

Unbound + Pi-Hole + Docker + Synology - die beste Methode!

YouTube Video: [sglbR68oW4c](#)

Video-Details

- **Kanal:** Navigio - Jürgen Barth
- **Dauer:** 25:26
- **Upload:** 05.03.2021
- **Kategorie:** Science & Technology
- **Tags:** pi-hole, pihole

AI Model: openai-gpt-4o-mini

Zusammenfassung

HAUPTTHEMA

In diesem Video wird erklärt, wie man einen lokalen DNS-Server namens Unbound installiert und betreibt, um Privatsphäre zu schützen und Werbung zu blockieren.

KERNPUNKTE

• **DNS-Anfragen:** Das Video erläutert den Ablauf von DNS-Anfragen, wonach lokale Computer ihren Router und schließlich den Provider-DNS-Server befragen, um IP-Adressen zu erhalten. • **Probleme mit Provider-DNS:** Provider-DNS-Server können möglicherweise Informationen sammeln, manipulieren oder verkaufen, so dass die Nutzung eines eigenen Servers sinnvoll ist. • **Unbound und Privacy:** Mit Unbound wird die DNS-Anfrage innerhalb des lokalen Netzwerks verarbeitet, wodurch die Kontrolle über Daten und Surfverhalten zurückgewonnen wird. • **Caching:** Unbound nutzt ein internes Cache für häufige Anfragen, was die Antwortzeiten bei wiederholten Anfragen erheblich verbessert. • **Installation und Konfiguration:** Das Video führt Schritt für Schritt durch die Installation von Unbound in einem Docker-Container und die nötigen Konfigurationen. • **Fehlerbehebung:** Hinweise werden gegeben, wie man typische Probleme bei der Installation und Konfiguration behandelt.

FAZIT/POSITION

Das Video fördert die Nutzung eines eigenen DNS-Servers, um die Privatsphäre der Nutzer zu wahren und ungefilterte Informationen zu erhalten. Der Ersteller betont, dass die Kontrolle über das eigene Netzwerk und die Anfragen wichtig ist, um unerwünschte Werbung zu vermeiden.