# DNS-Spoofing: Cache Poisoning einfach erklärt

*Datum: 14.05.2019 | Internet, Sicherheit*




Sie erhalten eine E-Mail Ihrer Hausbank, in der Sie gebeten werden, die Login-Daten für Ihren Online-Banking-Account zu bestätigen. Einige Tage später stellen Sie fest, dass Unbekannte von Ihrem Konto mehrere tausend Euro gestohlen haben. Szenarien wie dieses sind das Ergebnis des sogenannten **DNS-Spoofings**, **bei dem Hacker Ihre Anfragen an das Internet heimlich auf gefälschte Webseiten umleiten, um so an Ihre sensiblen Daten zu gelangen**. In diesem Beitrag erfahren Sie, wie DNS-Spoofing funktioniert und was Sie tun können, um sich vor derartigen Angriffen zu schützen.

- ✔ DNS-Spoofing war besonders in den Anfangszeiten des Internets ein beliebte Form der Attacke.
- ✔ Die Spoofing-Attacke erfolgt häufig unter dem Deckmantel von scheinbar seriösen Webseiten.
- ✔ Durch ein umsichtiges Verhalten kann der PC-Nutzer selbst am meisten zur Vermeidung von DNS-Spoofing-Attacken beitragen.

**Inhalt** [Ausblenden]



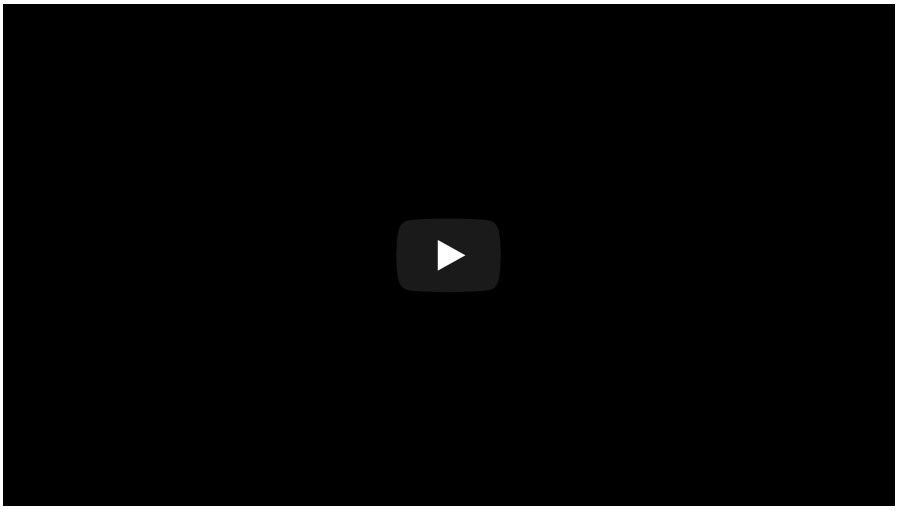
## 1. Was versteht man unter DNS-Spoofing?

DNS-Spoofing steht für eine ganze Palette von Angriffen, bei denen **auf dem DNS-Server gespeicherte Informationen ersetzt** werden, mit dem Ziel, den **Nutzer auf eine gefälschte Website umzuleiten**. So können beispielsweise **sensible Daten abgefangen oder Malware auf dem System eingeschleust** werden.

Man unterscheidet grundsätzlich zwischen **zwei Arten von Angriffen**:

- Beim **DNS-Cache-Poisoning** werden gefälschte Informationen in den DNS-Cache des Nutzers eingeschleust.
- Von **DNS-Spoofing** spricht man hingegen, wenn mittels IP-Spoofing gefälschte Informationen versendet werden.

**Gut zu wissen:** Eine verwandte Form der DNS-Angriffe ist das sogenannte DNS-Hijacking. bei dem die Hacker das DNS-System so manipulieren, dass es absichtlich falsche Antworten gibt.



## 2. Wie funktioniert DNS-Spoofing?


Der Nameserver wandelt die Namens-Adressen im Internet in die dazugehörige IP um.

**Beim DNS-Spoofing greifen die Hacker im ersten Schritt den sogenannten Nameserver an, auf dem das DNS-System aufbaut**. Dabei handelt es sich um einen Service, dem die IP-Adresse der Domain bekannt ist und der in der Lage ist, diese in beide Richtungen zu übersetzen. Der **Nameserver** funktioniert dabei wie eine Art Telefonbuch: Er **wandelt die im Internet gebräuchlichen Namensadressen (z.B. www.google.de) in die entsprechenden IP-Adressen um**.

Damit Sie eine Domain aufrufen können, muss dieser also immer erst ein Nameserver zugeordnet werden. Der Hacker verschafft sich Zugriff auf dessen Konfiguration und sorgt dafür, dass **beim Aufruf einer Internetseite falsche Informationen mitgeliefert** werden. Diese "falschen" **Daten des Nameservers sind auf dem Rechner des Nutzers gespeichert**, dadurch „erinnert“ sich dieser später daran und greift darauf zurück. Ziel der Hacker ist es, entweder direkt **Zugriff auf Ihre sensiblen Daten zu erhalten** oder zu genau diesem Zweck **gefälschte Inhalte bereitzustellen**.


Eine aktuelle Spoofing-E-Mail unter dem Deckmantel des Online-Versandhaus Amazon. Beim Klick auf den Button landen Sie auf einer gefälschten Webseite mit Schadcode, die Ihre Login-Daten abgreift.

Öffnen Sie nun beispielsweise Ihr Online-Banking, landen Sie durch das DNS-Spoofing auf einer Seite, **die dem Original Ihrer Hausbank**

**täuschend ähnlich sieht.** Sie dient aber lediglich dazu, Ihre **Login-Informationen abzufangen und / oder Schadsoftware auf Ihren Rechner zu laden,** mit sich der Hacker im Anschluss Zugang zu Ihren Konten verschafft. Die Seiten sind in den meisten Fällen **so gut gefälscht, dass nur IT-Experten in der Lage sind, den Unterschied zu erkennen**.

### 2.1. Emails als Überbringer "schlechter" Nachrichten

Der Code für die Spoofing-Software versteckt sich häufig aber auch **als Anhang in SPAM-Emails**. Diese stammen **auf den ersten Blick von einer serösen Quelle**. Öffnet der Empfänger die angehängte Datei, wird auf dem Computer Schadcode installiert, der **die Informationen des Cache verändert** und so während der alltäglichen Nutzung im Hintergrund sensible Daten abfängt. Selbst hinter Werbebildern oder -bannern kann sich Malware dieser Art verstecken, oft reicht ein Klick darauf schon aus, um den Rechner zu infizieren.

## 3. Welche Gefahren entstehen durch das DNS-Cache-Poisoning?


Selbst die Seiten von IT-Security-Anbietern sind gegen DNS-Spoofing nicht gefeit.

Das **DNS-Posining birgt eine ganze Reihe von Gefahren**, angefangen vom Diebstahl sensibler Daten bis hin zu schweren Infektionen durch Viren oder Trojaner.

Durch das Fälschen bekannter Webseiten, wie beispielsweise von Banken oder großer Online-Händler, **gelangen Hacker an Kreditkartendaten, Passwörter oder persönliche Informationen**. Sind diese erst einmal in den Händen der Internet-Kriminellen, entsteht dadurch in den meisten Fällen nicht nur ein **großer finanzieller Schaden**, sondern der Diebstahl hat häufig auch **einen massiven Eingriff in die Privatsphäre der Opfer** zur Folge.

Wenn die **Webseiten von IT-Security-Anbietern, wie z.B. Hersteller von Virenscannern oder Anti-Malware-Programmen**, von dem Angriff betroffen sind, wird der Computer damit einer **zusätzlichen Bedrohung durch Schadsoftware** ausgesetzt, da keine angemessenen Sicherheitsmaßnahmen mehr durchgeführt werden können (z.B. wird die Installation von Sicherheitsupdates blockiert).

## 4. Wie kann ich mich vor DNS-Spoofing schützen?

**Das DNS-Spoofing ist eine der ältesten Formen von Attacken im Internet**, das Dank verbesserter Sicherheitsmaßnahmen und einer umfangreichen Sensibilisierung der Nutzer **heutzutage keine allzu große Gefahr mehr** darstellt.

In den letzten Jahren wurden bereits **zahlreiche Ansätze für eine Verbesserung der Sicherheit umgesetzt**. Dazu zählt in erster Linie die **Verschlüsselung von sensiblen Daten und Inhalten.** Eine andere Abwehrmaßnahme setzt dagegen direkt beim DNS-Server an: Moderne **Nameserver senden bei einer Abfrage mehrere zufällige Informationen mit**, die dem Angreifer nicht bekannt sind. Damit der Browser des Benutzers die gefälschten Daten als zulässig anerkennt, müsste er diese erst erraten. Das stellt allerdings **in den meisten Fällen ein Ding der Unmöglichkeit** dar.


Das https in der URL zeigt an, dass es sich eine sichere Webseite handelt.

Überdies schützen inzwischen auch viele Browser die Anwender davor, **während Ihrer Anfragen ungewollte Informationen zu erhalten**. Zudem kennzeichnen **Webseiten-Zertifikate** wie HTTPS sichere Seiten. Beim Aufrufe einer (vermeintlich) unsicheren Seite **informiert Sie eine Browser-Meldung darüber**.

**Den größten Beitrag zur Sicherheit leistet allerdings immer der Nutzer selbst.** Durch ein umsichtiges Verhalten lassen sich sämtliche Formen von DNS-Spoofing nahezu vollständig vermeiden. **Klicken Sie daher niemals auf unbekannte Links oder öffnen Sie Webseiten, die als unsicher eingestuft wurden**. Führen Sie regelmäßige Sicherheitsscans auf Ihrem System durch und nutzen Sie dafür möglichst **ein lokal installiertes und kein gehostetes Programm.** Sonst besteht nämlich wieder die Gefahr, dass die Ergebnisse durch das Spoofing gefälscht werden könnten.

## 5. Und was, wenn es mich doch erwischt hat?

Sollte es trotz aller Schutzmaßnahmen dennoch zu einem DNS-Spoofing-Angriff gekommen sein, ist die Beseitigung der „Vergiftung“ leider

ein recht schwieriges Unterfangen. **Die Bereinigung des betroffenen Servers beseitigt nämlich nicht automatisch das Problem auf dem Client-Computer.** Im umgekehrten Fall infiziert sich dieser beim Verbindungsaufbau zum Server erneut. Die Client-Nutzer können das Problem durch **Leeren des Cache-Speichers** aber zumindest lokal auf Ihrem Rechner lösen.


Leeren Sie Ihren System-Cache über die Datenträgerbereinigung, um die lokalen DNS-Spoofing-Dateien zu entfernen.

**52 Bewertungen**

Ø 4,62

## Ähnliche Artikel:

- Mail-Spoofing: Betrügerische Mails erkennen und abwehren
- IP-Spoofing: Wenn Angreifer ihre IP verschleiern
- Avast Test 2019: Wie schlägt sich die Internet...
- Inkognito surfen – Wie anonym sind Sie tatsächlich?
- Gefahr durch Cryptojacking: So können Sie sich vor...
- PGP-Verschlüsselung: Funktionsweise und Sicherheit