Bundeskartellamt

Fallbericht 3. Februar 2022

Vorläufig kein Verfahren im Bereich der Verschlüsselung von DNS-Diensten

Branche:	Digitalwirtschaft
Aktenzeichen:	B7-2020/115

Das Bundeskartellamt hat nach einer mehrmonatigen Vorprüfungsphase entschieden, derzeit kein Verfahren im Bereich von DNS-Diensten einzuleiten. Es wird den Markt weiter beobachten und ggfs. zu einem späteren Zeitpunkt und bei validen Hinweisen von Marktteilnehmern zu Kartellrechtsverstößen ein Verfahren in diesem Bereich führen.

DNS-Dienste (DNS = Domain Name System) dienen der Namensauflösung von Adressen im Internet. Um eine Webseite zu erreichen, geben die Nutzer im Normalfall nur den Namen einer Webseite ein. Um die Seite aufzurufen, muss der Webseiten-Name in eine IP-Adresse übersetzt werden. Diese Aufgabe übernimmt im Hintergrund der sogenannte DNS Resolver oder Client. Dabei handelt es sich um eine spezielle Komponente des Betriebssystems, die bereits aufgerufene IP-Adressen im Cache (Zwischenspeicher) speichert und bei Bedarf ausliefert. Findet sich eine angeforderte IP-Adresse nicht im Cache des DNS Resolvers, wird die DNS-Anfrage an einen externen DNS Resolver wie den des Internetzugangsdienstleisters weitergeleitet. Der Betrieb von DNS Resolvern zur Namensauflösung ist in Deutschland Teil der Internetzugangsleistung.

Die Mehrheit der deutschen Internetnutzer greift auf diese betriebssystemseitig voreingestellten, vom Anbieter des Internetzugangs angebotenen DNS-Dienste zurück. Allerdings besteht die Möglichkeit, dass bestimmte Endgeräte, bestimmte Anwendungen oder auch der Nutzer selbst bzw. dessen Netzwerkadministrator die Voreinstellung bezüglich des DNS Resolvers verändert. Statt auf den DNS Resolver des Internetzugangsdienstleisters greift das Betriebssystem bzw. die jeweilige Anwendung dann auf einen eigenen oder auf einen allgemein verfügbaren Public DNS Resolver zurück.

Der Markt für Public DNS Resolver ist stark konzentriert. Aufgrund öffentlich verfügbarer Quellen geht das Bundeskartellamt davon aus, dass Google Public DNS sowohl in Deutschland als auch weltweit derzeit der mit Abstand am häufigsten verwendete Public DNS Resolver ist, gefolgt von Cloudflare DNS. Die Verwendung von Public DNS Diensten hat in den letzten Jahren stark zugenommen. Ein Grund dafür könnte die

Einführung von Verschlüsselungstechniken für DNS-Abfragen sein. Internetzugangsanbieter bieten derzeit erst sehr vereinzelt die Verschlüsselung von DNS-Abfragen an, während viele Public DNS Resolver Abfragen verschlüsselt durchführen.

In den USA leitet Mozilla DNS-Abfragen, die bei der Verwendung von Firefox gestellt werden, automatisch auf von Mozilla als vertrauenswürdig eingestufte DNS-Resolver um, die eine verschlüsselte Namensauflösung durchführen. Mozilla bezeichnet diese DNS-Resolver als „Trusted Recursive Resolver“. Der größte von Mozilla eingesetzte DNS Resolver ist Cloudflare.

Das Bundeskartellamt hat aufgrund von Hinweisen aus dem Markt Vorermittlungen dazu geführt, ob es im Zuge der Einführung der Verschlüsselung von DNS-Diensten zu möglichen Kartellrechtsverstößen gekommen ist. Dabei ging es unter anderem um konkurrierende Arten von Verschlüsselung (DNS over HTTPS oder DNS over TLS), um die mögliche Veränderung von Voreinstellungen in Betriebssystemen und in Browsern sowie um die Erfassung von mit der DNS-Namensauflösung verbundenen Dienstleistungen im Bereich Safe Browsing sowie möglicher Kinderschutzfilter. Das Bundeskartellamt hat dazu Gespräche mit verschiedenen Marktteilnehmern geführt, darunter u.a. Internetzugangsanbietern und Anbietern von Public DNS Resolvern. Der Verdacht hat sich bislang nicht bestätigt. Insbesondere in Bezug auf Google hat die Beschlussabteilung derzeit keine Hinweise, dass das Unternehmen die Einführung von Verschlüsselung dazu nutzt, DNS-Dienste und damit verbundene Dienstleistungen z. B. im Sicherheitsbereich an sich zu ziehen. Google trägt nach dem Eindruck der Beschlussabteilung zwar aktiv zur Verbreitung der Verschlüsselung von DNS-Diensten bei. Dies ist aber derzeit nicht mit einer Selbstbevorzugung des konzerneigenen DNS Resolvers Google Public DNS verbunden. Im Rahmen des von Google verwendeten Same-Provider-Upgrade-Konzepts findet eine Umleitung auf einen verschlüsselten DNS-Dienst nur dann statt, wenn dieser Dienst vom voreingestellten Anbieter angeboten wird.

Das Bundeskartellamt hat sich bereits im Rahmen möglicher DNS-Sperren zur Bekämpfung von Verletzungen des Urheber- und Leistungsschutzrechts mit DNS-Diensten beschäftigt (s. Pressemitteilung vom 11. März 2021). Im Dezember 2021 hat das Bundeskartellamt festgestellt, dass Google über eine überragende marktübergreifende Bedeutung für den Wettbewerb verfügt (s. Pressemitteilung vom 5. Januar 2022).