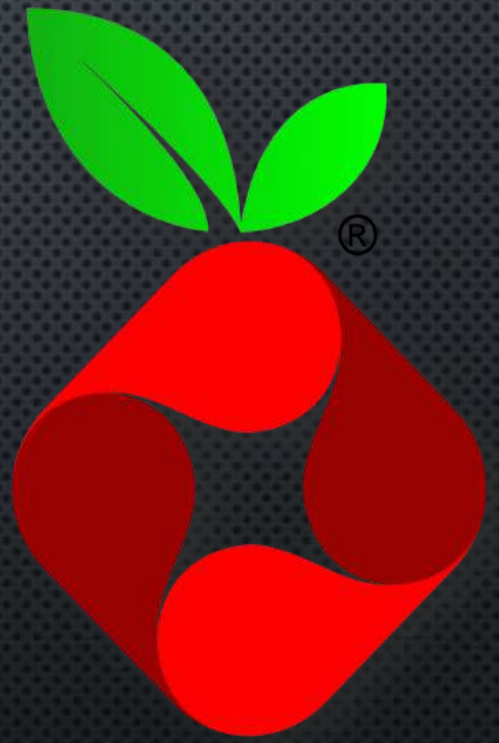
Vortragsreihe Digitale Selbstverteidigung mit freier Software
Thema heute:

PI-HOLE

DAS „SCHWARZE LOCH“ FÜR INTERNET WERBUNG ETC.



FRANK EWERT

EDU SECU IT

Ihr Referent

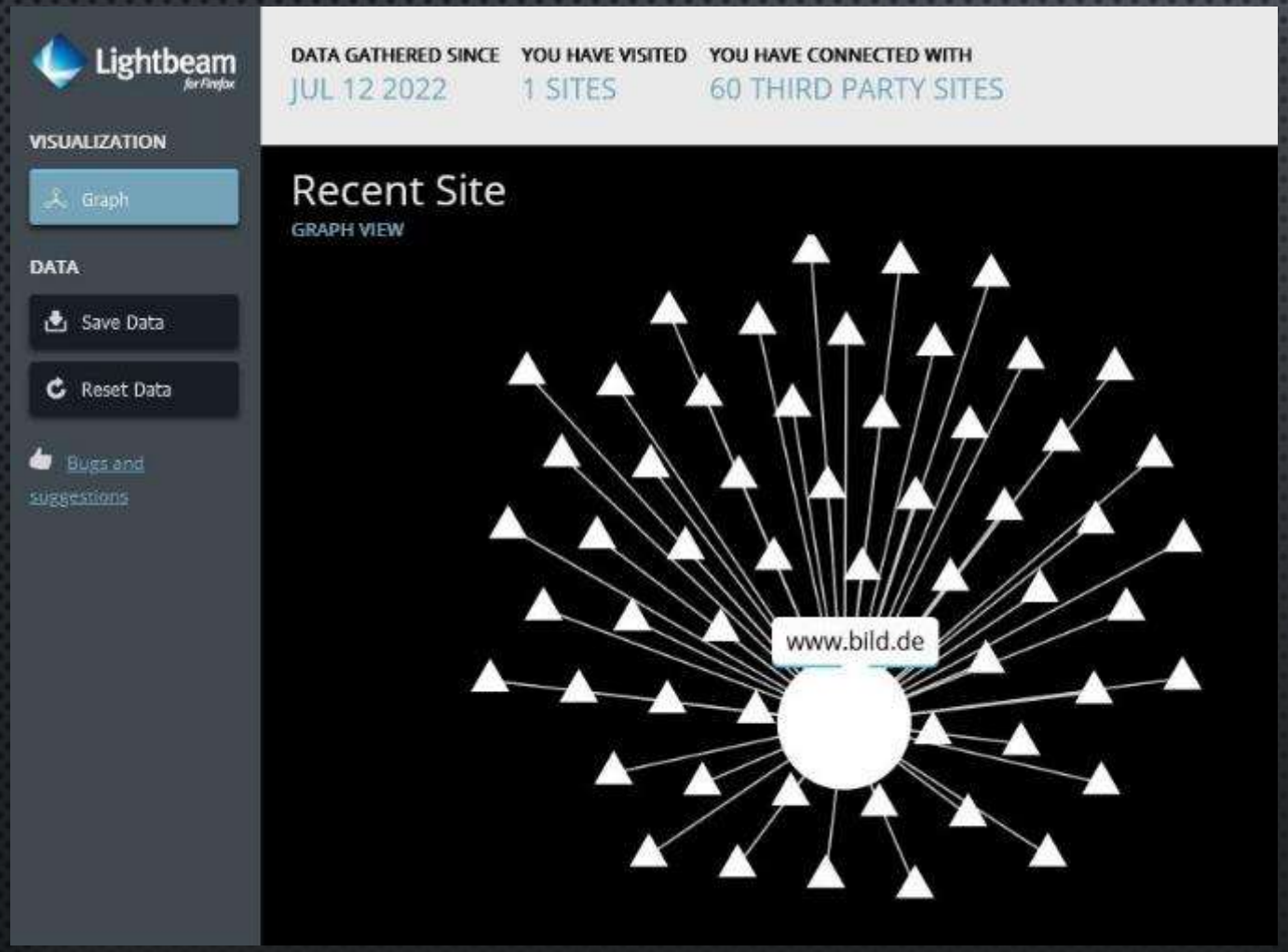
Frank Ewert

EDU SECU IT
stell. Vorstand „Sicheres Netz hilft e.V.“ *

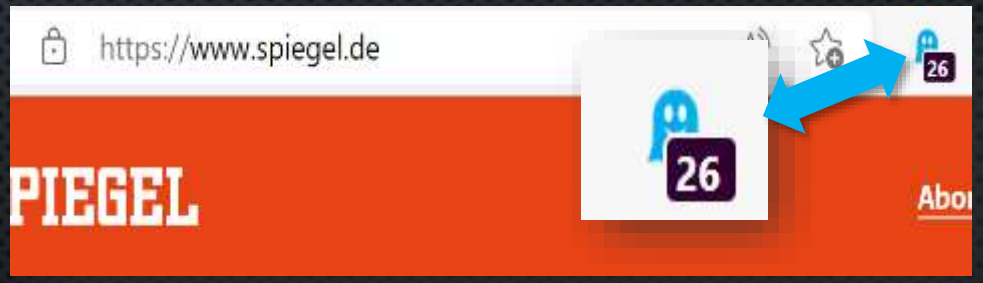
EDU - DV-Schulungen
SECU - „Live-Hacking“-Vorträge
IT - früher PC, heute µC-Entwicklungen

**** Leider Auflösung zum 31.07.22 (quasi „Corona-Opfer“…)***

Werbung und Tracking (1)

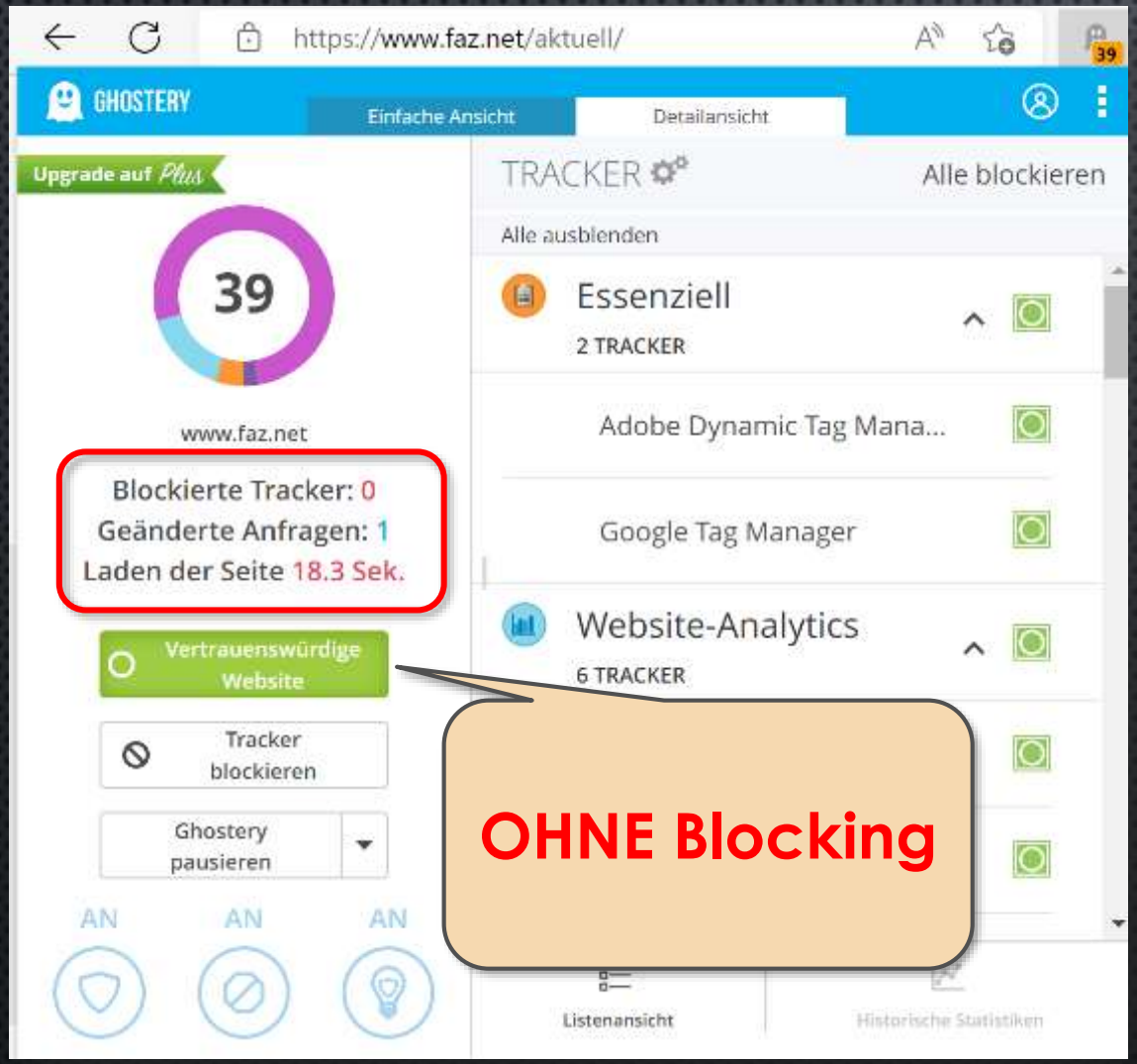


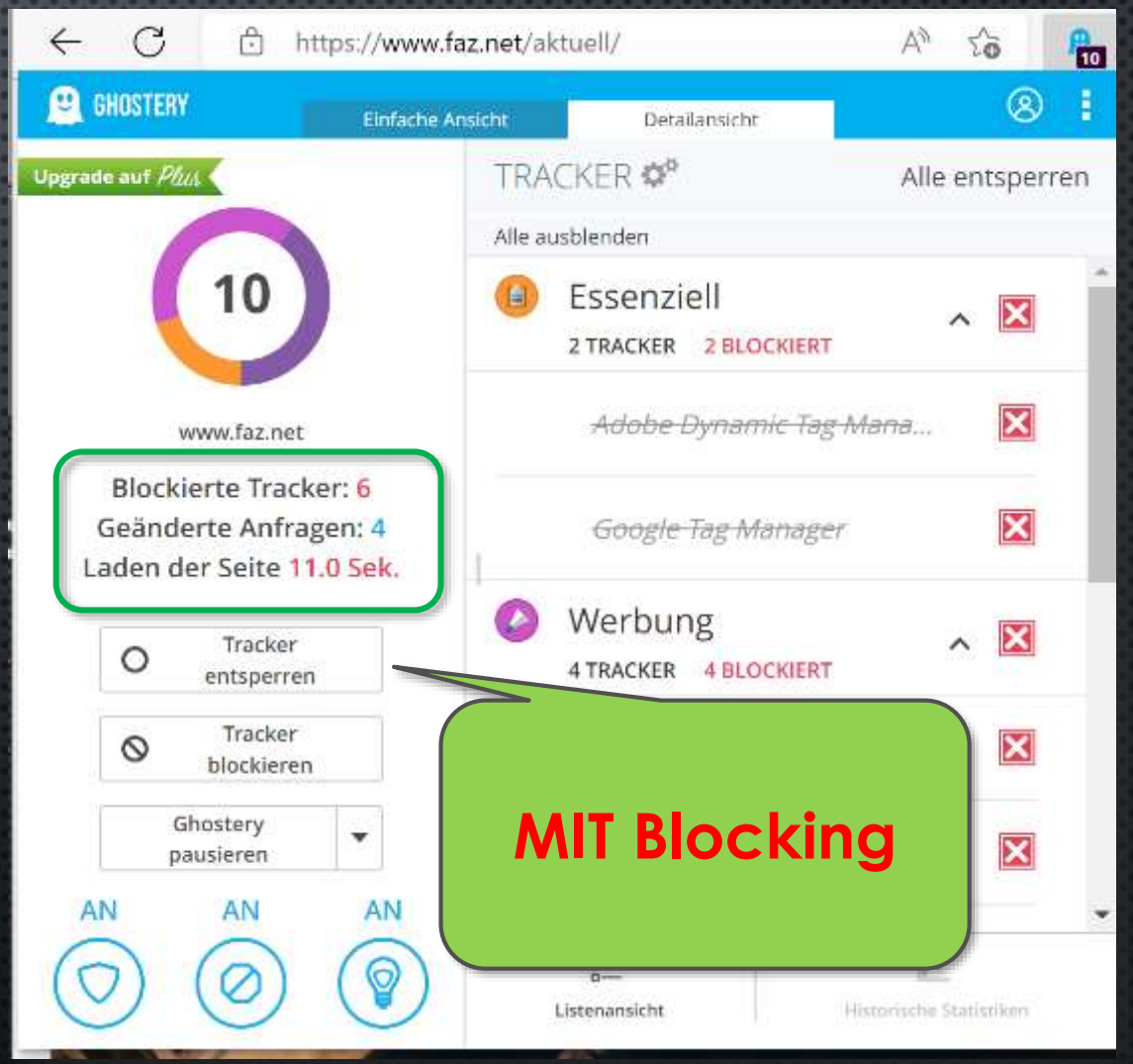
Lightbeam for Firefox (12.07.22 bei www.bild.de)



Ghostery for Firefox (Abruf 11.07.22)

Werbung und Tracking (2)





Ghostery for Firefox (www.faz.de am 12.07.22)

Werbung und Tracking (3)

Generell gibt es viele Programme bzw. Browser-erweiterungen, die sehr erfolgreich gegen sogenannte Webanalysen (Webtracking, Verlaufsanalysen, Clickanalysen etc.) vorgehen.

Ein Nachteil dieser System ist es, das sie auf jedem Endgerät/Browser installiert werden müssen…

***Pi-Hole* setzt hier als zentrale Lösung an, die alle im Netzwerk befindlichen Systeme (unabhängig deren Betriebssysteme, genutzten Browser etc.) schützt.**

ABER: Pi-Hole ist KEIN Contentfilter und Seiten, die KEINE DNS-Anfragen stellen, werden nicht geblockt!

Ghostery
(diverse Browser)

uBlock
(diverse Browser)

PrivacyBadger
(diverse Browser)

Werbestopper
(IOS/Android)

AdBlock Plus
(diverse Browser)

Brave
(diverse Betriebssysteme)

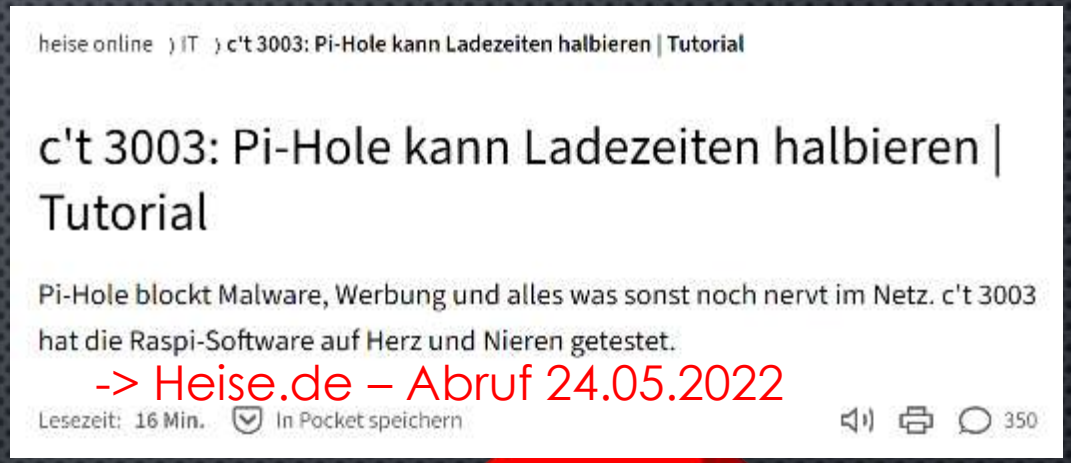
Das ist nur ein kleiner Überblick!!!

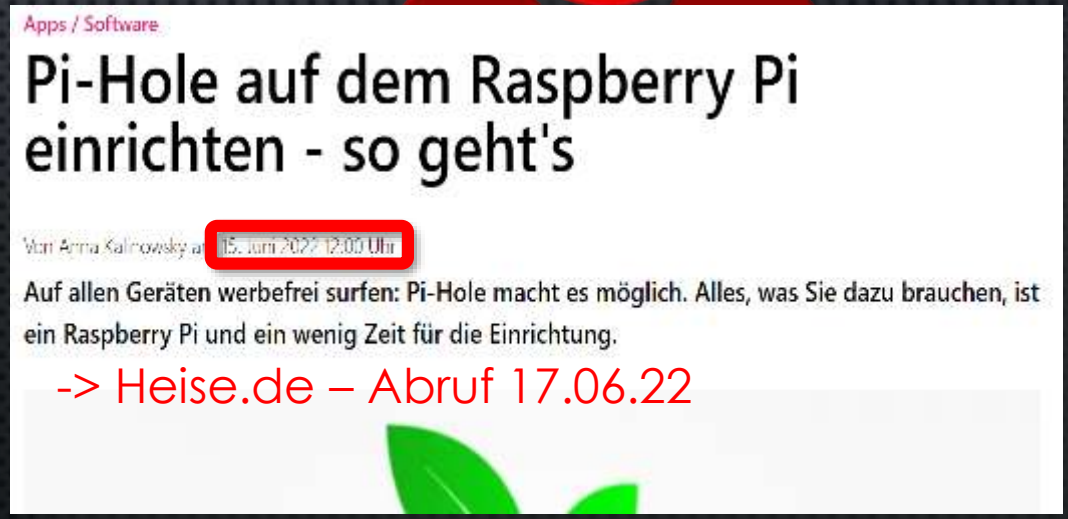
Pi-hole

Bei *Pi-Hole* handelt es sich um eine freie*, Open-Source-Software die auf einem Linux-System aufgesetzt wird und alle im zugehörigen Netzwerk befindlichen System schützt (Projektstart 2015).

Da der Einplatinencomputer „*Raspberry Pi*“ sehr günstig anzuschaffen ist und trotzdem ein voll-wertiges Linux-System beinhaltet, stellt er eine gute Basis für ein zentrales Schutzsystem dar.

***Pi-Hole* ist performant und kann deshalb durchaus auch auf einem „in der Bastelkiste“ vorhandenen älteren Pi aufgesetzt werden, denn ein Neukauf ist derzeit mit höheren Kosten bzw. langen Liefer-zeiten verbunden…**





*** Eine kleine „Donation“ zur Unterstützung ist aber nicht unerwünscht ;-)**

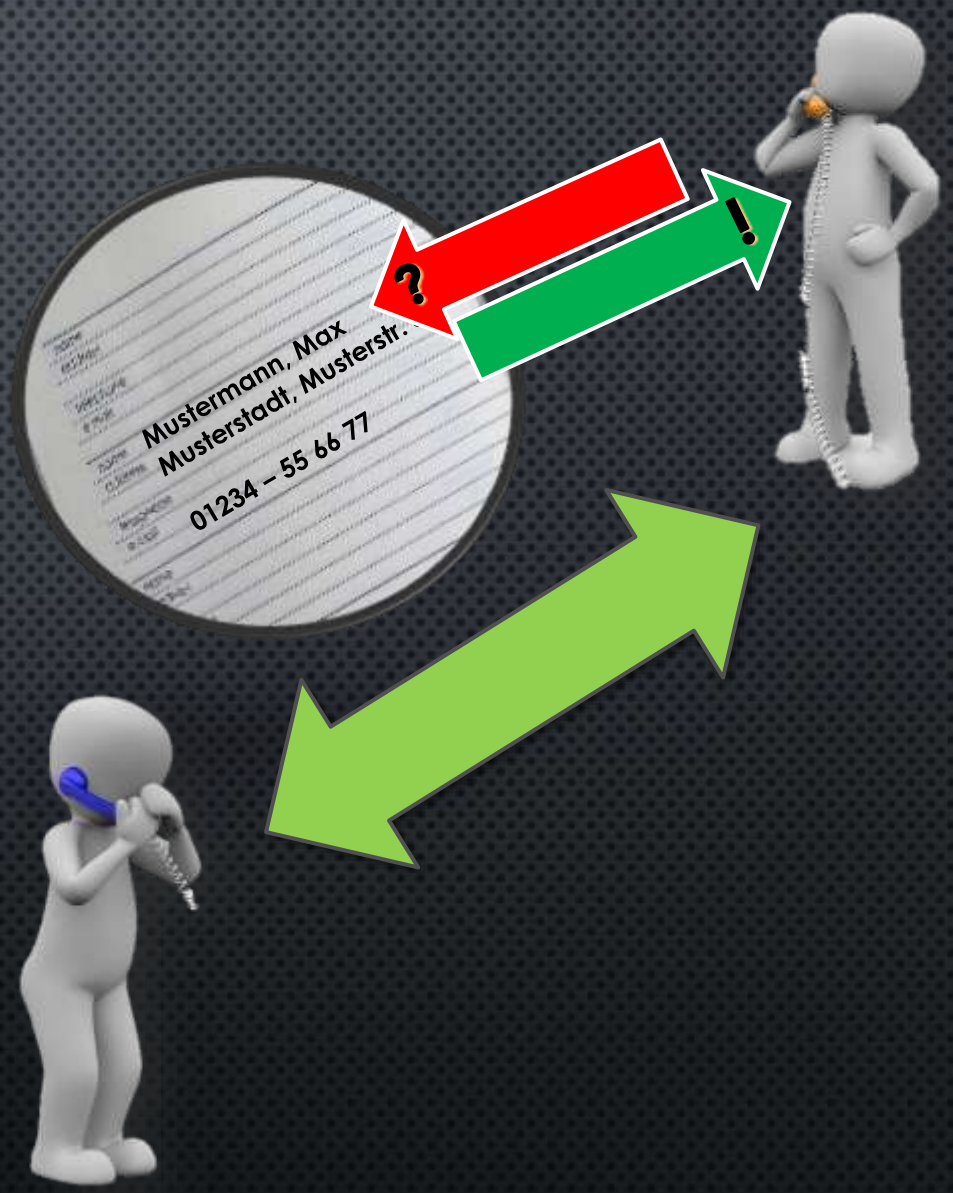
Funktionsweise

Wie kann aber ein kleiner Linux-Einplatinen-computer „ein ganzes Netzwerk“ schützen?

Machbar ist dies dank eines elementaren Netzwerkdienstes namens „*Domain Name Service*“, kurz *DNS*.

Stellen Sie sich vor Sie müssen Max Mustermann anrufen, kennen aber seine Telefonnummer nicht…

Hier hilft die Auskunft oder ein Telefonbuch, in welchem anhand (Land,) Ort, Name und ggfs. Adresse die Telefonnummer ermittelt und Ihnen mitgeteilt wird.



Funktionsweise

Wie kann aber ein kleiner Linux-Einplatinen-computer „ein ganzes Netzwerk“ schützen?

Machbar ist dies dann eines grundsätzlichen Netzwerkdienstes namens „*Domain Name Service*“, kurz *DNS*.

Stellen Sie sich vor Sie müssen Max Mustermann anrufen, kennen aber seine Telefonnummer nicht…

Hier hilft die Auskunft oder ein Telefonbuch, in welchem anhand (Land,) Ort, Adresse und Name die Telefonnummer ermittelt und Ihnen mitgeteilt wird.

Und im Internet läuft es technisch ähnlich ab:

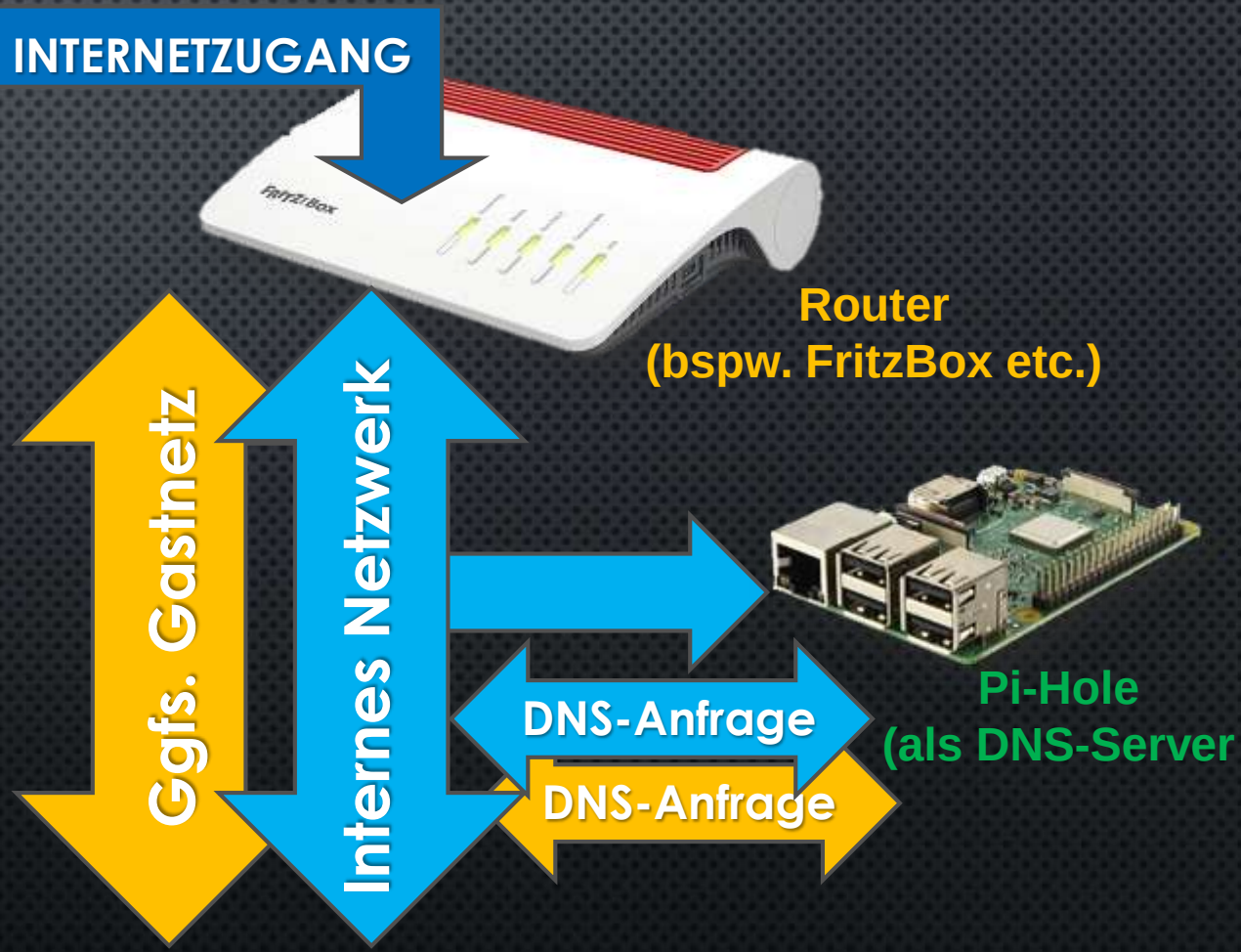
-> vdi.de – Abruf 14.07.22

Verwendung in Ihrem Heimnetzwerk

Entgegen der ersten Vermutung ist es recht einfach, einen Pi-Hole im eigenen Netzwerk nutzen zu können!

Der mit *Pi-Hole* ausgestattet Raspberry Pi wird im Netzwerk als „DNS-Server“ eingerichtet und übernimmt dann diese Aufgabe (-> idR. vom Router)

Die häufigste Art für solch eine Anwendung ist ein sogenanntes „*Headless System*“, bei dem der Raspberry weder über Monitor noch Maus/ Tastatur verfügt und rein übers Netzwerk bedient wird (SSH-Zugang)!



-> Bild der Fritzbox - https://avm.de/produkte/fritzbox/ Abruf 14.07.22

Was benötige ich?

Bei einem Headless System nur wenig:

- **Raspberry Pi -> Raspberry Pi 3**
- **Netzteil -> mind. 5V/2,5 A**
- **(Micro)SD-Karte -> mind. 4 GB**
- **Betriebssystem -> Raspberry OS**
- **Netzwerkkabel -> WLAN langsam…**
- **Statische (feste) IP**

https://www.raspberrypi.com/software/

Alternativ (Full System):

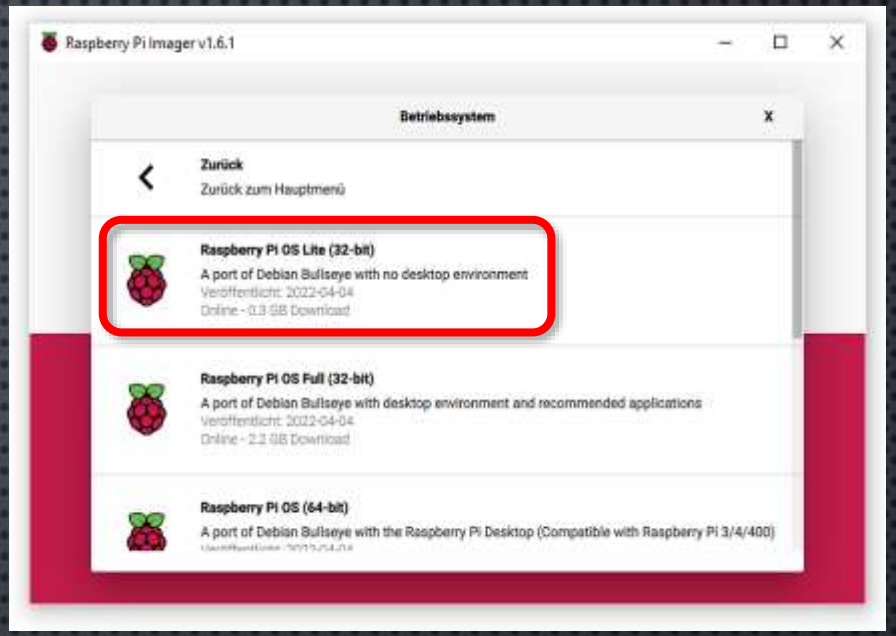
- **zusätzlich Monitor, Tastatur/Maus**
- **(Micro)SD-Karte -> mind. 8 GB**

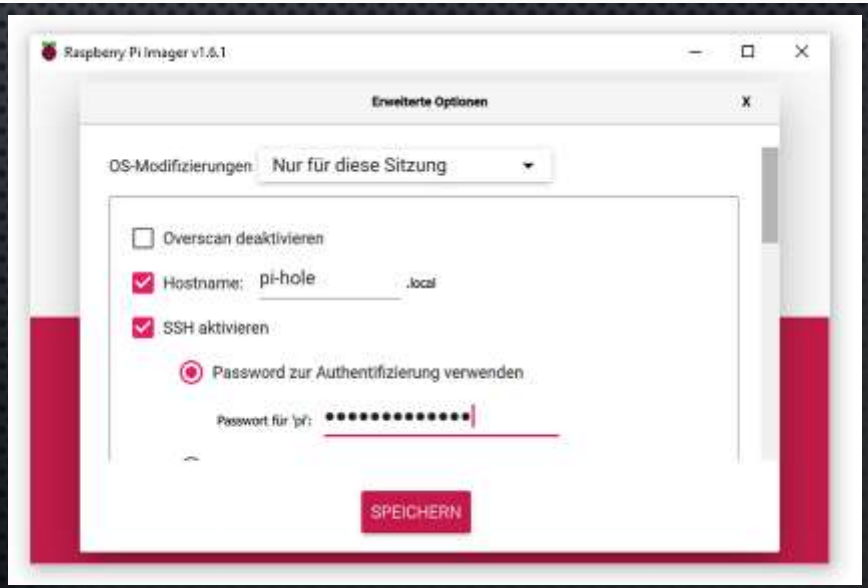
Headless System

Wenn über den *Pi Imager* das Betriebssystem auf eine SD-Karte aufgebracht werden soll, dann kann für ein *Headless System* das

Raspberry Pi OS Light

ausgewählt werden – hierin sind keine Desktop-Komponenten enthalten.





Tipp:
Über<*Strg*> + <*Shift*> + <*X*> *kann* nebenstehendes Zusatzmenü mit „*Erweiterten Optionen*“ geöffnet und eine Vorkonfiguration getroffen werden. So kann hier schon der SSH aktiviert und mit einem Passwort versehen werden.

… Weitere Informationen zur Installation über SSH im Handout…

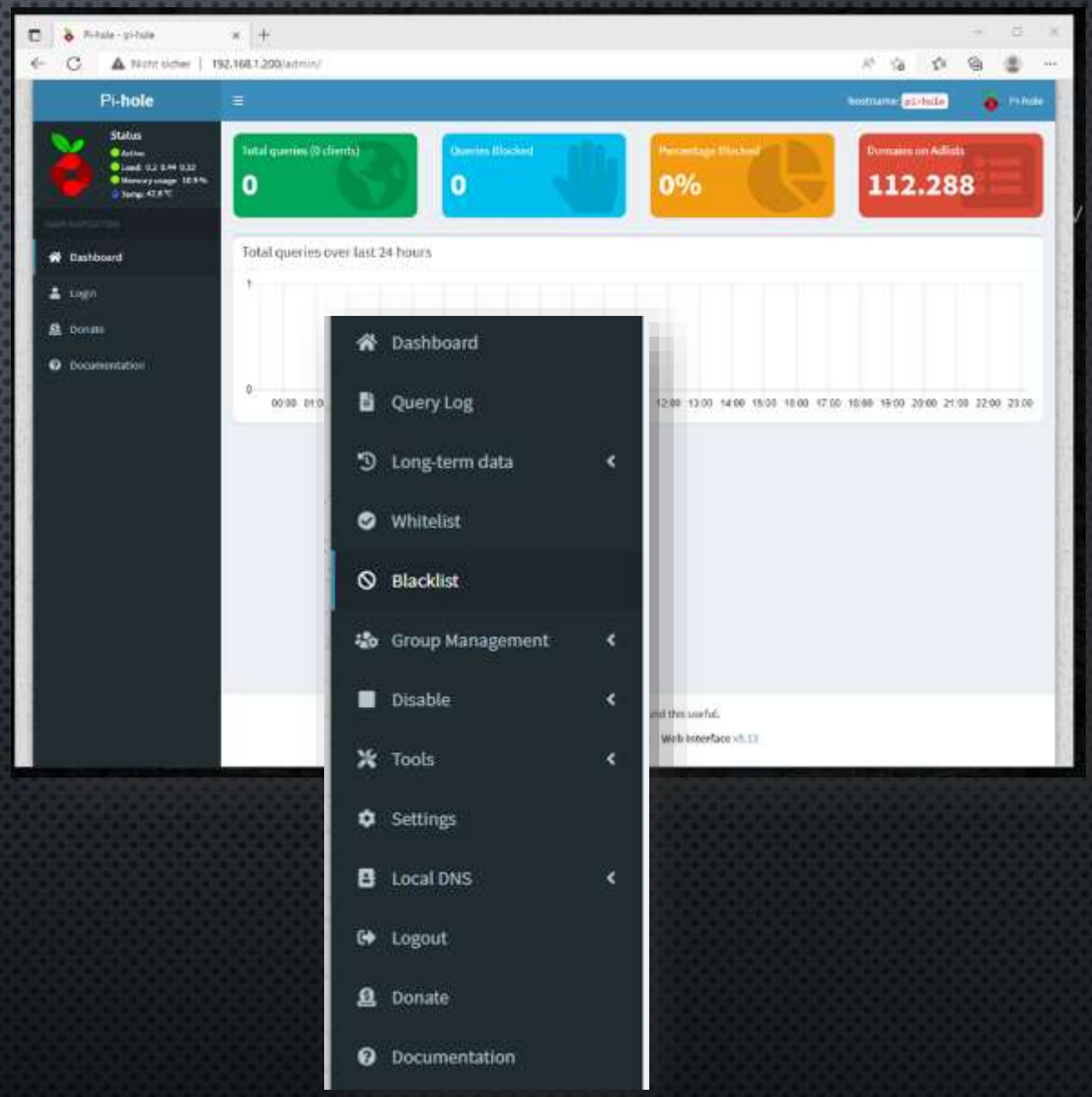
Das „Dashboard“

Wenn man den Pi-Hole konfigurieren oder seine Arbeit kontrollieren möchte, so kann er im Netzwerk über

IP-Adresse/admin
(bspw. XXX.XXX.XXX.XXX/admin)

angesprochen werden.

Nach der Anmeldung mit Kennwort erscheint neben dem sogenannten Dashboard, quasi dem Armaturenbrett des Pi-Holes, eine Navigation mit allen Menüs.



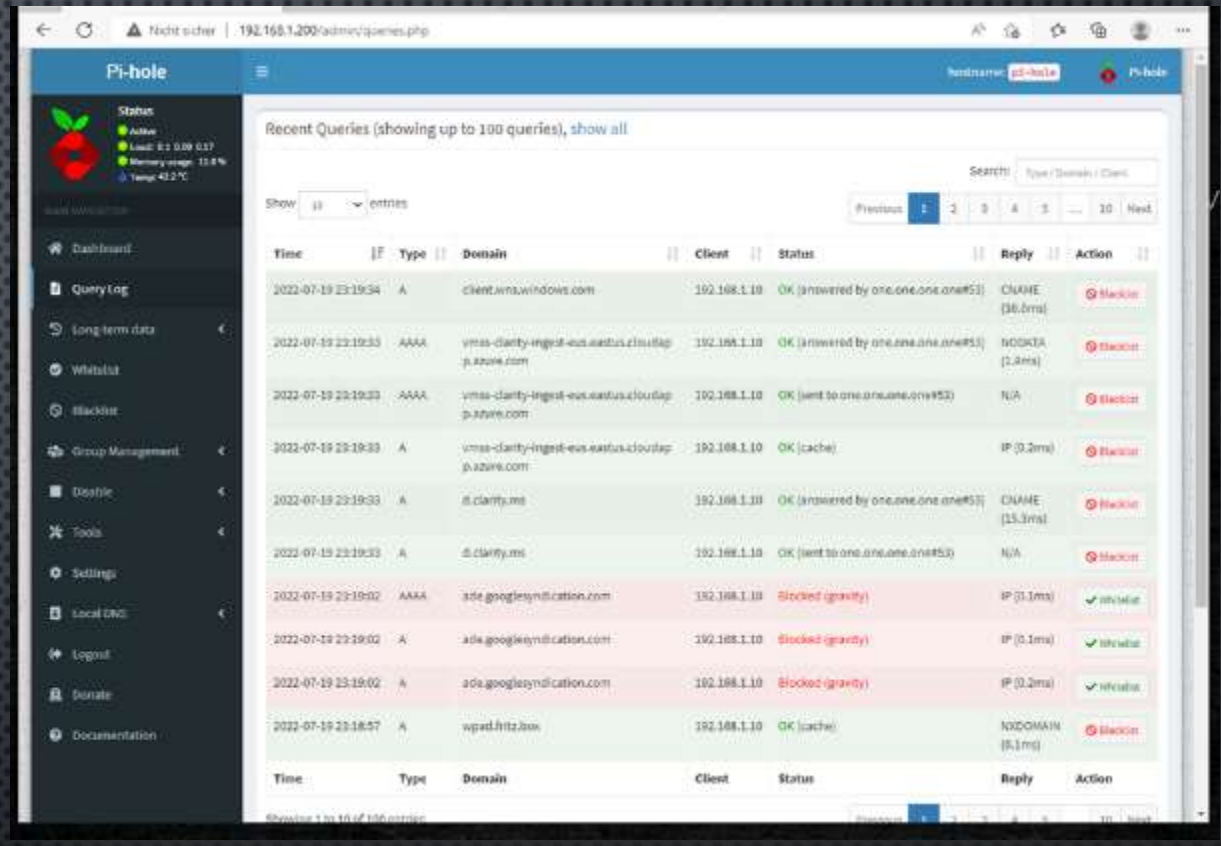
Query logs

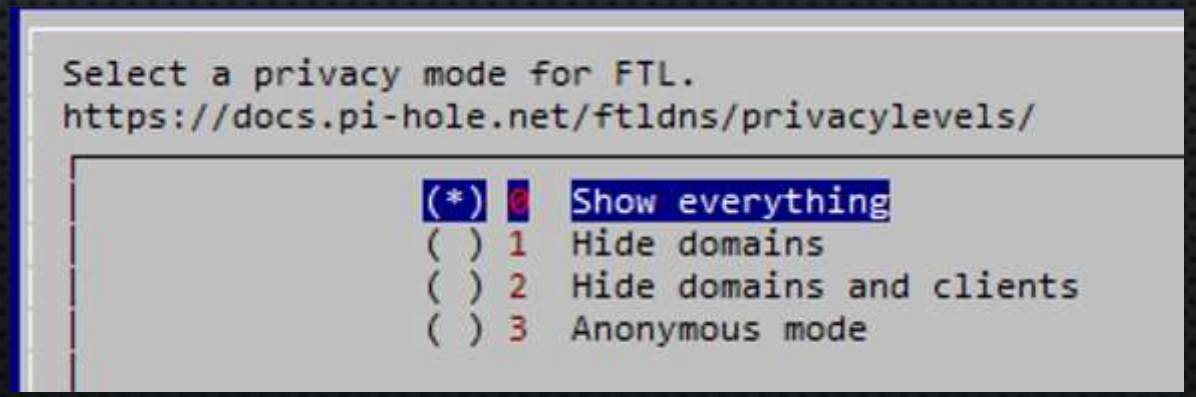
Erster Anlaufpunkt zur Überprüfung der Anfragen/ Blockaden ist das *Query Log*.

Ob und was hier angezeigt wird kann während der Konfiguration des *Pi-Holes* definiert werden!

Über die *Action-Spalte* können direkt aus den Logs heraus Seiten geblockt bzw. wieder freigegeben werden, indem sie auf die White- oder Blacklist gesetzt werden.

Die Basis für die Filterung wird über das Gravity-Modul durchgeführt, welches die *Adlisten* verwaltet.





Adlist

Im *Group Management* werden unter anderem die Adlists verwaltet.

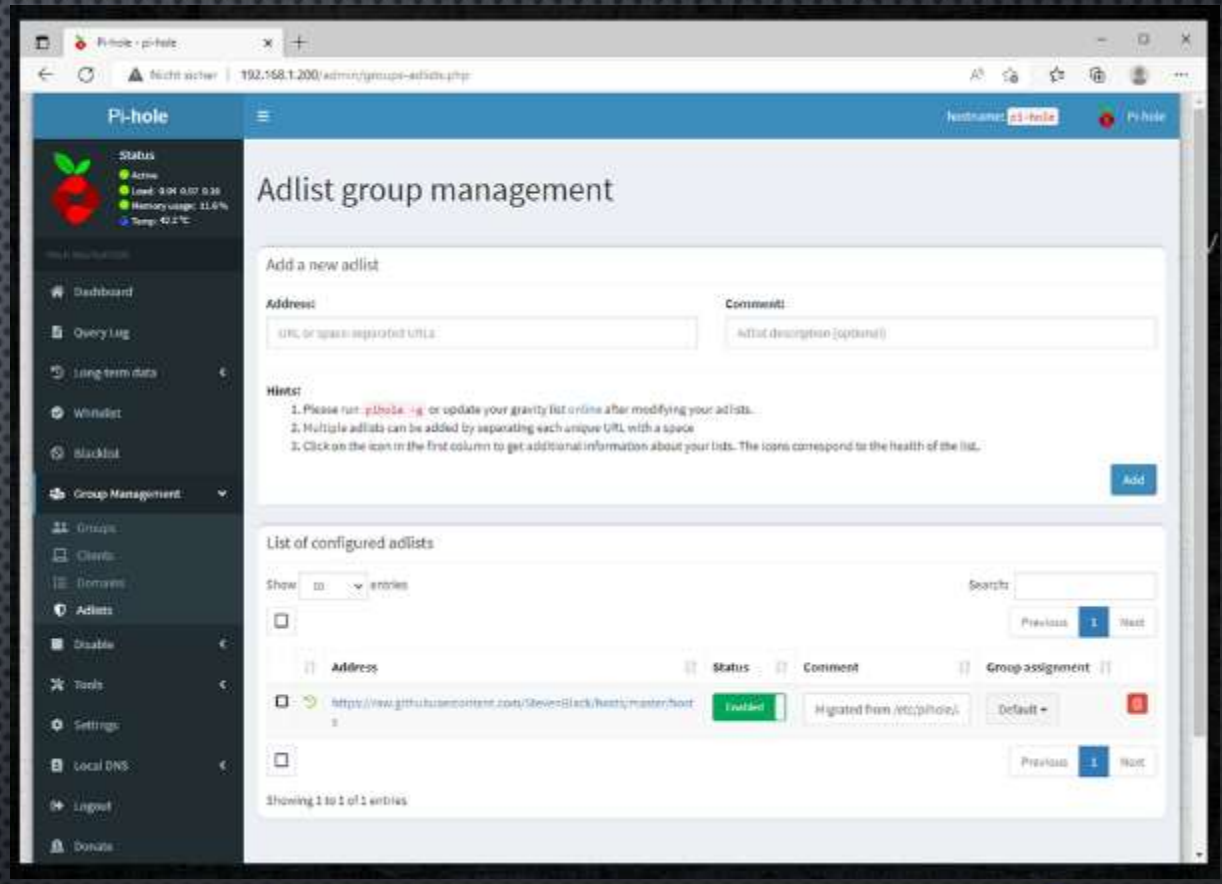
Während der Installation kann zwar schon eine Liste eingerichtet werden (ca. 123.000 Einträge), zielführend sind natürlich viele weitere.

Auf Github findet sich eine große Auswahl, die auch diverse Themenbereiche abdecken.

Beispielsweise:

https://github.com/topics/pihole-ads-list

Wichtig ist jedoch immer im Hinterkopf zu behalten, das die Blockaden nicht auf einer Contentfilterung basieren…



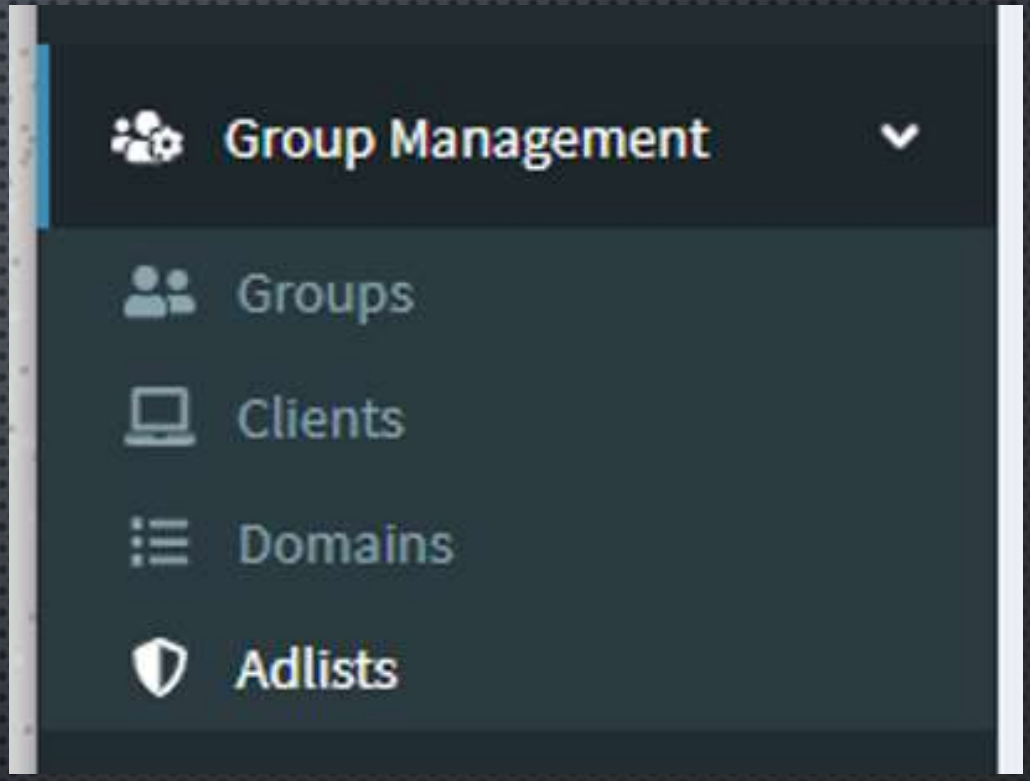
Usermanagement

Neben den Adlists werden im *Group Management* auf die Blockier.- bzw. Freigabegruppen, sowie die Clientverwaltung vorgenommen.

Out-of-the-box sind alle Seiten für alle Anfragenden über die *Default-Gruppe* blockiert.

Sofern man bestimmte Seiten nur selektiv sperren/freigeben möchte, so können Gruppen angelegt und diese dann der Adlist zugeordnert werden.

Die anfragenden Clients sind in der Rubrik Clients gelistet und können dort wiederum den jeweiligen Gruppen zugeordnet werden…

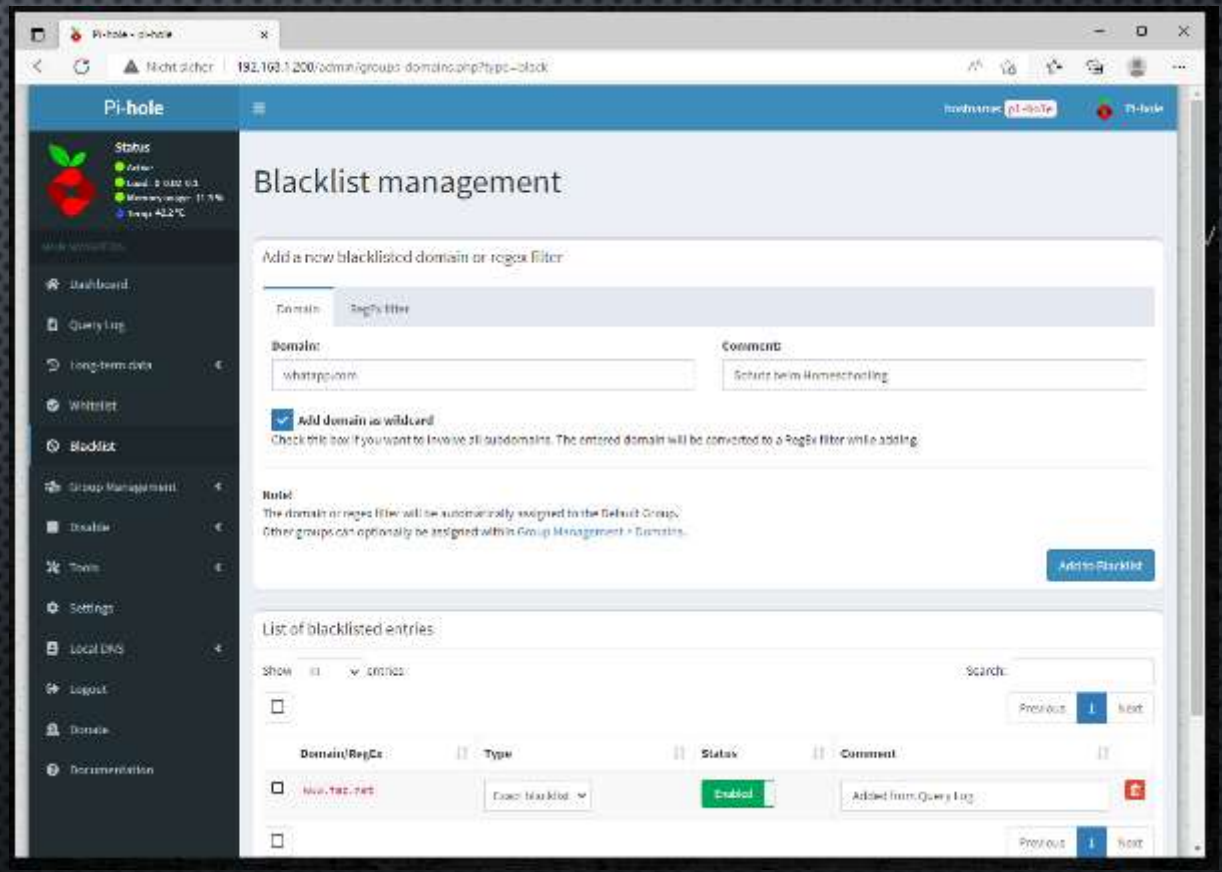


Black.-/Whitelisting

Wenn eine DNS-Anfrage über unseren *Pi-Hole* eingeholt und dabei unerwünschte Werbung/ Tracker erkannt wurde, sprich die Adresse steht auf einer Adlist (*Blacklist/Denylist), erhält der Anfragende 0.0.0.0 als „Ziel“ zurückgemeldet**

Um manuell Seiten zu blockieren/sperren kann man diese direkt im „*Query Log*“ unter *Action* auf die *Blacklist* bzw. *Whitelist* setzen.

Alternativ kann man bekannte Seiten auch manuell auf eine der Listen setzn. Hier unterscheidet Pi-Hole zwischen „reinen“ Domainnamen und sogenannten „RegEx“-Filter. Bei letzteren kann man durch spezielle Ausdrücke exaktere Filter definieren.



*** Black.-/Whitelisting sind derzeit noch namentlich in Pi-Hole enthalten….**

Tipps

Rien ne va plus – nichts geht mehr

Sollte im Netzwerk die Namensauflösung nicht mehr gehen muss es nicht nur am Pi-Hole liegen…

a. Router-Neustart
   -> Verteilung DNS-Server per DHCP

b. Pi-Hole neu starten

c. Gravity updaten (evtl. Datenbankproblem)

Client mit Werbung

Wenn ein Client im Netzwerk trotz Pi-Hole weiterhin Werbung anzeigt, prüfen ob die Namensauflösung auch wirklich durch den Pi-Hole läuft

Bspw. mit nslookup domainname

```
>nslookup vdi.de
Server:  dns.google
Address:  8.8.8.8

Nicht autorisierende Antwort:
Name:    vdi.de
Address:  194.245.143.90
```

Tipps

Netzteil

Beim Arbeiten mit einem Raspberry Pi ist das verwendete Netzteil sehr wichtig. Abhängig vom eingesetzten Typ ist der Ampere-Wert wichtig.

Bis zum Raspberry Pi 2 war ein 2A-Netzteil ausreichend, ab V3 sind mindestens 2,5A ratsam.
Die 4. Generation setzt auf USB-C und mind. 3A

Kühlkörper

Wer mit einem Raspberry Pi arbeitet wird im Internet immer auf den notwendigen Einsatz von Kühlkörper hingewiesen.

Sofern man den Raspberry Pi nicht übertaktet sind Kühlkörper für den Einsatz als Pi-Hole NICHT erforderlich – schaden aber auch nicht…

…und

Ja, man braucht keine Oberfläche…

Ja, es geht über die Kommandozeile ;-)

Infos unter:

https://docs.pi-hole.net/core/pihole-command/

Pi-hole Core

Feature	Invocation
Core	`pihole`
Whitelisting, Blacklisting and Regex	`pihole -w`, `pihole -b`, `pihole -regex`, `pihole -wild`
Debugger	`pihole debug`
Log Flush	`pihole flush`
Reconfigure	`pihole reconfigure`
Tail	`pihole tail`
Admin	`pihole -a`
Chronometer	`pihole chronometer`
Gravity	`pihole updateGravity`
Logging	`pihole logging`
Query	`pihole query`
Update	`pihole updatePihole`
Version	`pihole version`
Uninstall	`pihole uninstall`
Status	`pihole status`
Enable & Disable	`pihole enable`
Restart DNS	`pihole restartdns`
Checkout	`pihole checkout`

Linkliste

Betriebssystem :

Raspberry PI OS Imager Software zum Download des Betriebssystems, einrichten der SD-Karte

www.raspberrypi.com/software

Installationerklärung/Tutorial:

Sehr ausführliches Tutorial von KENO (ct Magazin)

https://www.heise.de/news/c-t-3003-Pi-Hole-kann-Ladezeiten-halbieren-Tutorial-7101911.html

Raspion :

Pi-Hole ist Teil der Rasion-Suite der ct, die viele nützliche Zusatz-funktionen bietet

https://www.heise.de/ct/artikel/c-t-Raspion-Projektseite-4606645.html

Foren :

https://discourse.pi-hole.net/c/bugs-problems-issues/11

deutsch: https://discourse.pi-hole.net/c/bugs-problems-issues/deutschsprachige-hilfe/15

Adlists : u.a. https://github.com/topics/pihole-ads-list

Fragen?

Danke für‘s

DABEISEIN

Wenn‘s noch Fragen gibt, gerne!

Bilderquelle

Soweit nicht speziell genannt entstammen die verwendeten Bilder von:

- www.pixabay.de
- www.pexels.com