Browser verschlüsseln DNS-Anfragen

Bislang läuft die Kommunikation von Browsern mit DNS-Servern meist unverschlüsselt. Weil dies als Unsicherheitsfaktor gilt, rüsten die Hersteller ihre Software nach: Firefox und Chrome beherrschen nun DNS over HTTPS (DoH).

Mozilla und Google setzen in ihren Browsern künftig auf DNS over HTTPS (DoH), um Namensauflösungen besser abzusichern. Mit DoH können Browser ihre DNS-Abfragen verschlüsseln, um beispielsweise die Privatsphäre der Nutzer besser zu schützen – insbesondere in offenen Netzen, etwa an Hotspots. Das ist auch sinnvoll, denn unverschlüsselte DNS-Abfragen sind durch Man-in-the-Middle-Attacken verwundbar – ein Angreifer kann den Traffic also manipulieren. DoH schützt vor DNS-Hijacking und Spoofing. Außerdem hilft DoH, DNS-gestützte Zensurmaßnahmen zu verhindern.

Mit Abfragen beim DNS erfahren Browser, welche IP-Adresse hinter einem Domain-Namen steckt. Nur mit der IP-Adresse erreichen sie den Webserver, von dem sie die Inhalte laden sollen. Standardmäßig fragen Browser beim DNS-Server nach, den das Betriebssystem vorgibt – meist bei dem des Internetproviders. Die Kommunikation erfolgt unverschlüsselt.

Firefox enthält seit Version 60 die Option, DoH als experimentelle Funktion zu aktivieren. Noch im September will Mozilla DoH nun zum Standard und nach und nach zur Voreinstellung machen – zunächst aber nur in den USA.

Allerdings erntet Mozilla Kritik an der Umsetzung: Derzeit stellt Firefox sämtliche DoH-Requests an den DNS-Dienst von Cloudflare. Mozilla arbeitet mit dem amerikanischen Cloud-Anbieter zusammen, um DoH in Firefox anbieten zu können. Cloudflare könne den Traffic zu Geschäftszwecken analysieren, was die Privatsphäre gefährde, so die Kritiker. OpenBSD etwa hat sich entschieden, aus diesem Grund im Firefox-Port der Distribution die automatische Verwendung von DoH zu deaktivieren.

Google hat derweil angekündigt, DoH ab Chrome 78 experimentell zu unterstützen, dessen stabile Variante am 22. Oktober erscheinen soll. Anders als Mozilla legt sich Google nicht auf einen DNS-Dienst fest: Für das Experiment arbeitet der Konzern mit einigen DNS-Providern zusammen, die DoH bereits unterstützen. Derzeit seien das Cleanbrowsing, Cloudflare, DNS.SB, OpenDNS, Quad9 sowie Google selbst.

Der vom Nutzer bislang verwendete DNS-Anbieter soll bleiben, Chrome versuche lediglich auf den gleichwerten DoH-Dienst des Providers umzustellen, teilte Google mit: „Mit diesem Ansatz ändert sich der verwendete DNS-Dienst nicht, sondern nur das Protokoll.“ Dadurch sollen bestehende DNS-Filter und Kinderschutzsysteme aktiv bleiben.

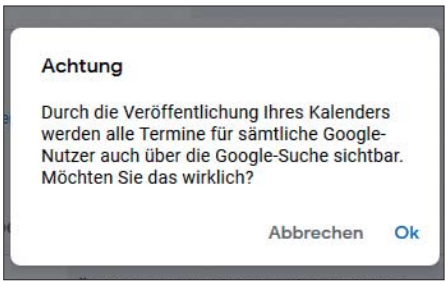
Chrome verwendet DoH wenn möglich, andernfalls arbeitet der Browser wie gehabt und sendet herkömmliche DNS-Anfragen. Der DoH-Test soll für „einen Bruchteil der Chrome-Anwender“ und auf allen unterstützten Plattformen laufen – dazu zählen iOS und Linux derzeit nicht.

(hob@ct.de)

Versehentlich veröffentlichte Google-Kalender

Im Web lassen sich tausende private **Google-Kalender** aufspüren und einsehen. Darauf wies der Sicherheitsforscher Avinash Jain hin, nachdem er die Probe aufs Exempel gemacht hatte. In einem Blog-Eintrag beschreibt Jain, mit welchen Suchparametern er die Kalender im Netz aufspürte. Auf diese Weise entdeckte er auch sensible Einträge, beispielsweise von einer Arztpraxis.

Google erklärte in einer Stellungnahme, dass öffentliche Kalender eben öffentlich seien. Es liege in der Verantwortung der Nutzer, ihre Daten zu schützen. Standardmäßig sind die Google-Kalender auf privat gestellt, betonte Google. Nur der jeweilige Besitzer hat also Zugriff darauf. Anwender können den Kalender aber auch für Familienmitglieder, Freunde oder Kollegen freigeben. Zudem ist es möglich, ihn öffentlich zu machen. In diesem Fall zeigt Google einen deutlichen Hinweis an: „Durch die Veröffentlichung Ihres Kalenders werden alle Termine für sämtliche Google-Nutzer auch über die Google-Suche sichtbar. Möchten Sie das wirklich?“ Der Vorfall zeigt: Nutzer sollten Warnhinweise lieber lesen statt blind abzunicken. *(hob@ct.de)*



Google warnt sehr deutlich vor der Freigabe eines Kalenders.

Ticketverkauf für die c’t <webdev> startet

Anfang Oktober startet der Ticketverkauf für die Frontend-Konferenz von c’t. Bis die Agenda feststeht – voraussichtlich Mitte Oktober –, gibt es ein vergünstigtes Wild-Card-Ticket für 499 Euro. Danach verkaufen wir 100 Tickets zum Frühbucherpreis von 589 Euro. Der reguläre Preis wird bei 699 Euro liegen. Bei der c’t <webdev> wird sich an den zwei Konferenztagen, dem 5. und 6. Februar, wieder alles um die Entwicklung von Frontends aller Art drehen (www.ctwebdev.de). *(jo@ct.de)*

Geteilte Verantwortung

Die Betreiber von gewerblichen **Fanpages auf Facebook** sind mitverantwortlich für die Datenverarbeitung, die im Hintergrund läuft. Bei schweren Mängeln dürfen Datenschutzbehörden daher die Betreiber verpflichten, die Unternehmensseite abzuschalten. Das hat das Bundesverwaltungsgericht in Leipzig entschieden. (Az.: 6 C 15.18) Auch wenn Facebook selbst ein Adressat für die Beschwerden sein könnte, dürften die Datenschützer aus Gründen der Effektivität auch die Seitenbetreiber in die Pflicht nehmen.

Der Entscheidung liegt ein Fall aus Schleswig-Holstein zugrunde. Das Unabhängige Landeszentrum für Datenschutz (ULD) forderte 2011 von der Wirtschaftsakademie Schleswig-Holstein die Deaktivierung ihrer Fanpage. Beim Aufruf der Seite würden Daten der Nutzer erhoben, ohne dass diese darüber informiert würden. Inwiefern diese Datenverarbeitung tatsächlich rechtswidrig war, müsse aber noch genauer geklärt werden, urteilten die Leipziger Richter. Sie verwiesen den Fall darum zur erneuten Verhandlung und Entscheidung an das Oberverwaltungsgericht in Schleswig-Holstein zurück.

In den Vorinstanzen war die Wirtschaftsakademie erfolgreich gewesen. Das Oberverwaltungsgericht hatte entschieden, sie sei nicht datenschutzrechtlich verantwortlich, weil sie keinen Zugriff auf die erhobenen Daten bei Facebook habe. Dagegen hatte sich das ULD in dem Revisionsverfahren gewandt.

(hob@ct.de)