denic ANYCAST services

NXNS Angriff
Sicherheitslücke im DNS

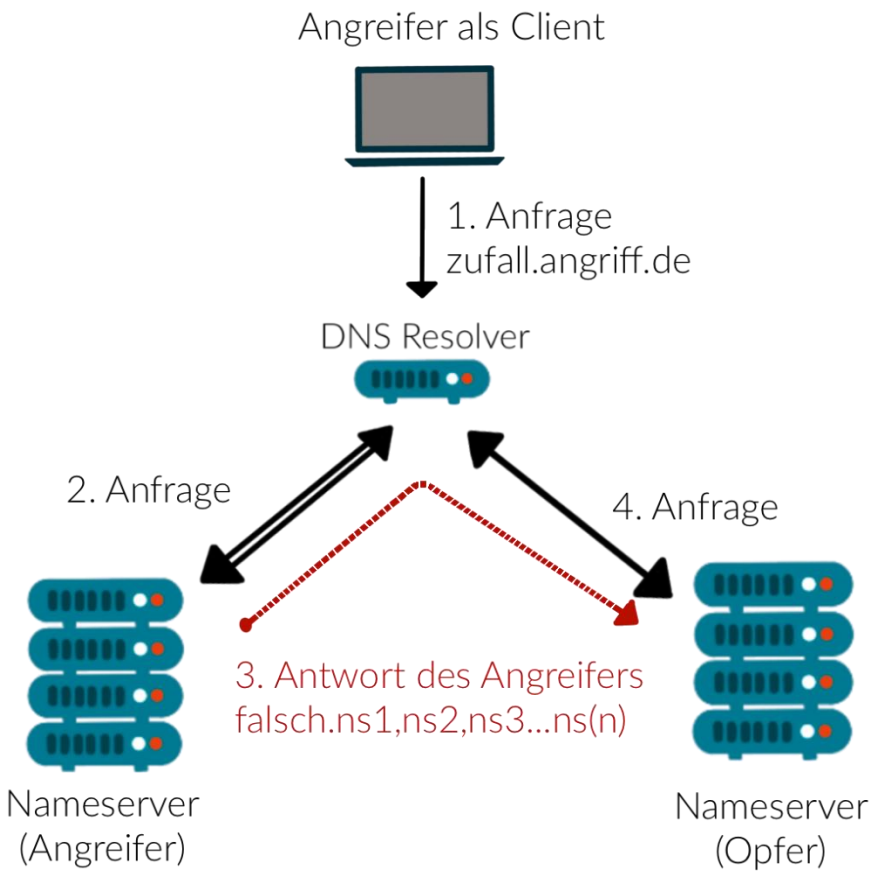
Um was geht es?

Ein NXNS Angriff kann verwendet werden, um einen massiven DDoS Angriff zu erstellen. Bereits bekannt ist der NX Domain Angriff (Mirai), der eine DNS-Abfrageflut durch Anforderungen zufälliger nicht vorhandener Subdomänen verursacht, die mit einer NX Domain Antwort beantwortet werden.

Mit einem Verstärkungsfaktor von 1620x ist der NXNS Angriff wesentlich größer als der NX Domain Angriff. Dies führt zu einem massiven Anstieg von Anfragen auf dem DNS-Server des Opfers und dabei auch zu einem Absturz.

Der Angriff erfolgt während der DNS-Delegierung und führt dazu, dass DNS-Resolver eine große Anzahl von Abfragen an den Nameserver des Opfers generieren.

Wie funktioniert es?



NXNS Angriff
Sicherheitslücke im DNS

Der Angreifer möchte den DNS-Server des Opfers abstürzen lassen.

Er besitzt die Domain **zufall.angriff.de** und sendet die Anfrage zum Auflösen seines eigenen Domainnamens an einen DNS-Resolver. Der Resolver kontaktiert dann den eigenen Nameserver des Angreifers.

Der Nameserver des Angreifers antwortet mit gefälschten Datensätzen wie **falsch.opfer.de**. Dies führt zu einem Datensatz, der keine IP-Adresse enthält. Daher muss der Resolver eine Verbindung zum Nameserver des Opfers herstellen, damit **opfer.de** nach den gefälschten Datensätzen in allen **Subdomänen** sowie auf **opfer.de** sucht. Da die Datensätze gefälscht sind, antwortet der Server mit einer Fehlermeldung.

Eine einfache Anfrage führt zu einem erheblichen Datenaustausch zwischen Resolver und dem Nameserver des Opfers. Wenn dies mehrmals pro Sekunde geschieht, ist die Datenmenge enorm und kann zu einem Absturz führen.

Wer ist betroffen?

Da diese Sicherheitslücke im DNS-Protokoll vorhanden ist, betrifft sie rekursive DNS-Resolver. Dies umfasst DNS-Resolver wie BIND, Unbound, Knot und PowerDNS. Kommerzielle DNS-Dienste sind ebenfalls betroffen.

DENIC Services Anycast DNS

Unsere DNS-Software wurde letzte Woche unverzüglich mit dem entsprechenden Patch aktualisiert. Der Patch soll verhindern, dass Angreifer die DNS-Delegierung missbrauchen, um einen massiven Datenverkehr zu erzeugen.

Für die Sicherheit und der Servicekontinuität unseres Anycast-DNS-Dienstes setzen wir eine hohe Priorität auf die Instandhaltung unserer Software, um diese so sicher wie möglich zu halten.