Internet-Sicherheit - DNS - Welche DNS-Server bieten welchen Schutz?

Kurzbeschreibung: Sicherheit in der IT, speziell auch bei der Verbindung ins Internet, ist ein vielschichtiges Thema. Es gibt keine Einzellösung mit maximalem Schutz, sondern nur sich ergänzende Module wie z. B. E-Mail-Sicherheit, Virenscanner, Firewall, Patchmanagement und vieles mehr. Ein kleiner, aber wichtiger und effektiver Baustein ist die Absicherung des DNS (Domain Name System) – konkret die Wahl eines sicheren DNS-Servers.

Für wen relevant?

- Alle, die ihre Internetverbindung durch die Wahl eines sicherheitsfokussierten DNS-Servers zusätzlich absichern möchten.

Kurze Erklärung – Warum ist der DNS-Server wichtig?

- Auf das Wichtigste heruntergebrochen stellt die Auswahl eines sicheren DNS-Servers das Herz der DNS-Absicherung dar.
- Von den DNS-Servern der Provider ist hier nicht generell abzuraten, jedoch stellen speziell auf Absicherung von Internetanfragen ausgelegte DNS-Server oftmals die zielführendere Wahl dar.

Hinweis Folgende DNS-Server werden hier genannt, ohne Anspruch auf Vollständigkeit und dauerhafte Aktualität.

Übersicht sicherheitsfokussierter DNS-Server

Anbieter	IP-Adresse 1	IP-Adresse 2	Sicherheit
OpenDNS (Cisco)	208.67.222.222	208.67.220.220	Ohne spezielles Konto bieten diese DNS-Server das Blocken von bekannten Phishing-Seiten.

Anbieter	IP-Adresse 1	IP-Adresse 2	Sicherheit
VeriSign	64.6.64.6	64.6.65.6	Der Anbieter kommuniziert eine „allgemein höhere Sicherheit" durch Einsatz seiner DNS-Server, mit Fokus auf Stabilität und Privatsphäre.
Quad9	9.9.9.9	149.112.112.112	Hinter diesem Anbieter (organisiert als gemeinnützige Schweizer Stiftung) stehen verschiedene Hersteller und Organisationen, u. a. IBM, PCH, GCA, welche sich für mehr IT-Sicherheit einsetzen. Durch den Einsatz unterschiedlicher Blacklisten wird der Zugriff auf das Internet gegen Schadsoftware, Phishing und Missbrauch besser abgesichert.
Cloudflare (Sicherheitsvariante)	1.1.1.2	1.0.0.2	Blockiert bekannte Schadsoftware- und Phishing-Domains.
AdGuard DNS (Standard/Familie)	94.140.14.14	94.140.15.15	Blockiert Schadsoftware, Phishing und Tracking; eine Variante mit zusätzlicher Werbeblockierung ist ebenfalls verfügbar.
NextDNS	individuell je Konto	individuell je Konto	Konfigurierbarer Cloud-DNS-Dienst mit Schadsoftware-/Phishing-Blocking, Blocklisten und detaillierten Auswertungen; erfordert ein kostenloses Konto zur individuellen Konfiguration.

Achtung Die reine Standardadresse von Cloudflare (`1.1.1.1` / `1.0.0.1`) bietet **keinen** Schutz vor Schadsoftware – sie ist auf schnelle, private DNS-Auflösung ausgelegt, ohne Filterung. Erst die Sicherheitsvariante `1.1.1.2` / `1.0.0.2` blockiert bekannte Schadsoftware- und Phishing-Domains (eine zusätzliche Variante `1.1.1.3` / `1.0.0.3` blockiert zusätzlich Erwachseneninhalte).

Tipp Viele der genannten Anbieter unterstützen inzwischen verschlüsselte DNS-Abfragen über DNS-over-HTTPS (DoH) oder DNS-over-TLS (DoT). Das verhindert, dass DNS-Anfragen auf dem Übertragungsweg unverschlüsselt mitgelesen werden können – ein sinnvoller zusätzlicher Baustein, sofern Router bzw. Endgeräte dies unterstützen.

Unsere eigene Lösung: Securepoint Cloud Shield (by CSG)

Als zertifizierter Securepoint-Partner bieten wir Ihnen **Securepoint Cloud Shield** an – eine DNS-gestützte Sicherheitslösung, die Ihr gesamtes Netzwerk sowie internetfähige Geräte (auch Smart-TVs oder Netzwerkdrucker) auf DNS-Ebene absichert.

- **Funktionsweise:** Der gesamte DNS-Datenverkehr wird über sichere Securepoint-Server geleitet, wo gefährliche Verbindungen gestoppt werden, bevor sie zustande kommen. Jede Adresse wird vor dem Besuch mit einer stetig aktualisierten Sicherheitsdatenbank abgeglichen; bei einer sicheren Adresse baut Cloud Shield eine verschlüsselte Verbindung auf.
- **Kompatibilität:** Passt zu jeder Infrastruktur – kompatibel mit jedem Router, jeder Firewall und jedem VPN-Protokoll.
- **Wartungsaufwand:** 100 % Cloud-Service, komplett wartungsfrei, keine zusätzliche Hardware nötig.
- **Weitere Funktionen:** individuelle Content-Filter (z. B. für Jugendschutz), Geo-IP-Blocking (Sperrung von Verbindungen in bestimmte Länder), sowie Verwaltung und Auswertungen über ein Online-Portal.
- **Herkunft:** Securepoint ist ein deutscher Hersteller (Lüneburg) mit deutschem Rechenzentrum.

Unser Vertrieb berät Sie gern und informiert auch darüber, wie sich Cloud Shield in unser Gesamtangebot einfügt.

Weiterführende Informationen direkt bei Securepoint: Cloud Shield – Secure DNS

Kurze Checkliste

- Aktuell genutzten DNS-Server geprüft (Provider-Standard oder bereits ein sicherheitsfokussierter Anbieter)?
- Bei Cloudflare: sichergestellt, dass die Sicherheitsvariante (1.1.1.2/1.0.0.2) statt der Standardadresse genutzt wird, falls Schadsoftware-Blocking gewünscht ist?
- Verschlüsselte DNS-Abfragen (DoH/DoT) in Betracht gezogen, sofern Router/Endgeräte dies unterstützen?
- Individuelle Beratung zu Securepoint Cloud Shield gewünscht?

FAQ – kurz & knapp

- Reicht die Wahl eines sicheren DNS-Servers allein als Schutz aus?
  - Nein, DNS-Sicherheit ist nur ein Baustein von vielen (neben z. B. E-Mail-Sicherheit, Virenscanner, Firewall, Patchmanagement) und ersetzt keine der anderen Schutzmaßnahmen.
- Blockiert Cloudflares Standard-DNS (1.1.1.1) automatisch Schadsoftware?
  - Nein. Dafür ist die separate Sicherheitsvariante 1.1.1.2 / 1.0.0.2 nötig.
- Was ist der Unterschied zwischen den genannten kostenlosen Anbietern und Securepoint Cloud Shield?
  - Die kostenlosen Anbieter bieten meist eine feste, nicht individuell anpassbare Filterung. Securepoint Cloud Shield ist dagegen individuell konfigurierbar (Content-

Filter, Geo-IP-Blocking), wird über ein Online-Portal verwaltet und läuft auf deutscher Infrastruktur.

Fußzeile
Bei der Erstellung von BranchXStack-Inhalten kann auch KI zum Einsatz kommen. Alle Inhalte werden jedoch redaktionell von Menschen geprüft und bei Bedarf überarbeitet.

Short□□: https://csg.gmbh/faq-dns-sicherheit

Created 2026-07-31 05:45:37 UTC by CSGJRAdmin
Updated 2026-07-31 05:51:29 UTC by CSGJRAdmin