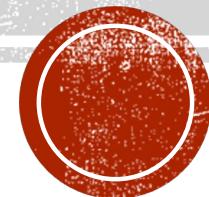


PRIVACY TO GO

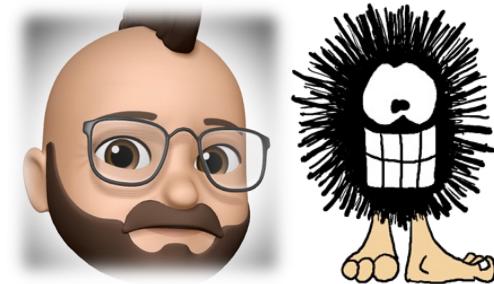
Der “Werbeblocker” für die Hosentasche
mit Pi-hole und WireGuard VPN



GPN22

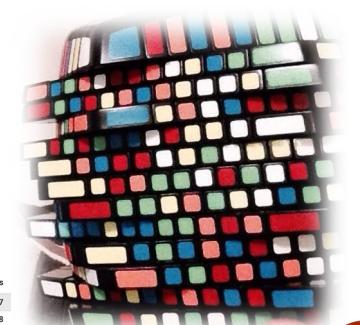
 [@abimelechbeutelbilch@fulda.social](mailto:abimelechbeutelbilch@fulda.social)
 github.com/thomasmerz/

BEVOR ES LOSGEHT: WER REDET DA?



- Linux seit 1994: Irix, Solaris, SUSE – Angewandte Informatik
- WEB.DE (SUSE; DNS, Webserver) 2J
- dm-drogeriemarkt / dmTECH
 - zOS und DB2 ~10J
 - SLES-for-SAP (HANA) + RHEL;
Lifecycle/Config/Patch-Management, IT-Sicherheit/Security ~10J
- Motördad und Metalhead + Radfahrer und Carsharing
- “Speedcubing” (3, 5, 7, ... 13)
- OpenSource ❤
- GitHub Fun-Facts ;-)
 - multilingual mit 17 Sprachen
 - Im Schlaf am aktivsten und produktivsten (3am)

Disziplin	NR	CR	WR	Einzelergebnis
3x3x3 Würfel	2752	45025	184775	47.07
5x5x5 Würfel	871	9675	29764	4:32.68



DISCLAIMER

- Alle Produktnamen sind nur (gute) Beispiele.
- Es gibt auch andere (gute) Tools.
- Dies ist kein Vortrag zum Bekehren.
- Dies ist kein Workshop. Fragen/Deepdive im Anschluss oder draussen...
- Dieser Talk zeigt nur einen bzw. zwei Bausteine wie man seine digitale Privacy schützen kann!
- **Digitale Souveränität**
 - Selbstbestimmte Nutzung und Gestaltung von Informationstechnik
 - digitale Kompetenz als Sachkenntnis
- ...führt zu **digitaler Selbstverteidigung**



WER IST ZIELGRUPPE?

- User, die keine Werbung, Tracking und Schadencode mögen und sich “irgendwie” selber schützen wollen
- Technisch versierte User mit **Linux** und **Docker** Knowhow sowie **Netzwerk**-Grundlagen!



HALLO, UM WAS GEHT ES ÜBERHAUPT?

- Surfen/Computernutzung **ohne Belästigung, Überwachung und Gefährdung** durch
 - Werbung
 - Tracking
 - >1000 Firmen (nicht nur GAFAM (“Big Tech”)) kennen dich besser als du dich selber kennst und deine Familie und Freunde dich kennen!!!
 - Malware
- Plus:
 - Jungendgefährdende Seiten (je nach Alter) / NSFW
 - Social Media (bei Bedarf)
 - Umgehung von Provider-Sperren/Zensur...
- Auf **allen Geräten**: Smartphone, Tablets, PCs, Fernseher, Sticks...
 - An allen Orten
 - Zuhause im WLAN
 - Unterwegs in Gäste-WLANs, im Mobilfunknetz, in jedem Land (DE, EU, Welt)



KAMPF DER IGNORANZ UND UNWISSENHEIT!

- “Werbung? Nutzt du keinen [#adblocker](#)?”
- “**ich sehe für mich keine Gefahr und möchte mich damit nicht beschäftigen. Es stört mich auch nicht.**”
- “Du siehst darin keine Gefahr, dass alle Seiten, die du besuchst, in einem Profil über dich landen und dieses Profil dann benutzt wird, um dich gezielt zu manipulieren?”
- “Und dazu kommt die latente und leider reale Gefahr sich durch Werbeseiten [#malware](#) [#schadsoftware](#) einzufangen. Hier im Büro hat genau das ein paar Windows Clients das Leben gekostet. Sagen zumindest die [#ITForensik](#) Experten”

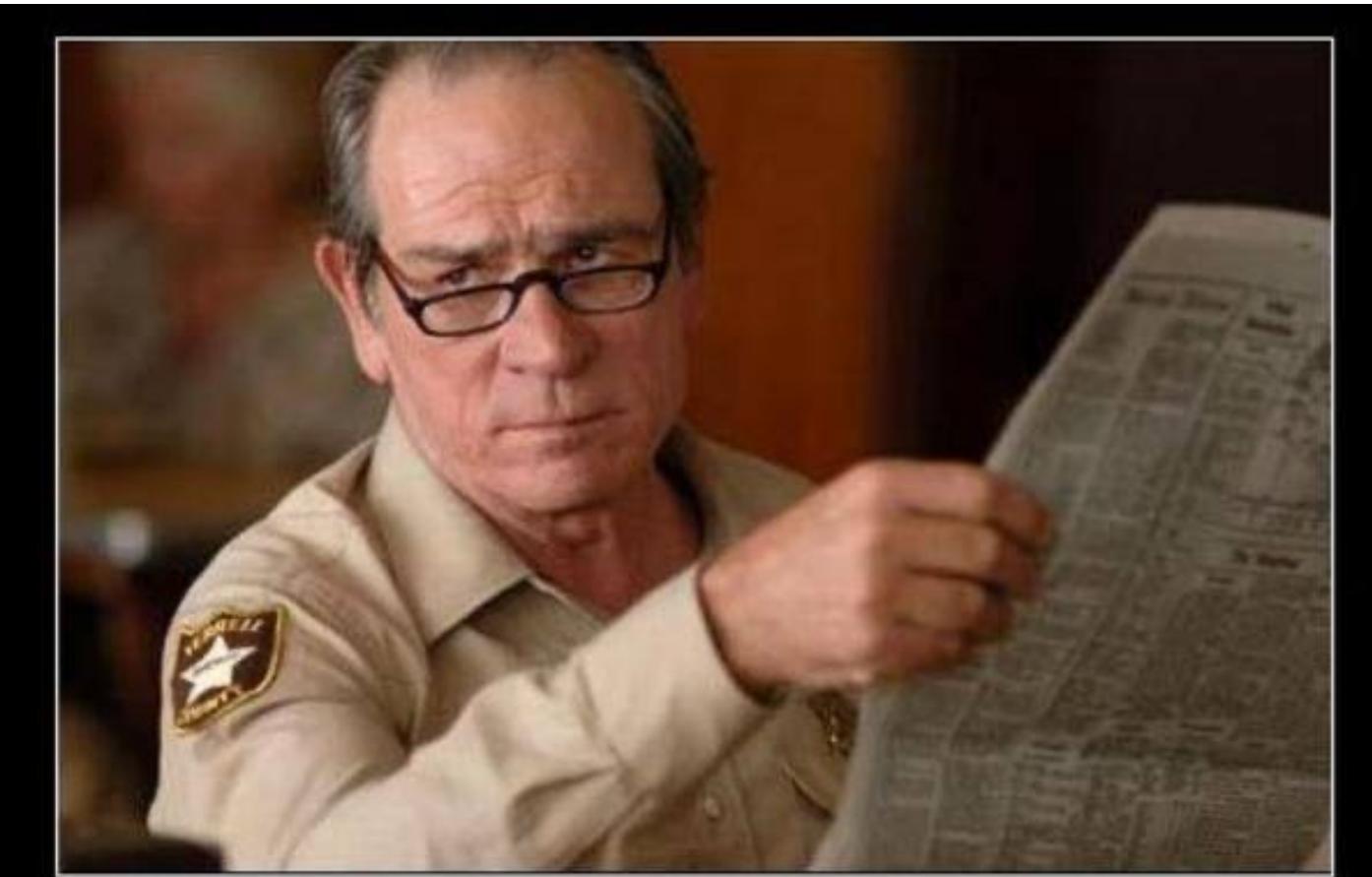
Die Autoren sind dem Referenten “bekannt”



ZAHLEN, DATEN, FAKTEN AUS C'T 12/2024

- Je jünger desto “anzeigenfreundlicher”:
- “Werbung macht mir nichts aus, wenn ich Gratisinhalte bekomme”
→ “Ist etwas kostenlos, dann bist du das Produkt!”
- “Die Nutzung meiner Daten durch Unternehmen für Werbezwecke macht mir nichts aus”
- “Ich kann Inhalte oft nicht von Werbung unterscheiden”





IMPLIED FACEPALM

When something is so utterly stupid
a full and proper facepalm is not even necessary



FRAGEN ANS AUDITORIUM

- Wer filtert schon Werbung?
- Wer glaubt schon Werbung zu filtern?
- Wie filtert ihr?
 - Browser-Extension?
 - App? (kostet die was?)
 - Pihole/AdGuard/Blocky/...?
 - /etc/hosts?
 - VPN? (im Ernst?)



SCAN ME



EMPFEHLUNG AUS DEM KUKETZ-BLOG

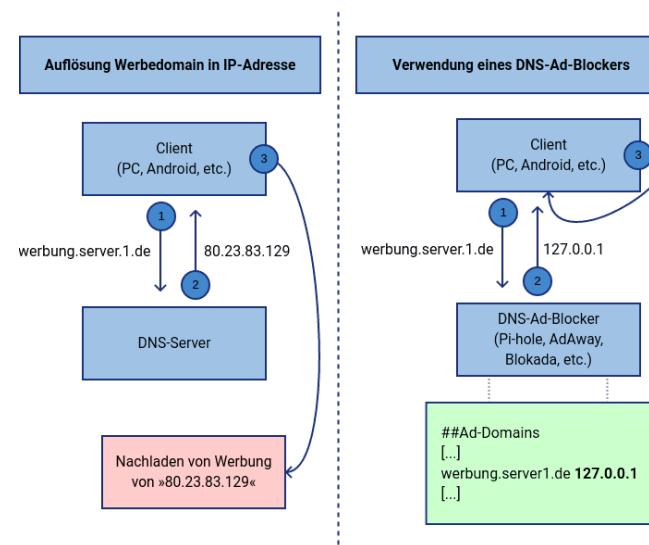
IT-SICHERHEIT | DATENSCHUTZ | HACKING

- <https://www.kuketz-blog.de/empfehlungsecke/#adblocker>
- Ein **Werde- bzw. Trackingblocker** zählt mittlerweile zur **Grundausstattung** der digitalen Selbstverteidigung. Denn die heile Welt der Online-Werbung hat längst ein großes Problem: **Malvertising** – also die Auslieferung von Werbung, die **Schadcode** enthält und damit ein **Risiko für den Nutzer bzw. seine Daten** darstellt.
- Aber nicht nur Malvertising ist ein Ärgernis, sondern auch Tracking-Firmen, die **ungefragt die Aktivitäten von Nutzern auf Webseiten und innerhalb von Apps aufzeichnen, auswerten und die Daten gewinnbringend vermarkten**. Man könnte sie auch als »**digitale Parasiten**« bezeichnen, die eigentlich niemand braucht, deren parasitäres Verhalten aber von den meisten Nutzern nicht bemerkt wird, weil es äußerst subtil und nahezu unsichtbar ist. **Aufgeklärte Nutzer** müssen sich aber nicht einfach mit diesen Privatsphäre missachtenden Protagonisten abfinden, sondern können **technisch aufrüsten** und ihnen **den Datenhahn zudrehen**.



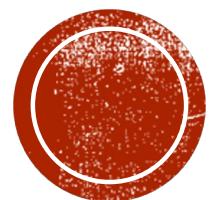
LEVELS OF DIGITALE SELBSTVERTEIDIGUNG

- DNS-Blocking [Anfänger/Bequeme]
dnsforge.de, dismail.de, NextDNS, AdGuard, Blokada, ...



- Empfehlenswerte Tools [Anfänger bis Fortgeschrittene] → Browser-Extentions
- **Mehr Kontrolle – höhere Blockraten** [Fortgeschrittene] → z.B. Pi-hole
- Kontrollfetischisten [Profis] → IPFire





BEGRIFFE . . .



“PRIVACY”

- **Privatsphäre** bezeichnet den **nichtöffentlichen Bereich**, in dem ein Mensch, unbekümmert von äußeren Einflüssen, sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt.^[1] Das *Recht auf Privatsphäre* ist als **Menschenrecht** in allen modernen **Demokratien** verankert. Dieses Recht kann aufgrund des öffentlichen Interesses an einer Person oder zum Zwecke der Strafverfolgung eingeschränkt werden.
- Neue Technologien haben dazu geführt, dass heute ein **Verlust an Privatsphäre** durch **viele moderne „Errungenschaften“** wie z. B. Mobiltelefone, Bankomatkarten und Kreditkarten zu beklagen ist. Oft ist es kaum möglich, den **nahezu omnipräsenen Überwachungstechnologien** zu entgehen.
- Aber auch **Wirtschaft** und **Werbung** stellen mit Scoring- (Schufa), Marktforschungs- Maßnahmen und **Konsumenten-Profilings** für Kritiker eine **zunehmende Bedrohung von Privatsphäre** dar.



PRIVACY / DATENSCHUTZ

- Schutz personenbezogener Daten
 - Unverletzlichkeit des Post- und Fernmeldegeheimnisses
 - Unverletzlichkeit der Wohnung
-
- **Datenschutz**
 - Schutz vor missbräuchlicher Datenverarbeitung
 - Schutz des Rechts auf informationelle Selbstbestimmung
 - Schutz des Persönlichkeitsrechts bei der Datenverarbeitung
 - **und auch Schutz der Privatsphäre**
 - jeder Mensch darf grundsätzlich selbst darüber entscheiden, wem wann welche „seiner“ persönlichen Daten zugänglich sein sollen.
 - **Machtungleichheit** zwischen Organisationen und Einzelpersonen
 - Entgegenwirken zum sogenannten **gläsernen Menschen**, dem Ausufern staatlicher Überwachungsmaßnahmen (**Überwachungsstaat**) und **Datenmonopolen** von Privatunternehmen



WAS IST PIHOLE?



- “Pi-hole
 - ist eine freie Software
 - mit der Funktion eines Tracking- und Werbeblockers ...
 - basiert auf einem Linux-System und ist entwickelt worden für den Einsatz auf Kleinstcomputern im Sinne eines eingebetteten Systems. Verbreitet ist der Einsatz auf Computern der Raspberry-Pi-Serie.
- Die Software wird als DNS-Server in ein bestehendes Netzwerk integriert
- und **steht damit allen Geräten im Netzwerk zur Verfügung,**
- **deren DNS-Einstellungen sich konfigurieren lassen.”**



WAS IST WIREGUARD?



- “WireGuard
 - ist eine freie Software
 - zum Aufbau eines virtuellen privaten Netzwerkes (VPN)
 - über eine verschlüsselte Verbindung.
- direkt im Linux-Kernel ab Version 5.6 integriert
- **höhere Verarbeitungsgeschwindigkeit als vergleichbare Lösungen wie IPsec oder OpenVPN”**



WAS IST EIN “VPN”?

- “**Virtual Private Network**
 - (**deutsch „virtuelles privates Netzwerk“; kurz: **VPN****)
 - bezeichnet eine Netzwerkverbindung, die **von Unbeteiligten nicht einsehbar** ist.”



SCAN ME



EMPFEHLUNG AUS DEM KUKETZ-BLOG

IT-SICHERHEIT | DATENSCHUTZ | HACKING

- <https://www.kuketz-blog.de/empfehlungsecke/#vpn-anbieter>
- Ein VPN ist nicht sinnvoll für folgende Zwecke:
 - **Erreichen von Anonymität**
 - Schutz vor Hacking, Cyber-Bedrohungen und/oder Identitätsdiebstahl
 - Verschleierung des GPS-Standorts (bspw. Mobilgerät)
 - Passwörter schützen
 - **Verhindern, dass Microsoft, Google oder Facebook private Daten sammeln**
 - **Verhinderung von unerwünschter Profilbildung/Tracking durch soziale Netzwerke, Suchmaschinen oder andere Dienstleister**
 - Vermeidung von Daten-Leaks, bei der Nutzung von Online-Diensten



KANN IN EINIGEN FÄLLEN NÜTZLICH SEIN:

- Verbesserung der Sicherheit in unsicheren/nicht vertrauenswürdigen öffentlichen Netzwerken (Cafés, Züge etc.) durch Prävention von [Man-in-the-Middle-Angriffen](#)
- **Umgehung von Zensur oder geografischen Sperren** (Geoblocking) von Websites und Inhalten
- **Verschlüsselung der Kommunikation, damit der Internet- oder Mobilfunkanbieter die Online-Aktivitäten nicht überwachen oder aufzeichnen kann**
- **Verschlüsselung der DNS-Anfragen, damit der Internet- oder Mobilfunkbetreiber die besuchten Domains nicht protokollieren kann**
- Verstecken/Maskieren der IP-Adresse vor den besuchten Websites und Servern
- **Getunnelte Verbindung nach Hause und/oder zum Arbeitgeber, um auf Dienste zuzugreifen, die nicht direkt über das Internet erreichbar sind**



TL;DR

- **Pi-hole**

- Abwehr von “nerviger” Werbung
- Schutz vor Tracking von neugierigen Firmen/Konzernen
- Malware-Schutz
- Schnellere Ladezeiten von Webseiten 

- **WireGuard VPN**

- Schutz vor “neugierigen” Providern
- Sowie staatlichen Institutionen (wer's braucht...)
- Split-Tunnel möglich:
 - nur DNS, keine Geoblocking-Umgehung, Kommunikationsüberwachung



LADEZEITEN / KNOFFHOFF: DNS

- Ähnlich wie **Telefonbuch**: spiegel.de has address 128.65.210.8
- Browser / irgendein Programm
- DNS-Resolver im OS (Windows, MacOS, Linux, Android, iOS)
- Router
- DNS-Resolver vom Provider (wenn man Kunde bei Vodafone ist und die VF-Station ohne eigenen Router nutzt!) **bzw. “andere”**
- Authoritative Nameserver → example.com
- TLD-Nameserver (DE-NIC, ...) je Land
- Root-Nameserver (13 weltweit)



Recent Queries (showing queries for domain spiegel.de)

Search:

Show All entries

Previous 1 Next

Time	Type	Domain	Client	Status	Reply	Action
2024-05-17 10:02:59	A	spiegel.de	docker-b r-5dcacaf 2848e_pi hole	OK (cache) INSECURE	IP (0.2ms)	 Blacklist
2024-05-17 10:02:48	DS	spiegel.de	pi.hole	OK (answered by dns2.adguard.com#53)	NODATA (18.7ms)	
2024-05-17 10:02:48	A	spiegel.de	docker-b r-5dcacaf 2848e_pi hole	OK (answered by dns2.adguard.com#53) INSECURE	IP (50.4ms)	 Blacklist
2024-05-17 08:32:02	DS	spiegel.de	pi.hole	OK (answered by dns2.nextdns.io#53)	NODATA (30.6ms)	
2024-05-17 07:27:30	DS	spiegel.de	pi.hole	OK (answered by dns2.adguard.com#53)	NODATA (22.1ms)	
2024-05-17 06:27:18	DS	spiegel.de	pi.hole	OK (answered by resolver1.opendns.com#53)	NODATA (20.0ms)	
2024-05-17 04:22:18	DS	spiegel.de	pi.hole	OK (answered by zero.dns0.eu#53)	NODATA (19.6ms)	
2024-05-17 02:22:05	DS	spiegel.de	pi.hole	OK (answered by dns11.quad9.net#53)	NODATA (21.9ms)	
2024-05-17 01:17:27	DS	spiegel.de	pi.hole	OK (answered by dns2.nextdns.io#53)	NODATA (21.0ms)	
2024-05-16 23:17:05	DS	spiegel.de	pi.hole	OK (answered by dns2.adguard.com#53)	NODATA (19.0ms)	
2024-05-16 21:12:09	DS	spiegel.de	pi.hole	OK (answered by dns2.adguard.com#53)	NODATA (25.5ms)	



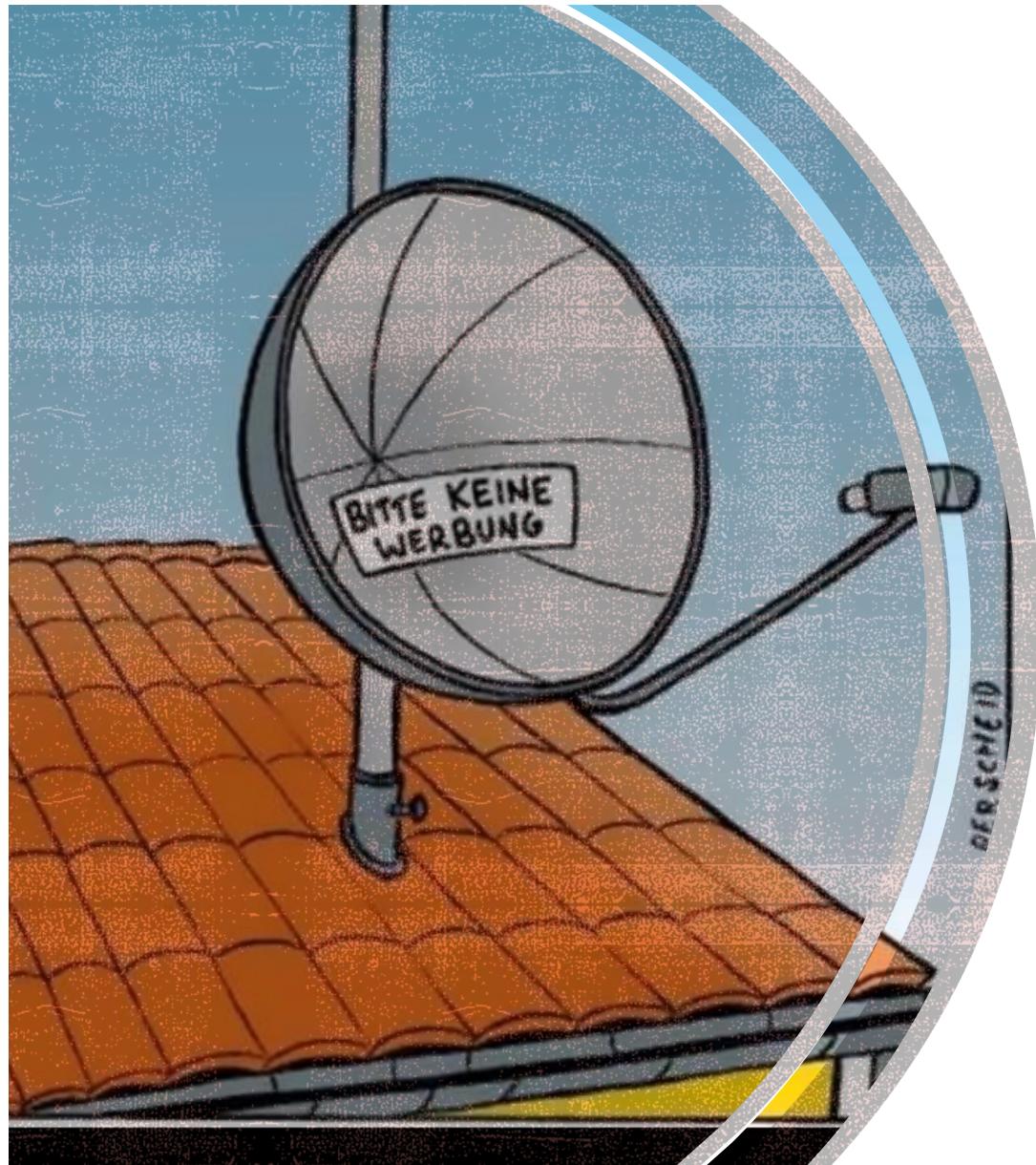
Recent Queries (showing queries for domain diesedomaingibtsnicht.co.uk)

Search:

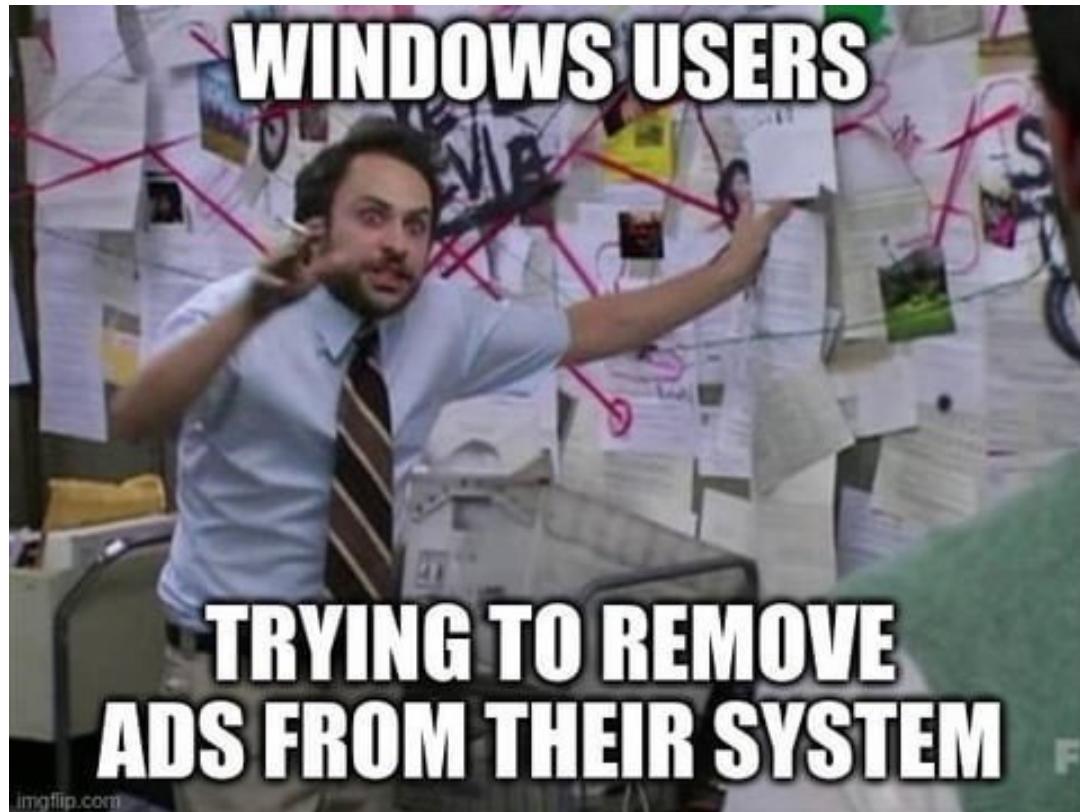
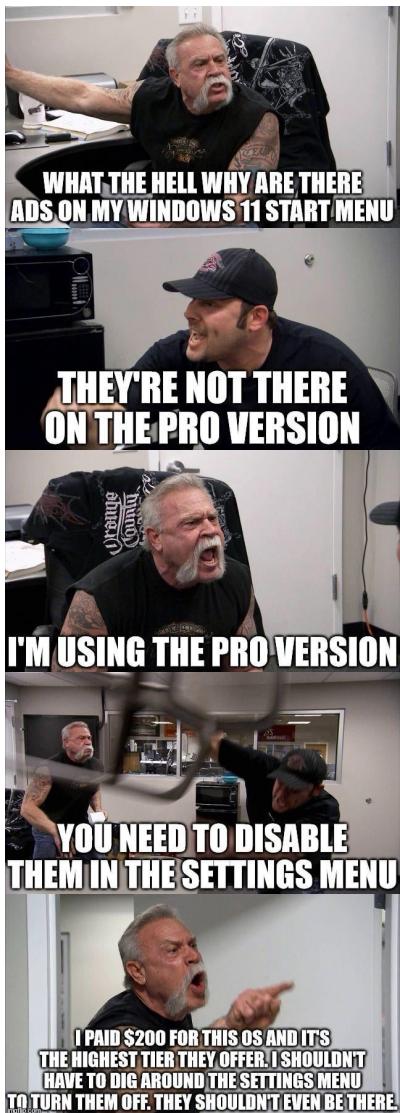
Show entries

Time	Type	Domain	Client	Status	Reply	Action
2024-05-17 10:57:33	A	diesedomaingibtsnicht.co.uk	docker-b r-5dcacaf 2848e_pi hole	OK (cache) SECURE	NXDOMAIN (0.5ms)	 Blacklist
2024-05-17 10:57:24	A	diesedomaingibtsnicht.co.uk	docker-b r-5dcacaf 2848e_pi hole	OK (answered by dns2.adguard.com#53) SECURE	NXDOMAIN (98.6ms)	 Blacklist
2024-05-17 10:57:24	A	diesedomaingibtsnicht.co.uk	docker-b r-5dcacaf 2848e_pi hole	OK (sent to dns2.adguard.com#53)	N/A	 Blacklist





**UND NUN ZUR
WERBUNG ;)**



Tracking (nicht Werbung!) gilt auch für MacOS, iOS, Android... 

BZW. ZUM TRACKING...



WHAT??

SCAN ME



SCAN ME



- Werbung / Tracking auf **Webseiten**
→ 100-1000+ “Partner” mit denen Daten geteilt werden!!!
- Zum Beispiel: Microsofts Datenmarktplatz Xandr mit 650.000 Kategorien, in die uns die Online-Werbeindustrie einsortiert
<https://netzpolitik.org/2023/microsofts-datenmarktplatz-xandr-das-sind-650-000-kategorien-in-die-uns-die-online-werbeindustrie-einsortiert/>
<https://media.ccc.de/v/37c3-11974-die-akte-xandr-ein-tiefer-blick-in-den-abgrund-der-datenindustrie>
- Euer **OS** (Windows, iOS, Android; aber nicht Linux) trackt euch!
- Euer **Browser** trackt euch!
- **Apps auf Smartphones** nutzen (un)absichtlich **SDKs** mit Telemetrie!



SCAN ME



<https://mastodon.gamedev.place/@shaneccelis/112466299054676076>



Informiert und freiwillig

In den Datenschutzbestimmungen [einer beliebten Wetterseite](#) beispielsweise kann ich mich über 1.400 Unternehmen informieren, die für die „Datenerhebung zur Auslieferung von nutzungsbasierter Online-Werbung“ zuständig sind. Ich kann auf die verlinkten Partner klicken und mir sogar durchlesen, was etwa Exit Bee Limited, VUUKLE DMCC oder 北京泛为信息科技有限公司 so tun. Bis ich damit fertig bin und top-informiert meine Einwilligung geben, ist der anstehende Gewitterschauer, für den ich mich interessiert habe, längst vorbeigezogen.

SCAN ME



“I HAVE READ AND AGREE TO THE TERMS” IS THE BIGGEST LIE ON THE WEB.

- Kennt ihr schon <https://tosdr.org/> ?
- Terms of Service Didn't Read

 PayPal Grade E

You waive your moral rights 

This service still tracks you even if you opted out from tracking 

This service holds onto content that you've deleted 

You must provide your identifiable information 

This service may keep personal data after a request for erasure for business interests or legal obligations 

[View All Points on Phoenix!](#)

[View Documents](#) [Visit Service](#)  Privacy Grade E

 Startpage Grade A

This service does not track you 

The service will resist legal requests for user information where reasonably possible 

IP addresses of website visitors are not tracked 

The cookies used by this service do not contain information that would personally identify you 

The cookies used by this service do not contain information that would personally identify you 

[View All Points on Phoenix!](#)

[View Documents](#) [Visit Service](#)  Privacy Grade A

 Facebook Grade E

Facebook stores your data whether you have an account or not. 

Your identity is used in ads that are shown to other users 

The service can read your private messages 

This service can view your browser history 

Deleted content is not really deleted 

[View All Points on Phoenix!](#)

[View Documents](#) [Visit Service](#)  Privacy Grade E

 Amazon Grade E

Third-party cookies are used for advertising 

Terms may be changed any time at their discretion, without notice to the user 

The service can delete your account without prior notice and without a reason 

This service tracks you on other websites 

You waive your right to a class action. 

[View All Points on Phoenix!](#)

[View Documents](#) [Visit Service](#)  Privacy Grade E

 Reddit Grade E

The service can read your private messages 

The service can delete specific content without prior notice and without a reason 

You sign away moral rights 

This service can share your personal information to third parties 

Tracking via third-party cookies for other purposes without your consent. 

[View All Points on Phoenix!](#)

[View Documents](#) [Visit Service](#)  Privacy Grade E

 Wikipedia Grade B

The service can delete your account without prior notice and without a reason 

The service may use tracking pixels, web beacons, browser fingerprinting, and/or device fingerprinting on users. 

Users have a reduced time period to take legal action against the service 

Your data may be processed and stored anywhere in the world 

You publish your contributions under free licenses 

[View Documents](#) [Visit Service](#)  Privacy Grade B



GOOGLE'S BROWSER HAS BECOME A THREAT TO USER PRIVACY (AND THE DEMOCRATIC PROCESS ITSELF)

- "So Google just switched off **third-party tracking** for 30 Million Chrome users - that's a good thing, right?" – "Well, child, get some snacks, make yourself comfortable and let me tell you the story of how this will affect you, me, and all of humanity..." [Distant thunder]

👉 <https://contrachrome.com>

- Ein hoch-interessanter und sehr wissenswerter Comic,
 - der erklärt wie Google **257 Milliarden US-\$ Umsatz**
 - **allein nur mit seinem kostenlosen Browser**
 - **und mit Werbung macht**   

SCAN ME



SCAN ME



MICROSOFT EDGE IS LEAKING THE SITES YOU VISIT TO BING

- Microsoft has a master filter ([available here](#)) for this creator follow feature, which includes domains like Pornhub where URLs are blocked from being sent to the Bing API site. It looks like, for every previously unchecked URL you visit, it passes it to [bingapis.com](#), which has **huge privacy implications**, especially when this **functionality is enabled by default**.
- Immerhin:
Anscheinend ist "Show suggestions to follow creators in Microsoft Edge" bei uns / in Deutschland / Europa (noch?) nicht aktiv...
- <https://www.theverge.com/2023/4/25/23697532/microsoft-edge-browser-url-leak-bing-privacy>



SCAN ME



BRANDNEU: FIREFOX TO COLLECT ANONYMIZED AND CATEGORIZED SEARCH DATA

- <https://blog.mozilla.org/en/products/firefox/firefox-search-update/>
- “Remember, you can always **opt out of sending any technical or usage data** to Firefox.” (Thunderbird auch!)

Firefox Data Collection and Use

We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information. [Privacy Notice](#)

- Allow Firefox to send technical and interaction data to Mozilla
[Learn more](#)
- Allow Firefox to make personalized extension recommendations
[Learn more](#)
- Allow Firefox to install and run studies [View Firefox studies](#)
- Allow Firefox to send backlogged crash reports on your behalf [Learn more](#)



SCAN ME



BSI NEWSLETTER:

- **Neue Malware kontrolliert Windows-Geräte**

Dass Cyberkriminelle ihre **Schadsoftware** hinter seriös wirkenden **Werbeanzeigen** verstecken, ist nichts Neues. In den vergangenen Monaten gab es bereits einige Berichte über **Malwaretising**, wobei bösartige Software über **Werbung** verbreitet wird. Nun haben Forscher von Elastic Security Labs entdeckt, dass ein neuer Fernzugriffstrojaner namens Lobshot über **Google Ads** verbreitet wurde.

- <https://www.csionline.com/de/a/neue-malware-kontrolliert-windows-geraete,3674581>



VIRENFUND AUF 65 CLIENTS

- Finale Rückmeldung der Forensik:

“Als verteilter Angriffsvektor ist hier vermutlich über Content Delivery Networks (CDN) ausgespielte **Werbung**, die im Browser angezeigt wird, relevant.”

Auswirkungen

- Zahlreiche Endgeräte mussten ersetzt bzw. gewiped und neu installiert werden.
- Betroffene müssen ihre Passwörter zurücksetzen:
 - auch private Accounts
 - Service User
 -  Offen: Alle Nutzer, die seit Oktober ein neues Gerät erhalten haben (ca. 1800)



**ICH, NACHDEM ICH AUSVERSEHEN
SPIEGEL.COM STATT SPIEGEL.DE EINGEGEBEN HABE.**

SCAN ME



imgflip.com

https://www.reddit.com/r/ich_iel/comments/1bg7vk7/ichiel/



ZUSAMMENFASSUNG: WHY???

- **Werbung!**
 - nervt!
 - macht Seiten unübersichtlich!
- **Tracking!! Telemetrie!**
- **Malware!!!**
- Schmuddelseiten... Social Media...
- **Ladezeiten!!!**



SCHREITEN WIR ZUR TAT...!

- 2014 Raspberry Pi(s) mit “pdsnd”
- 2015/2016 Windows komplett weg → Linux-only
- 2016 Werbeblocker mit “pdnsd”
- 2018/2019 Pi-hole statt pdnsd
- 2019/2020 VPS/Cloudserver für Nextcloud – plus WireGuard VPN + Pi-hole
- 2024 seid IHR dran! ;-)



WIE MACHE ICH DAS “ZUHAUSE”?

- **Browser-Extension?** uBlockOrigin oder AdBlockPlus...
 - auf jeden Fall AUCH nutzen für Cookies, JS, ...
 - Aber bitte nicht nur!!! Das ist “nur” eine weitere (sehr gute!) Abwehr!
- **Problem(e):**
 - Viele Browser: Firefox, Chrome, Iridium, Edge, Safari, Opera, ...
 - Nicht ein PC, sondern:
 - 1x Linux, 1x MacOS, 3x Windows, 1x Windows-VM, 5x iPhone, 3x iPad, 1x Switch, 2x PS4; 1x TV, 1x FireTV
 - D.h. **Das klappt da schon mal gar nicht auf allen Geräten (Mobile)! Ausserdem: Aufwand!!!**
:(
 - Ausserdem: **nicht nur der Browser...**
 - **auch/vor allem das OS**
 - + **Apps** (Smartphone) wegen SDKs, die wie die Weltmeister tracken! :(



EINE LÖSUNG FÜR ALLE GERÄTE

▪ **Pi-hole als networkweiter DNS-Server**

(und dabei unerwünschte Hostnames/Domains durch 0.0.0.0 ersetzen)

- Raspberry-Pi
oder Intel-NUC
oder auf eh 24x7 laufende Linux-Büxe
bzw. NAS mit Docker/Container-Support!
- Installation siehe Pi-hole-Seite...
- Am einfachsten mit Docker!
- Wichtig:

IPs anhand MAC-Adressen per DHCP statisch zuweisen!

Keine Private WLAN-Adresse!

Vor allem für “Pi-hole”,

eventuell auch für jedes Gerät für Nutzung von “Gruppen”

und “weiteren Filtermöglichkeiten je Device” (Eltern, Testing, Kinder, ...)



FINALE . . .

- Pi-Hole als DNS-Server für DHCP im Router eintragen – fertig.
 - **DHCP** = Zuweisung von IP-Adresse + DNS-Server 😊
Kann eh schon jeder/euer Router.
Ausnahme: Vodafone-Station!!!!!! 😞 → Router-Kaskade! Pi-hole als DHCP-Server!?
 - Alle Geräte im (W)LAN nutzen ab dem nächsten Reconnect den Pi-hole 😊
-
- **Lösung für zuhause – erl.**



ABER WAS IST MIT “UNTERWEGS”? MOBILE DATEN? FREMDE WLANS? AUSLAND?

- Idee “ehda-Prinzip”:
 - ich habe doch eh einen Cloudserver für meine Nextcloud (undso)...
 - Da packe ich doch einfach auch einen Pi-hole drauf
(und weil der von Haus aus kein TLS für die Admin-GUI kann,
brauche ich eh eine “Lösung” dafür: VPN!
Wireguard ist grade “modern” und im Linux-Kernel angekommen!)
- Und wenn ich nun eh schon einen VPN (damals spottbillige VM für <3€!!!) habe,
dann schaue ich doch mal, was ich mit so einem VPN noch so machen kann...



TODOS:

- **Pi-hole** analog auf Cloudserver (oder zuhause*) installieren
- **Wireguard** analog auf Cloudserver (oder zuhause*) installieren
 - Und für jeden Client, d.h. jedes Gerät **genaue eine WireGuard-Config generieren** (nicht pro User!!! WG macht Device-Auth und kein User-Auth!)
- Mit **Docker**(-Compose) “ruckzuck” fix&fertig!
- Notwendige Schritte:
 - WG: PEERDNS=auto (nutzt “nameserver 127.0.0.11” = Docker DNS Server)
 - OS:
 - `systemd-resolved.service disable/stop`
 - “nameserver 127.0.0.1” auf OS (plus weitere Upstream DNS für Fallback) = Pi-hole Docker Container

*= braucht entsprechenden Upload-Link und Port-Weiterleitungen! Engpass?!



WARUM SO WIE ES IST?

- Warum kein PiVPN oder WireHole oder Ähnliches/Anderes?
 - Ausrede:
weil das damals noch mit OpenVPN rumgeeiert ist (lahm!)
 - Wahrheit:
weil ich es nicht anders/besser wusste und quasi einen “Battle” mit einem Windows-Kollegen hatte, wer zuerst ein Wireguard-VPN aufgebaut bekommt
- Ausserdem: Vorteil von “meiner” getrennten Lösung:
Datenschutzkonform/mehr Privacy,
weil Pi-hole alle WG-Clients nur als Ganzes sieht
und kein Client direkt mit besuchten Domains verknüpft werden kann
(technisch: zwei Docker-Netzwerke, statt alles in einem Docker-Netzwerk)
(damit entfallen allerdings “weitere Filtermöglichkeiten je Device” (Eltern, Testing, Kinder, ...))



BONUS: TRUSTPID (EINGESTELLT)

- **TrustPID**
- Wer nicht von seinem **Mobilfunkprovider** umfassend getrackt werden möchte was das eigene **Surfverhalten** angeht, kann auf <https://trustpid.com/> seine "Einstellungen verwalten" und dem **dauerhaft widersprechen**. In der Hoffnung, dass das auch wirklich Beachtung findet.
- **Oder ein VPN nutzen:** Dann können sie einen nicht mehr tracken, weil man dann für sie technisch nicht mehr im "Mobilfunk" ist 
- <https://www.dr-datenschutz.de/trustpid-die-neue-datenkrake-von-vodafone-und-telekom/>

SCAN ME



Ihr TrustPid-Dienst ist inaktiv.

Sie sind in der Sperrliste eingetragen.

Um den TrustPid-Dienst zu nutzen, müssen Sie sich wieder aus der Sperrliste austragen. Klicken Sie hierzu bitte auf die Schaltfläche 'Sperrlisten-Eintrag entfernen'.

[Sperrlisten-Eintrag Entfernen](#)

SCAN ME



BONUS: UTIQ (NEU)

- **Neue Tracking-Firma Utiq: Wie Telekom, o2 und Vodafone im Datengeschäft mitmischen**
 - Die großen Telekommunikationsanbieter **wollen das Online-Verhalten von Millionen Mobilfunknutzer:innen auswerten** und so dem **Silicon Valley bei der Online-Werbung das Wasser abgraben.** ...
 - Davor warnt der digitalpolitische Verein D64 ... bezeichnet ... als „**Big Brother made in Germany**“.
 - Blanker Hohn:
„Utiq ist der authentische Einwilligungs-Service, der verantwortungsvolles digitales Marketing ermöglicht.“
 - Der Gründung von Utiq war 2022 eine **längere Testphase unter dem Namen TrustPid** vorausgegangen.
-
- <https://netzpolitik.org/2024/neue-tracking-firma-utiq-wie-telekom-o2-und-vodafone-im-datengeschaeft-mitmischen/>



SCAN ME



- Widersprechen: <https://consenthub.utiq.com/> - oder VPN nutzen!

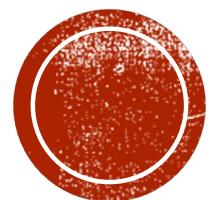


Zugang fehlgeschlagen!

Sie können nur zugreifen, wenn:

- Sie Kunde eines der teilnehmenden Netzbetreiber sind (derzeit Movistar, Orange, Jazztel und Simyo in Spanien; Orange, Bouygues Telecom und SFR in Frankreich und Deutsche Telekom, Vodafone, Congstar, Fraenk und O2 in Deutschland).
- Sie Ihre Mobilfunkverbindung nutzen, d.h. Ihr WLAN ist ausgeschaltet.
- Sie keine Werbeblocker oder VPN verwenden, da diese die Verbindung stören können.





SETUP...



TECHNISCHES SETUP: SERVER

- **Hardware-Anforderung**

- Klein(st)er Cloudserver bei renommierten deutschem Hoster:
1 CPU und 2 GB RAM sind mehr als ausreichend für eine ganze Familie
Kosten ca. 5€ monatlich
- Alternativ: zuhause auf Linux-Server/Desktop oder “Raspberry Pi”
keine zusätzlichen Kosten, wenn eh schon 24x7-Betrieb;
ansonsten nur wenige Euro Stromkosten jährlich

- **Benötigte Docker Container**

- VPN: ghcr.io/linuxserver/wireguard
- Tracking- und Werberblocker: [pihole/pihole](https://ghcr.io/pihole/pihole)

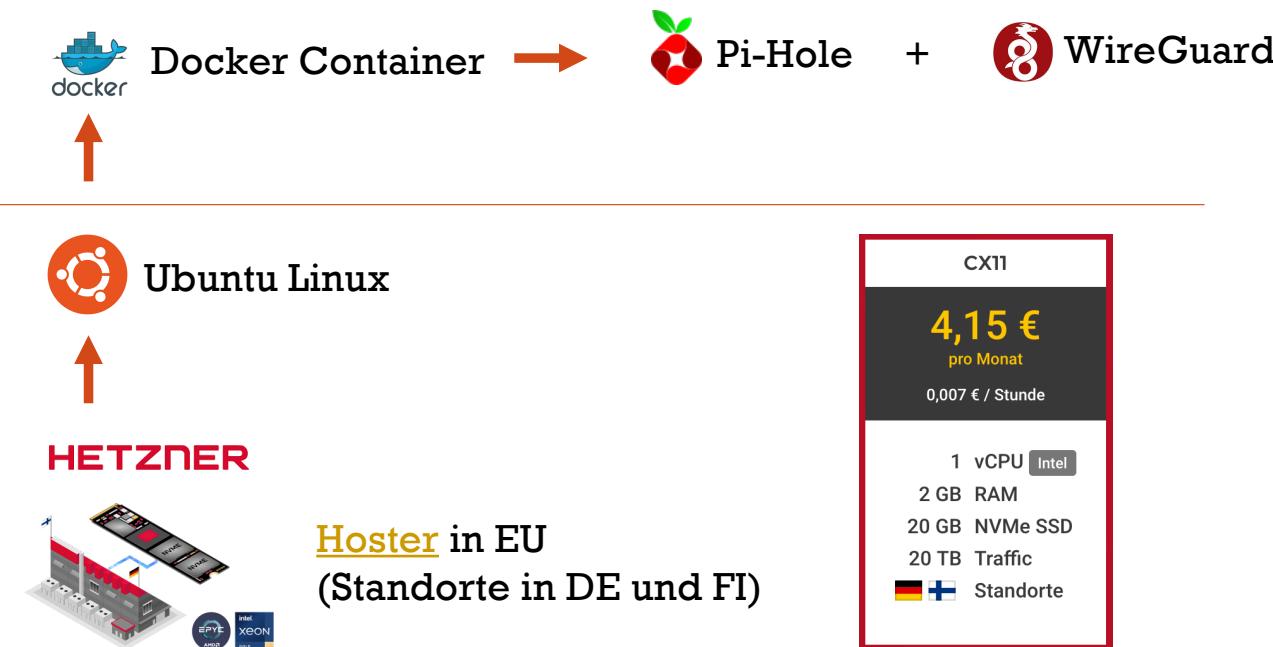


TECHNISCHES SETUP: CLIENT(S)

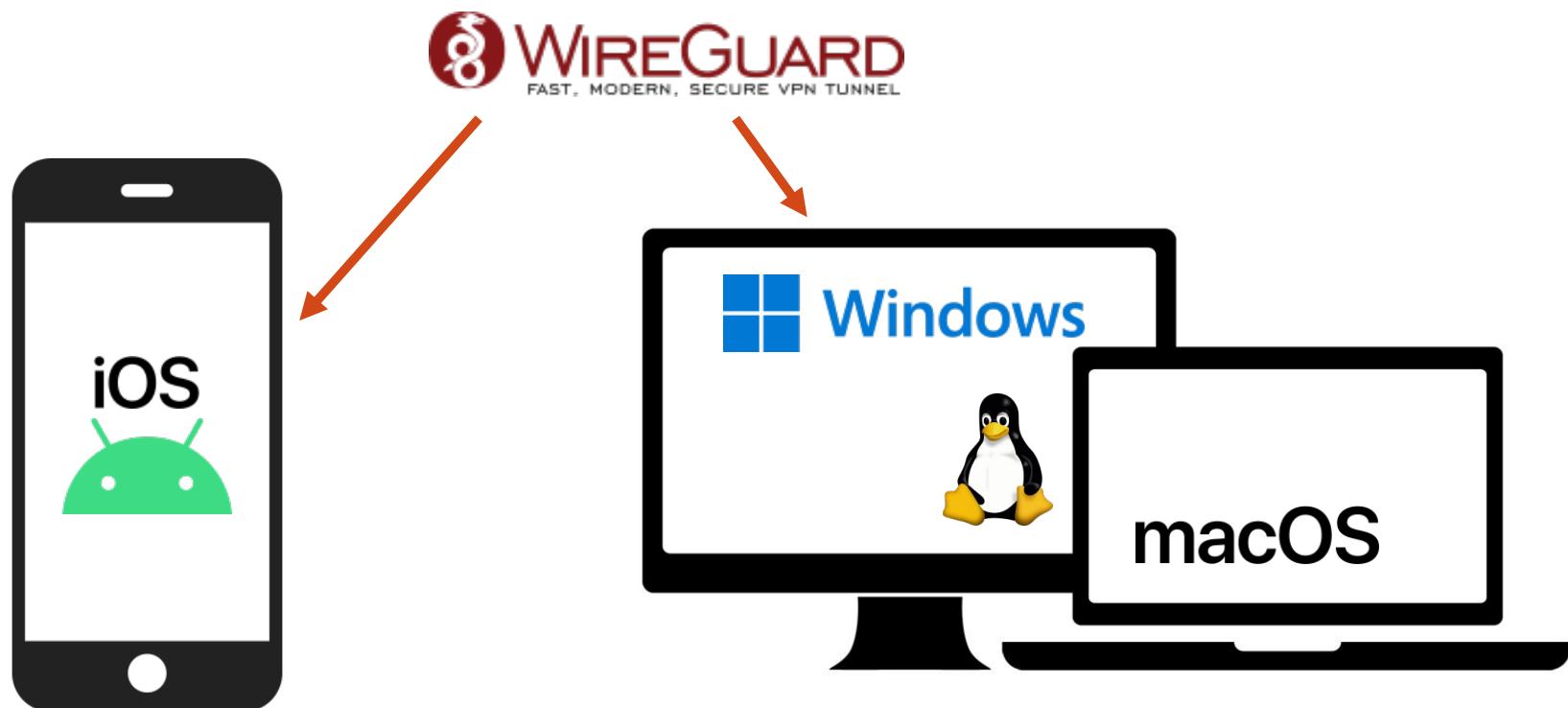
- Keine App für Pi-Hole notwendig – funktioniert mit jedem Gerät!
- Kostenlose WireGuard (VPN) App für
 - Smartphones (iOS, Android)
 - PCs (Windows, Linux, MacOS)



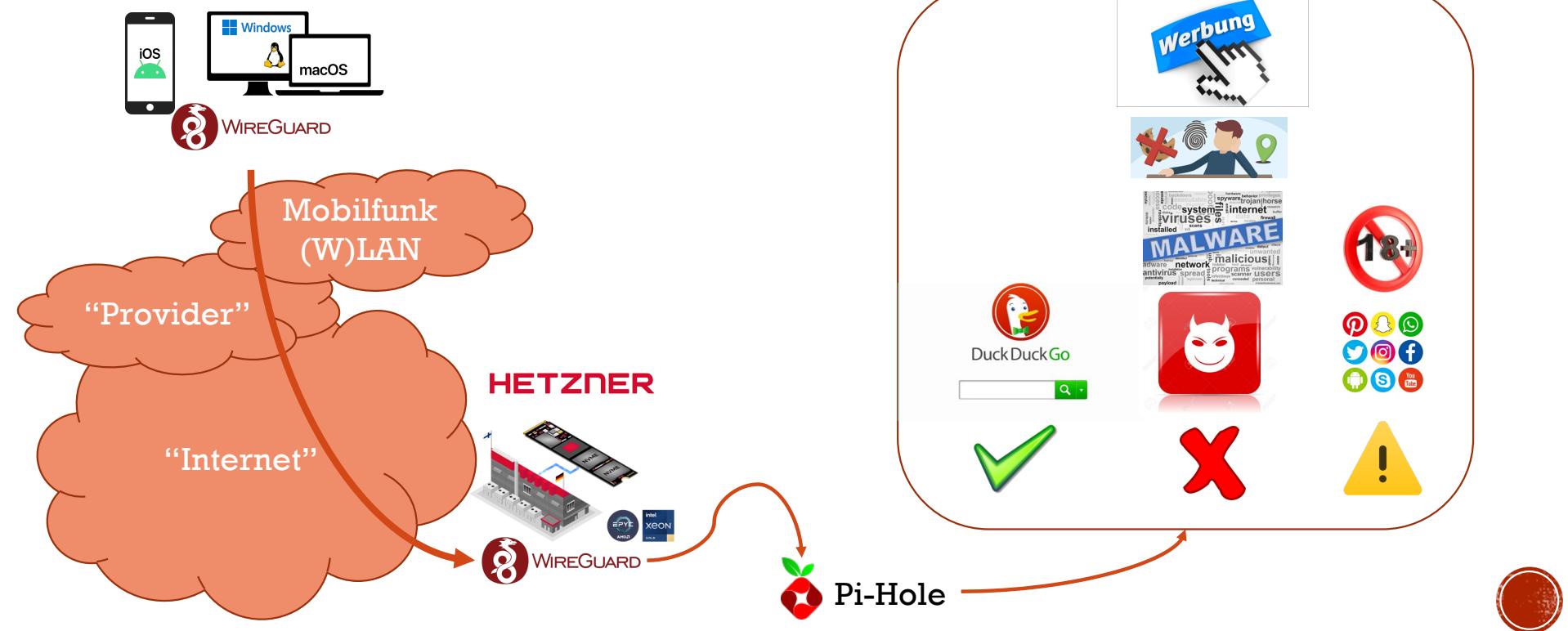
SERVER: HARDWARE- UND SOFTWARE



CLIENT: GERÄTE UND APPS



UND ACTION!



“ANBIETER”-VERGLEICH



- Zum Beispiel “NordVPN”:
6 Geräte (PC, Laptop, Smartphone – je Familienmitglied!?)
4€ / Monat im Jahresabo
3€ / Monat im Zweijahresabo
- DYI:
∞ Geräte für 5€ / Monat (DE/FI/US)
mit 20 Tbyte Traffic monatl. und 1 Gbit/s Down/Up
(aktuell: max. 7-10 gleichzeitig aktiv von 18, kleinste VM (1 CPU, 2 GB RAM) langweilt sich! (und macht daher noch weitere \$Dinge))
- Vertrauen?



AUSWIRKUNGEN

- **Positiv:**

- Ca. 20-30% Block-Rate – das ist kein Wettbewerb “wer mehr blockt”!
- Ca. 30-50% Cache-Rate – das kann man tweaken (TTL++)

- **Negativ:**

- “Overblocking” – Irgendwas funktioniert nicht!
- (automatische) Updates gehen fast nie schief...
→ Monitoring/Alerting! (mit GitHub Actions ;-)



GUTE BLOCKLISTEN (FÜR DEN START)

- StevenBlack* (wird bereits mitgeliefert)
- blocklistproject* ("Erwachsenenseiten")
- lightswitch05* (Tracking)
- Hagezi* (bei AdBlock Plus und NextDNS? aktiv genutzt!)
- RPiList* (diverse)
- oids.nl* (meta-liste)
- crazy-max (Windows-Spy-Blocker)
- Liamengland1* (Apple, Microsoft)

* = da habe ich selber schon contributed bzw. bin Sponsor

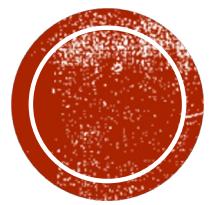


EXPERTEN-TIPP



- iPhone App-Datenschutzbericht! (Android?) → JSON





**DANKE UND VIEL SPASS
BEIM SELBERMACHEN!**

 [@abimelechbeutelbilch@fulda.social](https://abimelechbeutelbilch@fulda.social)
 github.com/thomasmerz/

SCAN ME



SCAN ME



NOCH EIN PAAR LINKS

- <https://thomasmerz.github.io/pihole-wireguard-knowhow/>
- https://thomasmerz.github.io/dnspingtest_rrd_ka/
- <https://thomasmerz.github.io/upptime/>

SCAN ME



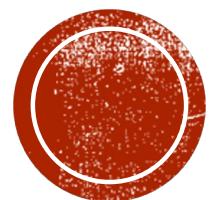
SCAN ME



SCAN ME

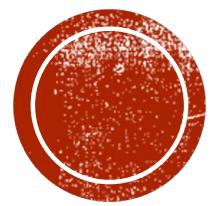






NERD-TEIL...





IPHONE DATENSCHUTZBERICHT IM DETAIL



YOU CAN CHECK THIS OUT!

- Auf deinem iPhone:
 - Einstellungen / Datenschutz / App-Datenschutzbericht “teilen”
(da es sich u.U. um höchst sensible und um deine personenbezogene Daten handelt: z.B. auf deiner eigenen Nextcloud – E-Mail ohne Verschlüsselung ist dafür “nicht geeignet”...)
 - Auswertung(en):
Welche Domains haben meine Apps auf meinem iPhone in den letzten x Tagen aufgerufen?
Wann zuerst/zuletzt?
Wie oft?



HARDCORE

SCAN ME



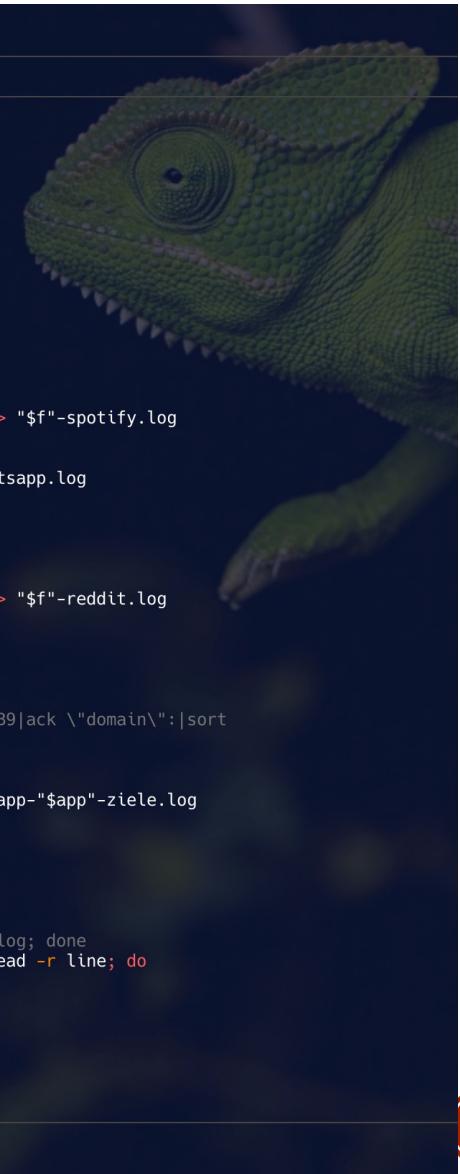
<https://gist.github.com/thomasmerz/5e643732bd28ee8b58c59cc32b3ccfd5>

```
thomas@merz-nimbus:~/Documents/iphone-privacy [0/5474]
00:10 $ bat auswertungen.sh

File: auswertungen.sh

1 #!/bin/bash
2
3 # ---
4 # wertet den App-Privacy-Report eines iPhones aus:
5 # Einstellungen / Datenschutz / App-Datenschutzbericht
6 # ---
7
8 for f in App_Privacy_Report_*ndjson; do
9
10   [ "$1" != "" ] && f="$1" # do not loop if filename is given
11
12   jq < "$f" | ack \"domain\": > "$f"-alle-domains.log
13   #jq < "$f" [ .domain, . ] > "$f"-domains_jq.log
14
15   # Auswertung Spotify:
16   jq < "$f" | ack \"domain\": -A9|grep com.spotify.client -B9|ack \"domain\":|sort > "$f"-spotify.log
17
18   # Auswertung WhatsApp:
19   jq < "$f" | ack \"domain\": -A9|grep WhatsApp -B9|ack \"domain\":|sort > "$f"-whatsapp.log
20
21   # Auswertung Google DNS:
22   jq < "$f" | ack "domain.*8\.8\. -A9 > "$f"-google-dns.log
23
24   # Auswertung Reddit:
25   jq < "$f" | ack \"domain\": -A9|grep com.spotify.client -B9|ack \"domain\":|sort > "$f"-reddit.log
26
27
28   # Alle Apps...
29   jq < "$f" | ack \"bundleID\": | sort -u > "$f"-alle-apps.log
30   # ... alle Ziele:
31   #for app in $(jq < "$f" | ack "^\\"bundleID\" | sort -u | cut -d "\\" -f4); do
32   #  echo Connections from "$app" to: jq < "$f" | ack \"domain\": -A9|grep "$app" -B9|ack \"domain\":|sort
33   #done > "$f"-alle-ziele.log
34   for app in $(jq < "$f" | ack \"bundleID\": | sort -u | cut -d "\\" -f4); do
35     echo Connections from "$app" to:
36     jq < "$f" | ack \"domain\": -A9|grep "$app" -B9|ack \"domain\":|sort | tee "$f"-app-"$app"-ziele.log
37   done > "$f"-alle-ziele-je-app.log
38
39   # got this file by:
40   # cd ~/dev/docker-pi-hole/etc-pihole
41   # ./pihole_adlist_tool -d 1 -t 10 -u -a -s hits DESC
42   # search for "Top blocked adlist domains" and copy domain|hits table
43   #for d in $(grep -E "\.com|\\.net" auswertungen.sh.top-10-1d); do ack "$d" "$f"-*.log; done
44   grep -E "\.com|\\.net" auswertungen.sh.top-10-1d | awk '{print $1}' | while IFS= read -r line; do
45     grep "$line" "$f"-app-* ziele.log
46   done
47
48   [ "$1" != "" ] && break # do not loop if filename is given
49
50 done
```

```
thomas@merz-nimbus:~/Documents/iphone-privacy [0/5474]
00:10 $
```



TOP-1: APP-MEASUREMENT.COM*

App_Privacy_Report_v4_2022-02-09T21_49_39.ndjson

Start: 2022-01-31T23:51:01.480+01:00 --- Ende: 2022-02-09T21:49:37.542+01:00

```
app-com.bose.boseconnect-ziele.log: "domain": "app-measurement.com",
app-com.google.ios.youtube-ziele.log: "domain": "app-measurement.com",
app-com.rebuy.App-ziele.log: "domain": "app-measurement.com",
app-com.reddit.Reddit-ziele.log: "domain": "app-measurement.com",
app-com.willenapps.cloudplayer-ziele.log: "domain": "app-measurement.com",
app-de.materna.bbk.mobile-ziele.log: "domain": "app-measurement.com",
app-overlook.fing-ziele.log: "domain": "app-measurement.com",
```

*Tops anhand Pi-hole “Top Blocked Domains”



TOP-4: FIREBASELOGGING-PA.GOOGLEAPIS.COM*

App_Privacy_Report_v4_2022-02-09T21_49_39.ndjson

Start: 2022-01-31T23:51:01.480+01:00 --- Ende: 2022-02-09T21:49:37.542+01:00

```
app-com.bose.boseconnect-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-com.crystlnix.ServerAuditor-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-com.ebay.iphone-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-com.ebaykleinanzeigen.ebc-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-com.github.stormbreaker.prod-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-com.ookla.speedtest-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-com.rebuy.App-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-com.reddit.Reddit-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-com.spotify.client-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-com.willenapps.cloudplayer-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-de.comdirect.phototan-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-de.materna.bbk.mobile-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-it.twsweb.Nextcloud-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-net.faz.FAZ-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
app-overlook.fing-ziele.log: "domain": "firebaselogging-pa.googleapis.com",
```



UND NATÜRLICH: FACEBOOK

App_Privacy_Report_v4_2022-02-09T21_49_39.ndjson

Start: 2022-01-31T23:51:01.480+01:00 --- Ende: 2022-02-09T21:49:37.542+01:00

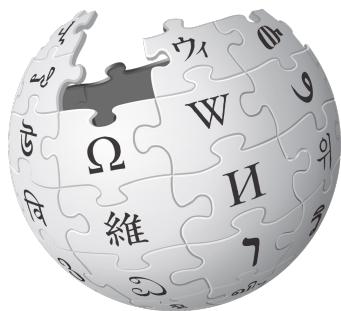
app-com.bose.**boseconnect**-ziele.log: "domain": "graph.facebook.com",
app-com.rebuy.App-ziele.log: "domain": "graph.facebook.com",
app-overlook.**fing**-ziele.log: "domain": "graph.facebook.com",



ABER AUCH ERFREULICHES ☺

- **Wikipedia-App**

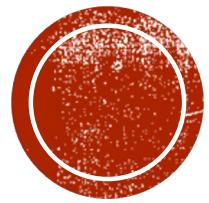
verbindet sich ausschliesslich mit wikipedia/wikimedia-Domains



URSACHE?

- Nicht zwangweise Tracking durch App
 - Sondern durch eingebundene Bibliotheken (SDK)
 - Teils auch “renommierte” Apps davon (un)wissenlich betroffen
 - D.h. Tracking durch unbeteiligte ”Dritte”!
-
- Das untersuchte iPhone ist nur bei Top-1 und Top-4 dabei, d.h. es werden andere Geräte wohl noch viel mehr getrackt!
→ Top-2 und Top-3 und Top-5 usw.





**DANKE UND VIEL SPASS
BEIM SELBERMACHEN!**

 [@abimelechbeutelbilch@fulda.social](https://abimelechbeutelbilch@fulda.social)
 github.com/thomasmerz/

SCAN ME



SCAN ME

