DNS records haben ein TTL value (time to live), welcher in Sekunden angibt wie lange die Kopie gespeichert wird bzw refreshed wird.

DNS Record Types

A Record: These records resolve to IPv4 addresses, for example 104.26.10.229

AAAA Record: These records resolve to IPv6 addresses, for example 2606:4700:20::681a:be5

CNAME Record: These records resolve to another domain name, for example, TryHackMe's online shop has the subdomain name store.tryhackme.com which returns a CNAME record shops.shopify.com. Another DNS request would then be made to shops.shopify.com to work out the IP address.

MX Record: These records resolve to the address of the servers that handle the email for the domain you are querying, for example an MX record response for tryhackme.com would look something like alt1.aspmx.l.google.com. These records also come with a priority flag. This tells the client in which order to try the servers, this is perfect for if the main server goes down and email needs to be sent to a backup server.

TXT Record: TXT records are free text fields where any text-based data can be stored. TXT records have multiple uses, but some common ones can be to list servers that have the authority to send an email on behalf of the domain (this can help in the battle against

spam and spoofed email). They can also be used to verify ownership of the domain name when signing up for third party services.

Eigene Recherche

DNS records are instructions that live in authoritative DNS servers and provide information about a domain including what IP address is associated with that domain and how to handle requests for that domain. These records consist of a series of text files written in what is known as DNS syntax. DNS syntax is just a string of characters used as commands that tell the DNS server what to do.