

LU16c - Sichere DNS Abfragen



Selbst wenn meine Daten mit HTTPS gesichert sind, werden DNS-Anfragen noch oft im Klartext und ungesichert übertragen.

Ungesicherte DNS-Abfragen bieten zwei Sicherheitslücken:

- Ein Angreifer kann mir gefälschte DNS-Einträge liefern und mich somit auf seinen Server umleiten.
- Jeder Server über den meine Anfrage läuft, kann die Daten mitlesen und aufzeichnen.

Weiteres Material

- https://www.unibesecure.unibe.ch/tipps_tricks/dot_doh_und_dnssec/index_ger.html
- https://www.chip.de/news/Sicherer-surfen-So-verschluesseln-Sie-Ihren-Browser_184307520.html

Domain Name System Security Extension (DNSSEC)

Siehe auch  [Domain_Name_System_Security_Extensions](#)

DNSSEC stellt die Authentizität und die Integrität des Domain Name Systems sicher. Ähnlich wie bei HTTPS wird mittels Signatur geprüft, ob die DNS-Daten echt sind. Die Daten werden jedoch nicht verschlüsselt übertragen.

Verschlüsselte DNS-Anfragen

Die Auswertung meiner DNS-Anfragen lässt Schlüsse über mein Surfverhalten und damit über meine Gewohnheiten zu. Ausserdem nutzen viele Web Content Filter die DNS-Anfragen, um unerwünschte Webseiten zu blockieren. Um dies zu verhindern, gibt es verschiedene Ansätze, die DNS-Anfragen verschlüsselt zu übertragen.

-  [DNS_over_TLS](#) DoT
-  [DNS_over_HTTPS](#) DoH

m231-AnG



Marcel Suter

From:

<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:

<https://wiki.bzz.ch/modul/m231/learningunits/lu16/securedns>

Last update: **2024/03/28 14:07**

