# Wie ODNS Surfgewohnheiten geheim hält

DNS ordnet menschenlesbare Namen für Computer und Dienste, wie etwa nakedsecurity.sophos.com, den numerischen IP-Adressen zu, die Computer benötigen, um miteinander zu kommunizieren. Leider hat DNS ein Datenschutzproblem: DNS-Abfragen können gelesen werden und man sieht genau, wer wo surft, selbst wenn diese Personen darauf achten, die genauen Details ihres Surfens mit HTTPS zu verschlüsseln. Es gibt bereits viele Ansätze um dieses Problem zu lösen. Ein junge und sehr vielversprechende Technologie ist ODNS (Oblivious DNS**)**. Sophos erklärt, wie sie funktioniert.

**So funktioniert DNS**

Um eine bestimmte Webseite, zum Beispiel *www.example.org*, über den Webbrowser aufzurufen, muss der Computer die IP-Adresse dieser Seite kennen. Diese Informationen erhält man über DNS. Dazu stellt der Computer die Frage "Wie lautet die IP-Adresse von *www.example.org*?" an einen rekursiven Resolver, der möglicherweise vom ISP oder einem Drittanbieter wie CloudFlare unter der IP-Adresse 1.1.1.1 oder Google unter der IP-Adresse 8.8.8.8 betrieben wird. Über mehrere Server gelangt die Anfrage letztlich an einen autoritativen Server, der die Adresse kennt. Der autoritative Server beantwortet die ursprüngliche Frage und sendet die IP-Adresse, im Falle von www.example.org 93.184.216.34 an den rekursiven Resolver, der sie an den Computer zurückschickt. Dieser gesamte Datenverkehr ist für jeden, der sich im selben Netzwerk wie der Computer aufhält ebenso wie für den ISP (oder den VPN-Provider) auf dem Weg durch das Netzwerk sichtbar. Er ist aber auch auf dem DNS-Resolver und dem autoritativen Server sowie oft auch auf den anderen Servern, die der rekursive Resolver konsultiert, sichtbar.

„Sämtliche Informationen, die so auf dem Weg durchs Netz abgefragt und beantwortet werden kann ein Dritter, der die Kommunikation zwischen einem Client und einem rekursiven Resolver oder sogar zwischen einem rekursiven Resolver und einem autoritativen Server abhört, in Ruhe mitlesen," erläutert Michael Veit, Technology Evangelist bei Sophos. „Da diese Informationen an jeden DNS-Server gesendet werden, können darüber hinaus auch DNS-Betreiber die Informationen der Clients einsehen."

**Verfahren zum Sichern von DNS**

Es gibt eine Vielzahl von Lösungsansätzen, die sich mit den Datenschutzproblemen von DNS befassen. Die meisten Lösungen erfassen dabei jedoch nur einen Teil des Problems und einige erfordern eine Art der Umrüstung, die den Prozess verlangsamen könnte. So reduziert beispielsweise eine DNS Query Name Minimierung die Menge an Informationen, die der rekursive Resolver mit einigen DNS-Servern teilt. Snooping, also Schnüffeln am oder zwischen Resolvern, ISP oder autoritativem Server ist jedoch weiterhin möglich.

DNS-over-TLS und DNS-over-HTTPS erfordern eine Umrüstung bestehender Systeme, um den DNS-Verkehr zu verschlüsseln und so Snooping zu verhindern. Sie lösen zwar aufwändig dieses Problem, verhindern aber nicht, dass der Verkehr am Resolver oder anderen Zielen trotzdem überwacht wird.

Rekursive Resolver, die extra für den Datenschutz entwickelt wurden, gehen das Resolver-Problem an, indem sie versprechen, den Nutzer nicht zu überwachen oder Protokolle über seine Aktivitäten zu führen. Das ist ein schöner Ansatz, aber Privatsphäre und Sicherheit erfordern ein stärkeres Fundament als die Zusicherung von "Sie können uns vertrauen".

**Oblivious DNS als sichere Variante ohne erforderliche Umrüstung**
Oblivious DNS versucht, Spionage am Resolver oder an anderen Zielen ohne nennenswerte Umrüstung zu bekämpfen. Der Computer stellt immer noch die Frage "Wie lautet die IP-Adresse von www.example.org?"? aber dieses Mal wird es an einen lokalen ODNS-Resolver auf dem Computer gesendet. Dieser lokale Resolver erstellt einen Sitzungsschlüssel, verschlüsselt die Domäne damit und fügt dann .odns am Ende hinzu, wodurch man einen völlig unkenntlichen Domänennamen wie 9fab9405429045fe5.odns erhält. Der Sitzungsschlüssel selbst wird dann mit einem öffentlichen Schlüssel verschlüsselt, der von einem autoritativen Server für die .odns-TLD (Top-Level-Domain) bereitgestellt wird. Jeder kann etwas mit dem öffentlichen Schlüssel verschlüsseln, aber nur der autoritative Server kann es lesen. Der verschlüsselte Sitzungsschlüssel wird der DNS-Abfrage hinzugefügt und an einen normalen rekursiven Resolver, wie ihn ein ISP betreibt, gesendet. Das Schnüffeln zwischen dem Computer und dem Resolver oder am Resolver selbst wird so vereitelt. Zwar kann ein Dritter erkennen, wer eine Anfrage stellt, aber nicht, wofür die Anfrage ist, da der Domainname verschlüsselt wird, bevor er den Computer verlässt

Derzeit ist dieses Verfahren noch ein Prototyp, aber das Forschungsteam arbeitet mit Hochdruck daran, Surfen zukünftig komplett sicher zu gestalten.

Den gesamten Beitrag zum Thema ODNS lesen Sie auf auf Sophos Naked Security unter:
https://nakedsecurity.sophos.com/2018/04/10/how-odns-keeps-your-browsing-habits-secret/

**Pressekontakt**

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de