PRIVACY TO GO

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

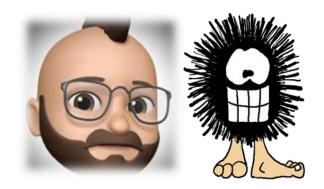
Workshop bei Aramido, 26.09.2024

@@abimelechbeutelbilch@fulda.social

github.com/thomasmerz/



WER BIN ICH?



- Linux seit 1994: Irix, Solaris, SUSE Angewandte Informatik
- WEB.DE (SUSE; DNS, Webserver) 2J
- dm-drogeriemarkt / dmTECH
 - zOS und DB2 for SAP ~10J
 - SLES-for-SAP (HANA) + RHEL;
 Lifecycle/Config/Patch-Management, IT-Sicherheit/Security ~10J
- Privacy-to-go seit 2019/2020
- Motördad und Metalhead + Radfahrer und Carsharing
- "Speedcubing" (3, 5, 7, ... 13)
- OpenSource ♥ (EFF, FSF)
- 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

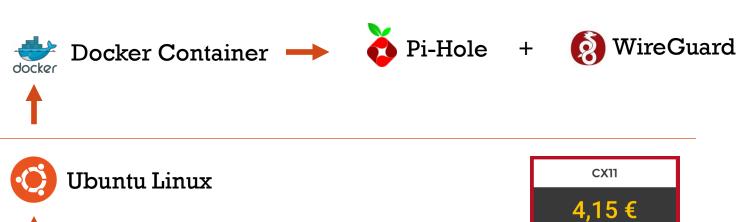




30-45 Minuten WAS und WARUM

Rest WIE

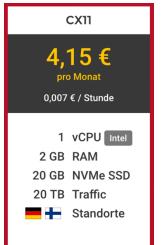
SERVER: HARDWARE- UND SOFTWARE





HETZNER

Hoster mit Standorten in DE und FI - und US



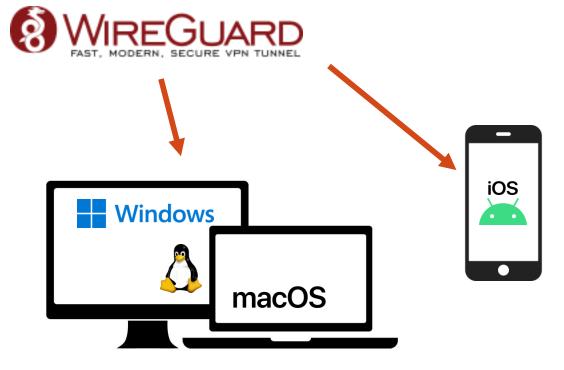


CLIENT: GERÄTE UND APPS

• <u>Keine App</u> für Pi-Hole notwendig – funktioniert mit jedem Gerät!

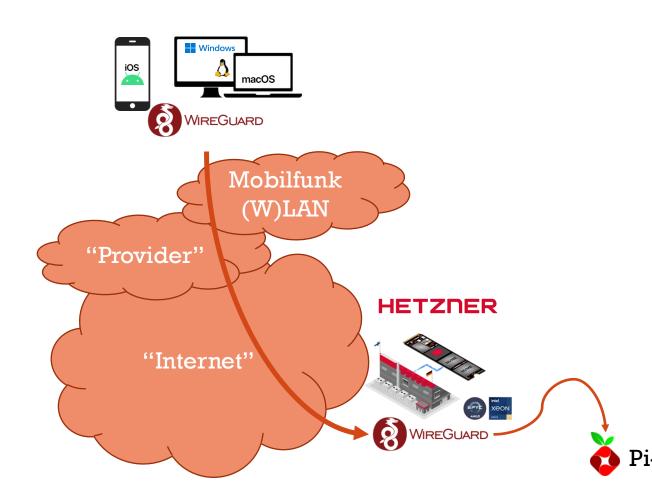


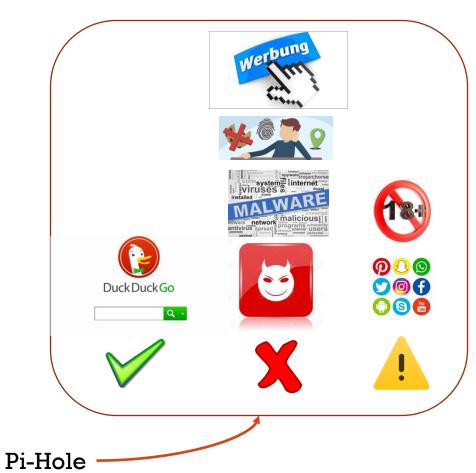
- Kostenlose WireGuard (VPN) App für
 - Smartphones (iOS, Android)
 - PCs (Windows, Linux, MacOS)





UND ACTION!



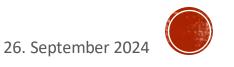




"ANBIETER"-VERGLEICH



- 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?



TECHNISCHES SETUP: SERVER

Hardware-Anforderung

- Klein(st)er Cloudserver bei einem deutschem/europäischen 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: http://nedacc.de//2023/021/home-uber-den-ment/desktop

Benötigte Docker Container

- VPN: ghcr.io/linuxserver/wireguard
- Tracking- und Werbeblocker: pihole/pihole





WAS IST PIHOLE?



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





EMPFEHLUNG AUS DEM KUKETZ-BLOG

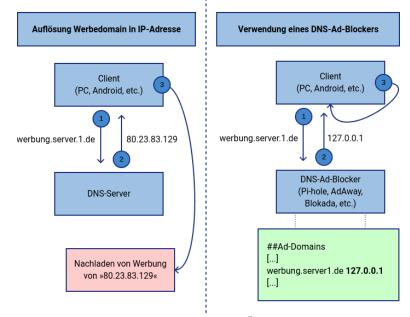
IT-SICHERHEIT | DATENSCHUTZ | HACKING

- https://www.kuketz-blog.de/empfehlungsecke/#adblocker
- Ein Werbe- 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 <u>Tracking-Firmen</u>, 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] \rightarrow z.B. Pi-hole
- Kontrollfetischisten [Profis] → IPFire



WAS IST WIREGUARD?



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



WAS IST EIN "VPN"?

- "Virtual Private Network
 - (<u>deutsch</u> ,,<u>virtuelles</u> <u>privates</u> <u>Netzwerk</u>"; *kurz*: **VPN**)
 - bezeichnet eine Netzwerkverbindung, die von Unbeteiligten nicht einsehbar ist."







EMPFEHLUNG AUS DEM KUKETZ-BLOG

IT-SICHERHEIT | DATENSCHUTZ | HACKING

- https://www.kuketz-blog.de/empfehlungsecke/#vpn-anbieter
- Ein VPN ist <u>nicht</u> 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 <u>Man-in-the-Middle-Angriffen</u>
- 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







SURFEN/COMPUTERNUTZUNG OHNE BELÄSTIGUNG, ÜBERWACHUNG U. GEFÄHRDUNG

- Werbung / Advertising
- Tracking + Telemetrie
 - >1000 Firmen (nicht nur GAFAM ("Big Tech")) kennen dich besser als du dich selber kennst und deine Familie und Freunde dich kennen!!!
- Malware / Malvertising
- 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)





"PRIVACY"

- Privatsphäre bezeichnet den nichtöffentlichen Bereich, in dem ein Mensch, unbehelligt von äußeren Einflüssen, sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt. 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 omnipräsenten Überwachungstechnologien zu entgehen.
- Aber auch <u>Wirtschaft</u> und <u>Werbung</u> stellen mit Scoring- (<u>Schufa</u>), <u>Marktforschungs</u>-Maßnahmen und Konsumenten-Profiling für Kritiker eine zunehmende Bedrohung von Privatsphäre dar.



PRIVACY / DATENSCHUTZ

- Schutz personenbezogener Daten
- Unverletzlichkeit des Post- und Fernmeldegeheimnisses
- Unverletzlichkeit der Wohnung

Datenschutz

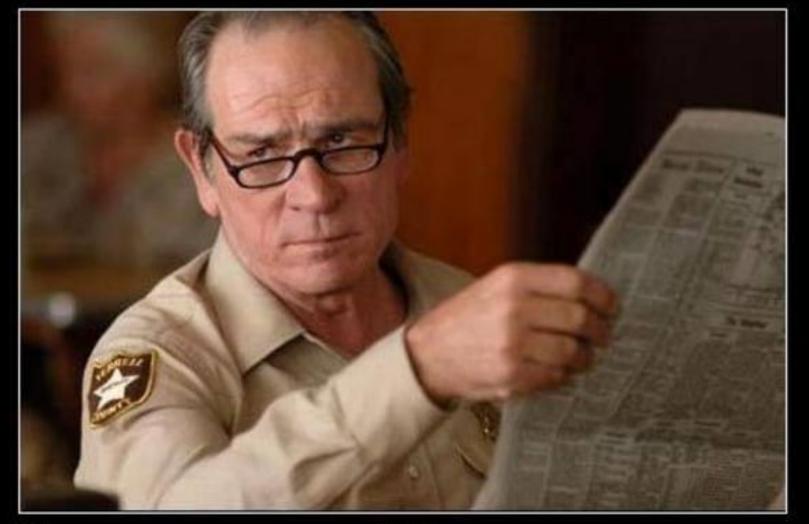
- Schutz vor missbräuchlicher Datenverarbeitung
- Schutz des Rechts auf informationelle Selbstbestimmung
- Schutz des Persönlichkeitsrechts bei der Datenverarbeitung
- und auch Schutz der Privatsphäre
- jeder Mensch darf grundsätzlich selbst darüber entscheiden, wem wann welche "seiner" persönlichen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



BEDEUTUNG DES DATENSCHUTZES

- Seit der Entwicklung der Digitaltechnik stetig gestiegen
- weil Datenhaltung, Datenverarbeitung, Datenerfassung, Datenweitergabe und Datenanalyse immer einfacher werden und industrielle Ausmaße angenommen haben
- Technische Entwicklungen ... schaffen neue Möglichkeiten zur Datenerfassung.
- Dieser Entwicklung steht eine gewisse Gleichgültigkeit großer Teile der Bevölkerung gegenüber, in deren Augen der Datenschutz keine oder nur geringe praktische Bedeutung hat. ☺

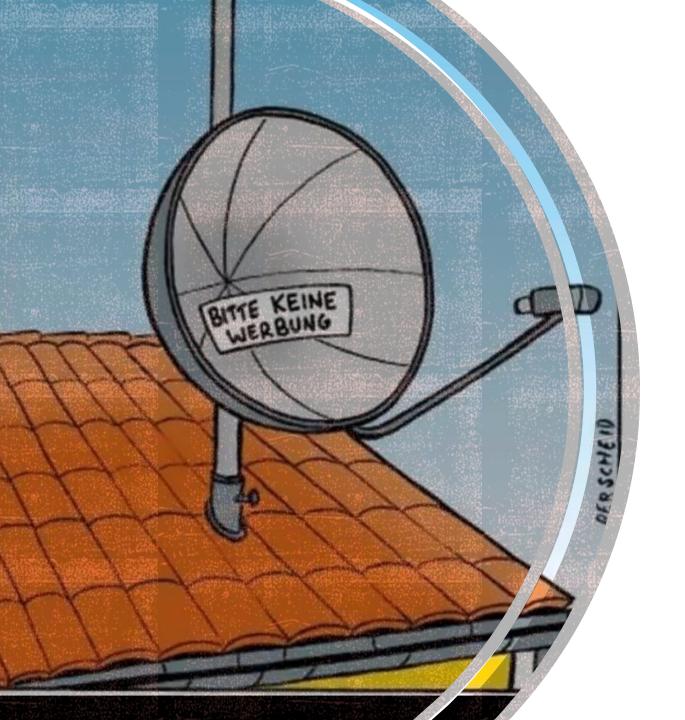




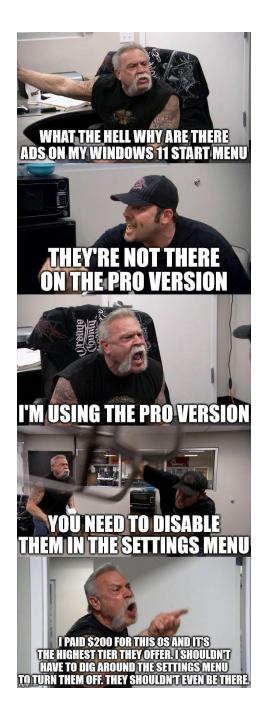
IMPLIED FACEPALM

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





UND MUN ZUR WERBUNG;





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



WERBUNG IST NICHT NUR NERVIG

- "Sie verbraucht auch eine Menge Daten und verlangsamt damit Webseiten und Apps. Werbeplätze werden in automatischen Auktionen an die Meistbietenden verkauft. Dazu werden verschiedenste Daten über dich gesammelt und verkauft. Außerdem gibt es immer wieder Fälle, in denen Werbung für eine Anwendung gar nicht vom Anbieter stammt sondern von Angreifer*innen, die dich zu Seiten mit Trojanern locken. Oder es wird sogar in der Werbung selbst Schadcode auf seriösen Seiten ausgeliefert."
- https://infosec.exchange/@seism0saurus/113139921880991064









WHAT??

- 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, MacOS, iOS, Android; aber nicht Linux) trackt euch!
- Euer Browser trackt euch!
- Apps auf Smartphones nutzen (un)absichtlich SDKs mit Telemetrie!





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 topinformiert meine Einwilligung geben, ist der anstehende Gewitterschauer, für den ich mich interessiert habe, längst vorbeigezogen.

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 DE GB FR











- 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





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 reprovide and improve Firefox for everyone. We always ask permiss receiving personal information. Privacy Notice					
Allow Firefox to send technical and interaction data to Mozilla					
<u>Learn more</u>					
Allow Firefox to make personalized extension recommendations	<u>Learn</u> <u>more</u>				
Allow Firefox to install and run studies View Firefox studies	<u>5</u>				
\square Allow Firefox to send ba <u>c</u> klogged crash reports on your behalf	f <u>Learn</u>				





BSI NEWSLETTER:



Neue <u>Malware</u> 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 <u>Ads</u>** verbreitet wurde.

https://www.csoonline.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

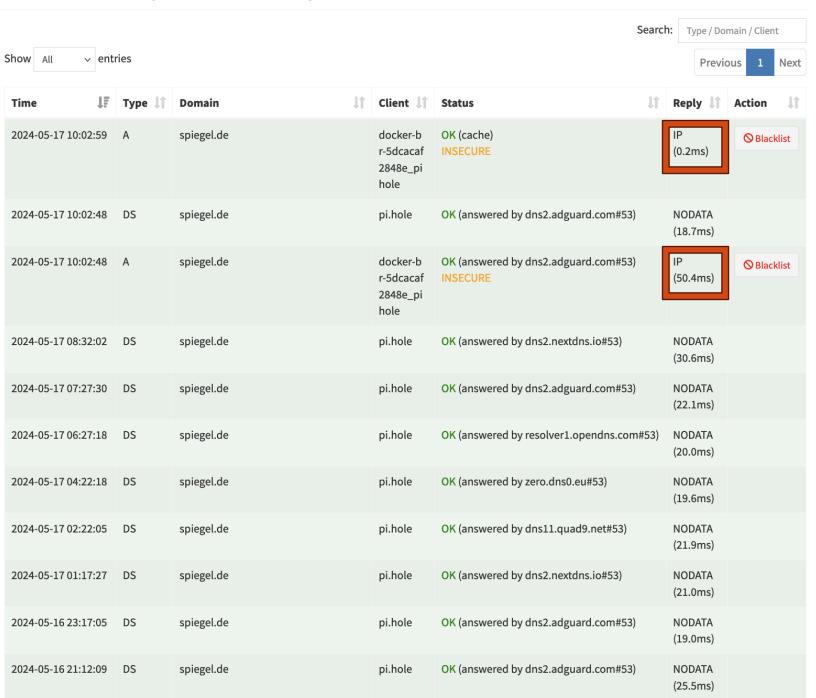
- Zahlreiche Endgeräte mussten ersetzt bzw. gewiped und neu installiert werden.
- Betroffene müssen ihre Passwörter zurücksetzen:
 - auch private Accounts
 - Service User
 - o A Offen: Alle Nutzer, die seit Oktober ein neues Gerät erhalten haben (ca. 1800)



LADEZEITEN / KNOFFHOFF: DNS

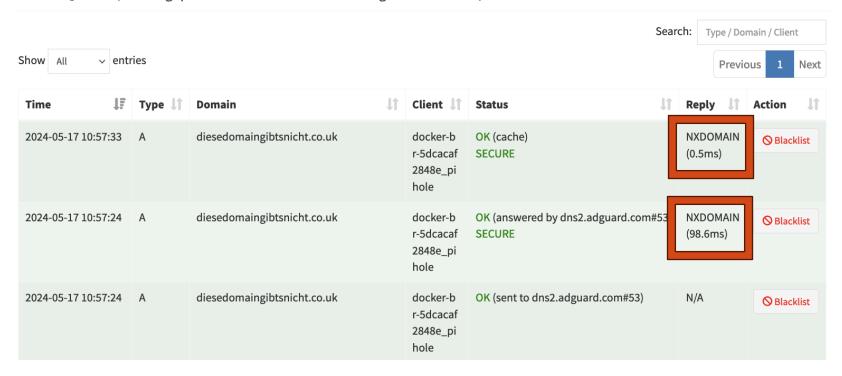
- Ähnlich wie **Telefonbuch**: spiegel.de has address 128.65.210.8
- Browser / irgendein Programm
- DNS-Resolver im OS (Windows, MacOS, Linux, Android, iOS)
- Router
- DNS-Resolver vom Provider (wenn man Kunde bei Vodafone ist und die VF-Station ohne eigenen Router nutzt!) bzw. "andere"
- Authoritative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







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





ZUSAMMENFASSUNG: WHY???

- Werbung!
 - nervt!
 - macht Seiten unübersichtlich!
- Tracking!! <u>Telemetrie</u>!
 - aufgrund der Nutzungsdaten können Rückschlüsse über den Benutzer gezogen warden
 - im Kontext des Datenschutz problematisch!
- Malware!!!
- Schmuddelseiten... Social Media...
- Ladezeiten!!!



WIE MACHE ICH DAS "ZUHAUSE"?

- **Browser-Extension**? uBlockOrigin oder AdBlockPlus...
 - Bitte nicht nur!!! Das ist "nur" eine weitere (sehr gute!) Abwehr!
 - Aber auf jeden Fall AUCH nutzen für Cookies, JS, ...
- Problem(e):
 - Viele Browser: Firefox, Chrome, Iridium, Edge, Safari, Opera, ...
 - Nicht nur 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 netzwerkweiter DNS-Server

(und dabei unerwünschte Hostnames/Domains durch 0.0.0.0 ersetzen)

- Am einfachsten mit Docker!
- Tipp:

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 <u>zuhause</u> erl.



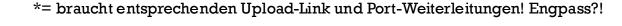
ABER WAS IST MIT "UNTERWEGS"? MOBILE DATEN? FREMDE WLANS? AUSLAND?

- Idee "ehda-Prinzip":
 - ich habe doch eh einen Cloudserver für meine Nextcloud (und andere \$Dinge)...
 - 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 f
 ür <3€!!!) habe, dann schaue ich doch mal, was ich mit so einem VPN noch so machen kann...



HOWTO:

- 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 Tweaks:
 - 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





VPN-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-neuedatenkrake-von-vodafone-und-telekom/







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





VPN-BONUS: UTIQ (NEU)

- Neue Tracking-Firma Utiq: Wie Telekom, o2 und Vodafone im <u>Datengeschäft</u> 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 <u>"Big Brother made in Germany"</u>.
- 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/







BSI WARNT VOR UTIQ

- "Schützen Sie Ihre digitale Privatsphäre"
- Aktuell steht der Vorwurf im Raum, dass Verbraucherinnen und Verbraucher der Online-Werbeplattform Utiq unverhältnismäßig getrackt werden. Die Plattform Utiq wurde von europäischen Netzbetreibern gegründet, um den Medien und der Anzeigenkundschaft eine EU-datenschutzkonforme Alternative zu den US-Werbenetzwerken anzubieten. Zu ihren Medienpartnern zählen etwa die FAZ, die Süddeutsche Zeitung oder das Handelsblatt.
- BSI Newsletter SICHER INFORMIERT vom 23.05.2024
- Widersprechen: https://consenthub.utiq.com/ oder VPN nutzen!

Zugang fehlgeschlagen!

Sie können nur zugreifen, wenn:

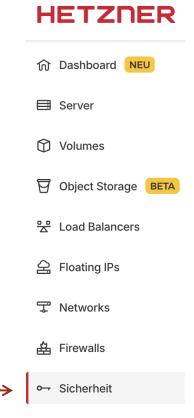
- Sie Kunde eines der teilnehmenden Netzbetreiber sind (derzeit Movistar, Orange, Jazztel und Simyo in Spanien; Orange, Bouygues Telecom und SFR in Frankreich und Deutsche Telekom, Vodafone, Congstar, Fraenk und O2 in Deutschland).
- Sie Ihre Mobilfunkverbindung nutzen, d.h. Ihr WLAN ist ausgeschaltet.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

LOS CEHTS!

CLOUDSERVER ANLEGEN:



- Ubuntu 22.04 LTS / 24.04 LTS
- Shared vCPU (Arm64) CAX11
- IPv4, IPv6, Privates Netzwerk (10.1.0.0/16)
- SSH-Key ("ssh-keygen -t ed25519" + vorher hochladen!)
- Root-PW bei "Rescue" zurücksetzen bringt nix, weil "PermitRootLogin yes" fehlt (24.04) bzw. prohibit-password (22.04)
- Kein: Volume, Firewall, Backup, Platzierungsgruppe, Label, Cloud Config.
- Beliebiger Name → 4,51€ / Monat





LIVE S WIREGUARD

- Klein(st)e VM (mit ssh-Key für root!) rebuild!
- command ssh root@168.119.104.123 -i /Users/thomas.merz/.ssh/id_ed25519 (ssh root@168.119.104.123 -i ~/.ssh/id_ed25519_2018_10)
- apt update && apt upgrade -y && apt install -y docker.io docker-compose(-v2)
- mkdir wireguard && cd wireguard
- docker-compose.yaml (copy&paste + anpassen!):
 - https://github.com/linuxserver/docker-wireguard?tab=readme-ov-file#docker-compose-recommended-click-here-for-more-info
 - docker-compose up -d && docker exec -it wireguard /app/show-peer 1 → QR-Code
 - cat config/peerl/peerl.conf → Config als Text
 - Check: https://myip.ms/ (oder: curl wtfismyip.com/text)
 - Check: docker exec -it wireguard wg

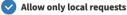


LIVE © PI-HOLE

- mkdir **pihole** && cd pihole
- docker-compose.yaml (copy&paste + anpassen!):
 - https://github.com/pi-hole/docker-pi-hole?tab=readme-ov-file#quick-start
 - docker-compose pull
 - systemctl stop systemd-resolved.service && systemctl disable systemd-resolved.service
 - vim /etc/resolv.conf → nameserver 127.0.0.1
 - docker-compose up -d
 - Check: http://168.119.104.123/admin/login.php
 - Check mit VPN: http://10.1.0.1/admin/login.php
 - Passwort: docker logs pihole 2>&1 | grep "Assigning random password"
 - GANZ WICHTIG: http://10.1.0.1/admin/settings.php?tab=dns
 - vim etc-pihole/setupVars.conf → IPV4_ADDRESS=0.0.0.0
 - docker restart wireguard pihole
 - Check: dig wetrack.it +short; dig wetrack.it +short @9.9.9.9

Interface settings

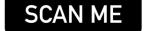
Recommended setting



Allows only queries from devices that are at most one hop away (local devices)











NACHARBEITEN!

sshd

- sed -i -e '/^PasswordAuthentication/s/^.*\$/PasswordAuthentication no/' /etc/ssh/sshd_config
- sed -i -e '/^#MaxAuthTries/s/^.*\$/MaxAuthTries 2/' /etc/ssh/sshd_config
- sed -i -e '/^#Port 22/s/^.*\$/Port 65432/g' /etc/ssh/sshd_config

• OS:

- snap install canonical-livepatch && canonical-livepatch enable xyz123
- pro attach abcd4567
- Cronjobs für Auto-Patching oder Watchtower oder ...
 - docker-wireguard-update.sh https://gist.github.com/thomasmerz/6ebc63b75393b8fa149297820a377ad3
 - pi-hole-update.sh https://gist.github.com/thomasmerz/ee6d401fdb09dbd607e8f0015436a2bd
 - DEBIAN_FRONTEND=noninteractive apt-get update > /dev/null &&
 DEBIAN_FRONTEND=noninteractive apt-get upgrade -y --with-new-pkgs > /dev/null; systemctl is active docker -q || systemctl start docker
 - [-f/var/run/reboot-required] && shutdown -r +1; apt-get clean >/dev/null
 - needrestart -klp >/dev/null | { needrestart -klp; shutdown -r +1; }



TWEAKS

- https://thomasmerz.github.io/pihole-wireguard-knowhow/#tweaks
- Keep database "small" / disable DoH and Apple's iCloud Private Relay / reduce queries + Reduce also blocked queries
- Force network-wide usage of SafeSearch (Google, Startpage.com)



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* (diverses)
- oids.nl* (meta-liste)
- crazy-max (Windows-Spy-Blocker)
- Liamenglandl* (Apple, Microsoft)



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

FAZIT

- "Bitte keine Werbung, Malware und Tracking"
- Zuhause und unterwegs zum Spottpreis/kostenlos (also egal wo!)
- Braucht aber etwas "Spaß"
 - am Administrieren
 - und an/mit Linux/Docker
- Manchmal muss was gefixt werden ("Overblocking")
 - lokal per Whitelist
 - oder dem Blocklistenbetreiber melden
 - oder PR machen und Contributor werden!



EXPERTEN-TIPP ...

iPhone App-Datenschutzbericht! (Android?) → JSON





DANKE UND VIEL SPAß BBEIM SELBERMACHEN!

- @abimelechbeutelbilch@fulda.social
- github.com/thomasmerz/
- Privacy-ToGo@Rhoenwurz.de

SCAN ME



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/
- https://github.com/thomasmerz/talks/



























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?





SCAN ME

5e643732bd28ee8b58c59cc32b3ccfd5

https://gist.github.com/thomasmerz/

```
thomas@merz-nimbus:~/Documents/iphone-privacy [0/5474]
00:10 $ bat auswertungen.sh
         File: auswertungen.sh
         # Einstellungen / Datenschutz / App-Datenschutzbericht
         for f in App_Privacy_Report_*ndjson; do
          ["$1"!= ""] && f="$1" # do not loop if filename is given
           jq < "$f" | ack \"domain\": > "$f"-alle-domains.log
          # Auswertung Spotify:
           ig < "$f" | ack \"domain\": -A9|grep com.spotify.client -B9|ack \"domain\":|sort > "$f"-spotify.log
           # Auswertung WhatsApp:
           jq < "$f" | ack \"domain\": -A9|grep WhatsApp -B9|ack \"domain\":|sort > "$f"-whatsapp.log
           # Auswertung Google DNS:
           jq < "f" | ack "domain.*8 \ .8 \ ." -A9 > "f"-google-dns.log
          # Auswertung Reddit:
           jq < "$f" | ack \"domain\": -A9|grep com.spotify.client -B9|ack \"domain\":|sort > "$f"-reddit.log
           jq < "$f" | ack \"bundleID\": | sort -u > "$f"-alle-apps.log
           # echo Connections from "$app" to: jq < "$f" | ack \"domain\": -A9|grep "$app" -B9|ack \"domain\":|sort</pre>
          for app in $(jq < "$f" | ack \"bundleID\": | sort -u | cut -d "\"" -f4); do</pre>
            echo Connections from "$app" to:
             jq < "$f" | ack \"domain\": -A9|grep "$app" -B9|ack \"domain\"|sort | tee "$f"-app-"$app"-ziele.log</pre>
           done > "$f"-alle-ziele-je-app.log
          # ./pihole adlist tool -d 1 -t 10 -u -a -s hits DESC
          # search for "Top blocked adlist domains" and copy domain|hits table
           #for d in $(grep -E "\.com|\.net" auswertungen.sh.top-10-1d); do ack "$d" "$f"-*.log; done
           grep -E "\.com|\.net" auswertungen.sh.top-10-1d | awk '{print $1}' | while IFS= read -r line; do
            grep "$line" "$f"-app-*-ziele.log
          [ "$1" != "" ] && break # do not loop if filename is given
 thomas@merz-nimbus:~/Documents/iphone-privacy [0/5474]
```

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.crystalnix.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.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-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)wissentlich 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 SELBERWACHEN!

- @abimelechbeutelbilch@fulda.social
- github.com/thomasmerz/
- Privacy-ToGo@Rhoenwurz.de











