TrutzBox Kompendium

Version 9.3

Hermann Sauer
Comidio GmbH

Februar 2024

Dokumenthistorie

19.12.2016 – Beschreibung der TrutzBox E-Mail Alternativen zugefügt
19.01.2017 – Mail-Subject Anpassung für verschlüsselt und signiert angepasst
06.02.2017 – Erklärung der Keywörter in Status zugefügt
07.03.2017 - Unterschied zwischen TrutzBrowse und TrutzContent zugefügt
01.09.2017 – VPN-Zertifikate zugefügt
28.09.2017 - feste IP-Adresse beim Setup zugefügt, Beschreibung des TrutzBox-Netzwerks erweitert
29.09.2017 – Kapitel „Was ist eine „Privacy-Box“ zugefügt
01.10.2017 – neues Comidio Layout eingebaut
30.10.2017 – TrutzBox Gesamt-Architektur unter „TrutzBox Netzwerk“ eingefügt
07.12.2017 – TrutzContent Beispiel zugefügt
15.01.2018 – Account Verwaltung hinzugefügt
16.01.2018 – TrutzMail Beschreibung bzgl. des automatischen Zertifikats-Updates überarbeitet
16.01.2018 – TrutzMail Logfile Beschreibung hinzugefügt
22.02.2018 – Gruppen-Chat zugefügt
23.03.2018 – „Session Replay“ zugefügt
25.05.2018 – weitere TrutzMail Use-Cases zugefügt
28.05.2018 – externes TrutzBox-Netzwerk um Ipv6 ergänzt
26.09.2018 – Fernzugriff: TrutzDynDNS und TrutzBox Let´s Encrypt Zertifikat zugefügt
27.10.2018 – Beschreibung für Zugriff über das Internet auf TrutzBox-Anwendungen, ohne Fernzugriff zugefügt
27.11.2018 – XMPP-Client Swift zugefügt
08.01.2019 – Ports für TrutzRTC angepasst
14.01.2020 – Neues Userinterface
16.01.2020 - TrutzBox-Business vs- TrutzBox-Home
22.01.2020 – einige aktuelle Überwachungs-Fakten zugefügt
08.08.2020 – TrutzBrowse deaktivieren zugefügt
21.04.2021 –UI Erweiterungen hier dokumentiert
21.05.2021 – Erklärung für Standard-Filterlisten zugefügt
22.05.2021 – System-Logs zugefügt
08.09.2023 – Nach langer Zeit eine komplette Überarbeitung des Kompendiums begonnen
28.01.2024 – Neue Funktionen unter „Sichern und Wiederherstellen“ beschrieben

Die Herausforderung

Das Sammeln von Daten ist eines der wichtigsten Geschäftsmodelle des Internets. Es ist der Rohstoff des digitalen Zeitalters. Nicht erst seit den Aufdeckungen von Edward Snowden wissen wir, dass wir uns im Internet nicht unbeobachtet bewegen, sondern permanent ausspioniert und manipuliert werden. Und dass es im Internet auch Kriminelle gibt, die an unser Geld wollen.
Nicht nur Berufsgruppen, die besonders sensitive Information austauschen müssen wie Ärzte, Rechtsanwälte, Steuerberater, Politiker, Geistliche, Sozialarbeiter (Sorgentelefon), Journalisten, politische Aktivisten usw. sind durch dieses massenweise Ausspähen von Daten kompromittiert, sondern auch jeder private Internet-Nutzer und jeder Mitarbeiter einer Firma. €350 Milliarden beträgt schätzungsweise der Schaden, der weltweit alleine durch Cyber-Kriminalität verursacht wird[1]
Zu den Ausspähern zählen:

- „kommerzielle digitale Überwachung“, eine milliardenschwere Industrie bestehend aus riesigen Monopolisten sowie geschätzte 81.000 Firmen, die vom Erfassen und Handeln von Daten leben,
- Geheimdienste und andere staatliche Einrichtungen, die illegalerweise oder zumindest an der Legalitätsgrenze in unsere Privatsphäre eindringen und
- kriminelle Internet-Hacker.

Sie alle beobachten, erfassen und speichern unsere Aktivitäten im Internet. Diese Gruppen sind durch ihre fast unbegrenzten Budgets, ihr Know-how, ihre technischen und juristischen Möglichkeiten dem durchschnittlichen Internet-Nutzer weit überlegen. Der durchschnittliche Internet-Nutzer hat keine Chance, sich dieser Massenüberwachung zu entziehen. In der Regel merkt er noch nicht einmal, dass er überwacht wird, geschweige denn, dass Daten von ihm gesammelt werden.
Die Comidio GmbH wurde von acht erfahrenen IT-, Sicherheits-, Rechts- und Marketing-Experten gegründet, um sowohl dem Technik-Laien als auch dem Internet-Experten Mittel an die Hand zu geben, sich gegen dieses Ungleichgewicht zu wehren.
Der Firmenname Comidio leitet sich aus dem lateinischen c**om**modus (bequem) + praes**idio** (Schutz) ab. Jeder hat ein Recht auf Anonymität und die meisten Menschen sind dagegen, dass sie so umfänglich und anhaltslos überwacht werden. Viele, die sich dieses Problems bewusst sind, meiden kostenlose Internet-Dienste wie Facebook, Google, X (vormals Twitter) u.ä.; sie nutzen beim Bezahlen möglichst Bargeld und haben keine Kundenkarten. Aber bei der sonstigen Nutzung des Internets würden sie auch unterbinden, dass ihre Nutzungs-Profile gesammelt werden, aber wissen nicht, was sie dagegen tun können.
Das Comidio Team hat über Jahre hinweg sowohl den Markt, als auch die technischen Möglichkeiten dieser drei Angreifer-Gruppen analysiert. Parallel wurde analysiert, welche technischen Werkzeuge zur Verfügung stehen, um sich gegen solche Angriffe zu schützen. Dieses Kompendium gibt einen groben Überblick über die gewonnenen Erkenntnisse und geht detailliert auf die Architektur der TrutzBox® ein.
Die Auswertung hat gezeigt, dass es sehr viele technische Möglichkeiten gibt, sich im Internet zu schützen.
Allerdings sind die verfügbaren Werkzeuge einzeln nicht ausreichend:

[1] http://www.rolandberger.de/media/pdf/Roland_Berger_TAB_Cyber_Security_20150305.pdf

- End-Geräte-Firewalls & -Virenscanner: gibt es nur für PCs oder für mobile Geräte. Darüber hinaus verhindern Firewalls & Virenscanner nicht das User-Profiling (Erstellen von Benutzerprofilen) beim Zugriff aufs Internet.
- Anonymisierungs-Browser-Plugins: z.B. Ghostery, AdBlockPlus oder NoScript. Diese Plugins gibt es oft nur für PCs und nicht für Mobile Devices. Da der Browser bestimmt, welche Kommunikations-Daten solche Plugins zu sehen bekommen, ist es möglich, den Benutzer trotz dieser Plugins zu tracken. Zudem sind sie vom Laien kaum bedienbar.
- Scripting oder Cookies im Browser abzuschalten führt dazu, dass viele Webseiten nicht mehr funktionieren. Das gleiche gilt für Werkzeuge wie Tor-Browser oder Tails.
- Anonymisierungsdienste wie Tor-Browser oder Tor-Boxen, VPNs/Proxys sind teuer oder langsam und anonymisieren oftmals die IP-Adresse nicht. Je nach Betreiber könne VPNs/Proxys sogar als zusätzliches Spionage-Werkszeug missbraucht werden. Ferner sind sie nicht von allen Internet-Geräten nutzbar.
- PGP-Verschlüsselungs-Plugins für E-Mail Clients sind umständlich und kompliziert zu bedienen, überlassen die Verwaltung der Schlüssel dem Anwender und verschlüsseln die Metadaten nicht.
- Professionelle Firewalls/DPI: sind sehr teuer, und vom Laien nicht bedienbar.

Selbst wenn alle diese Tools genutzt würden, wäre dies keine optimale Lösung. Man müsste dazu nicht nur technisch sehr versiert sein, es ist auch mühsam und aufwändig, diese Tools auf den unterschiedlichen Internet-Geräten zu installieren, up-to-date zu halten und zu bedienen. Und wer hat überhaupt noch einen kompletten Überblick über alle seine internetfähigen Geräte zu Hause? Für manche Geräte im Haushalt, die sich heute oder zukünftig mit dem Internet verbinden (Smart Home und Internet der Dinge - IoT)(z.B. Fernseher, Kühlschrank, Auto, Waschmaschine, Fitnessarmband…), sind uns keine Werkzeuge bekannt,die solche Geräte vor Angriffen oder Tracking schützen würden.
Mit dieser Erkenntnis war dem Comidio Team klar, dass eine Lösung benötigt wird, die möglichst viele der aktuell verfügbaren Technologien zur Abwehr von Internet-Angriffen und Datenspionage in einem Gerät vereint, so dass dieses eine Gerät nicht nur alle internetfähigen Geräte schützt, sondern auch einfachst zu installieren und zu bedienen ist.
Comidio ist davon überzeugt, dass es gelungen ist, eine solche Lösung unter dem Namen TrutzBox® zu entwickeln!
Der Name „TrutzBox®“ ist von den Trutzburgen abgeleitet die es im Mittelalter gab. Mit Trutzburg werden solche Belagerungsburgen bezeichnet, die nahe einer anderen Burg errichtet wurden, oder Gegenburgen, die territoriale Machtansprüche in Grenzregionen sichern sollten.. Trutz ist die mittelhochdeutsche Form von Trotz und beschreibt somit einen Akt der Gegenwehr[2]. Die TrutzBox® schützt ihren Besitzer (im eigentlichen Sinne das Haus des Besitzers inkl. aller Bewohner) vor Diebstahl der persönlichen Daten und böswillige Angriffe aus dem Internet.
Allerdings gibt es keine 100%ige Sicherheit; auch nicht mit Einsatz der TrutzBox®. Zur Basisabsicherung sollte der Anwender immer einen Virenscanner auf seinen Rechnern installiert haben und zeitnah Updates auf allen seinen Geräten einspielen.

[2] http://de.wikipedia.org/wiki/Trutzburg

Für weitergehende Informationen zum Thema Internet-Angriffe, -Technologien und -Schutzmechanismen, empfiehlt sich ein Blick in das „Privacy-Handbuch“[3], „Security in a box“[4] oder in das „Crypto-party-Handbook“[5].
Dieses TrutzBox Kompendium beschreibt ausführlich die aktuelle Bedrohungslage, vor welchen Angriffen die Comidio TrutzBox schützt und wie sie im Detail funktioniert.

Kommerzielle Daten-Tracker und Daten-Händler

„Alle Daten sind Kreditdaten, wir wissen nur noch nicht, wie wir sie einsetzen werden“

Der Satz ist aus dem Jahre 2018 und stammt von Douglas Merrill, der 2009 nach fünf Jahren als Chief Information Officer bei Google das Unternehmen ZestCash gründete, das inzwischen unter dem Namen ZestFinance Kreditwürdigkeitsanalysen auf Basis personenbezogener Daten anbietet.
Mehr als 1.000 Firmen haben sich darauf spezialisiert, Daten zu sammeln und diese gewinnbringend zu verkaufen. Die amerikanische Wettbewerbs- und Verbraucherschutzbehörde (FTC), beschreibt in der Studie „Data Brokers, A Call for Transparency and Accountability“[6] im Detail, wie sich dieser Markt mittlerweile entwickelt hat und welche negativen Einflüsse dieses Geschäftsmodell auf die Gesellschaft ausübt. Diese Daten-Händler sammeln und verkaufen Ihre Daten ohne Ihr Wissen oder Ihre Zustimmung und, da es deren „Kapital“ darstellt, löschen sie diese Daten nie. Selbst wenn der Internet-Nutzer eine seriöse Internetseite ansteuert, wird mittlerweile mit ziemlicher Sicherheit sein Surf-Profil (der digitale Fußabdruck) bei Google und weiteren Daten-Sammlern erfasst, auch wenn er nie eine Google-Seite direkt aufgerufen oder irgendwelchen Google-AGBs zugestimmt hat. Im Jahr 2023 hatte allein focus.de 10 verschiedene Daten-Tracker in der Homepage eingebaut.
Und die Anzahl der Firmen, die sich für Daten interessieren, steigt rapide an. Selbst bei einem TV-Gerät kann man nicht mehr sicher sein, dass keine persönlichen Daten an TV-Sender oder sogar -Hersteller oder dritten Firmen übermittelt werden. Der TV-Hersteller Samsung empfiehlt in seinen Nutzungsbedingungen, besser nichts Privates in Anwesenheit eines Smart-TVs zu sagen, weil die Spracherkennung dies irgendwohin übermitteln könnte[7].
Aber nicht nur das Mikrofon am Fernseher könnte den Benutzer ausspionieren. Aktuelle Fernseh-Generationen kommen technologisch den Smartphones immer näher, indem die Funktionalität des Fernsehers mit Herunterladen von Apps erweitert werden kann. Und dazu gibt es noch interaktives TV (HbbTV). Somit sind App-Anbieter, TV-Gerätehersteller, HbbTV-Anbieter, Anbieter elektronischer Programmführer (Electronic Programm Guide – EPG) und TV-Sender in der Lage, das Benutzerverhalten zu tracken[8],[9],[10]. Und mit Hilfe eines kleinen preiswerten DVB-Senders ist es sogar jedem möglich, einen

3 http://de.wikibooks.org/wiki/Privacy-Handbuch

4 https://securityinabox.org/en

5 http://key.cryptoparty.is/files/cryptoparty-handbook-2013-08-21/cryptoparty-handbook-2013-08-21.pdf

6 http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

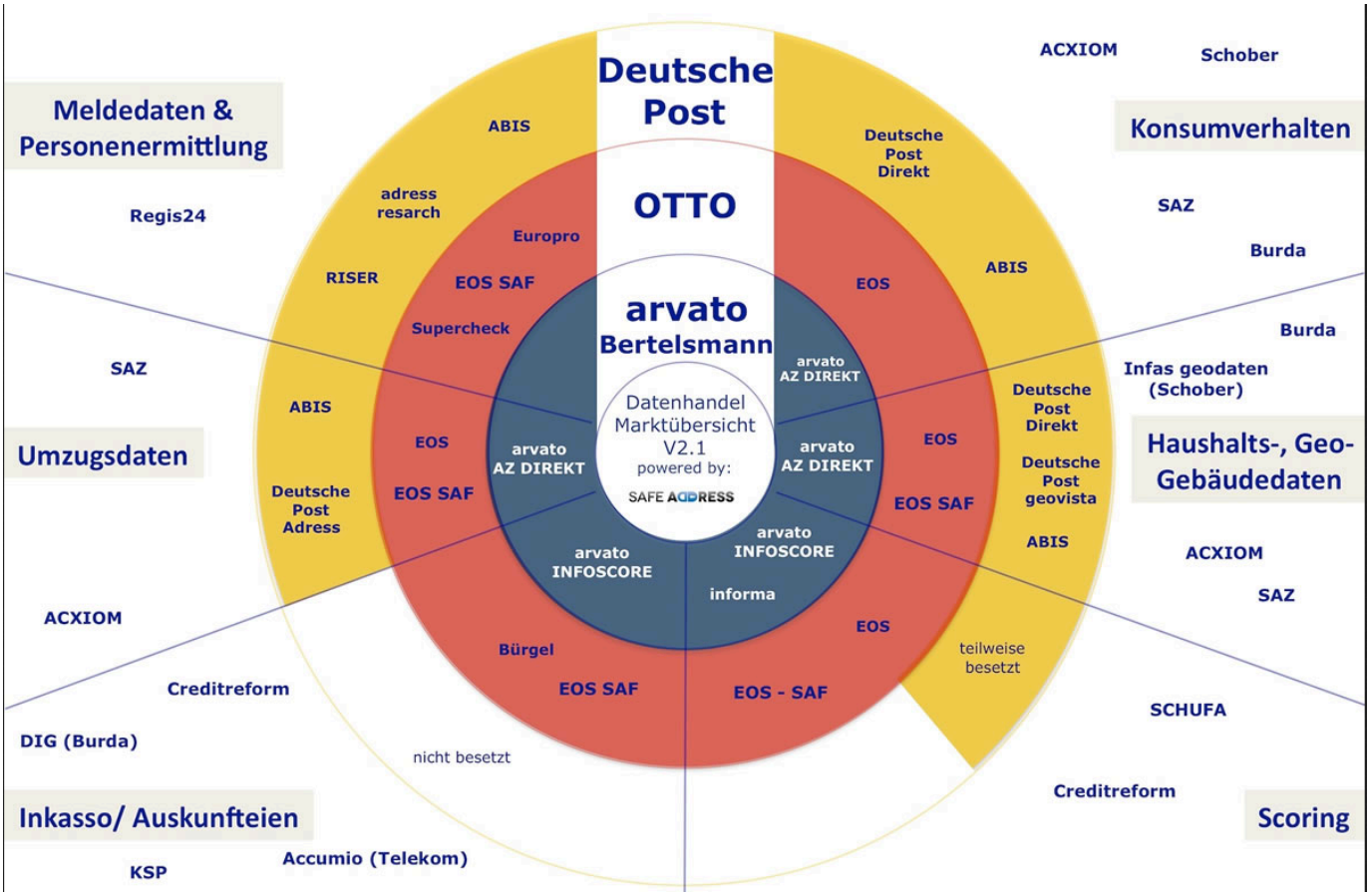
7 https://netzpolitik.org/2015/samsung-warnt-bitte-achten-sie-darauf-nichts-privates-vor-unseren-smarttvs-zu-erzaehlen/

8 https://netzpolitik.org/2015/studie-anonyme-nutzung-von-smart-tvs-kaum-moeglich/

9 http://www.faz.net/aktuell/feuilleton/medien/smart-tv-wenn-der-fernseher-zum-datensammler-wird-13648552.html

10 https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/150227%20PM%20Datenschutz%20und%20Smart-TV.pdf

"Man in the Middle Attack" zum Fernseher durchzuführen und den kompletten Empfangs- und Sende-Stream zu manipulieren[11].
Diese Übersicht der Datenhändler-Marktführer im deutschen Datenhandel zeigt, welche Unternehmen sich zu welchen Zwecken positioniert haben (ohne Internetplattformen)[12] - Stand 11.2014:



https://de.wikipedia.org/wiki/Datei:Datenhandel_prisma_2.1.jpg

Aus diesen gesammelten Daten werden mit Big Data Analysen Informationen über Internet-Nutzer zusammengestellt; z.B. Informationen über

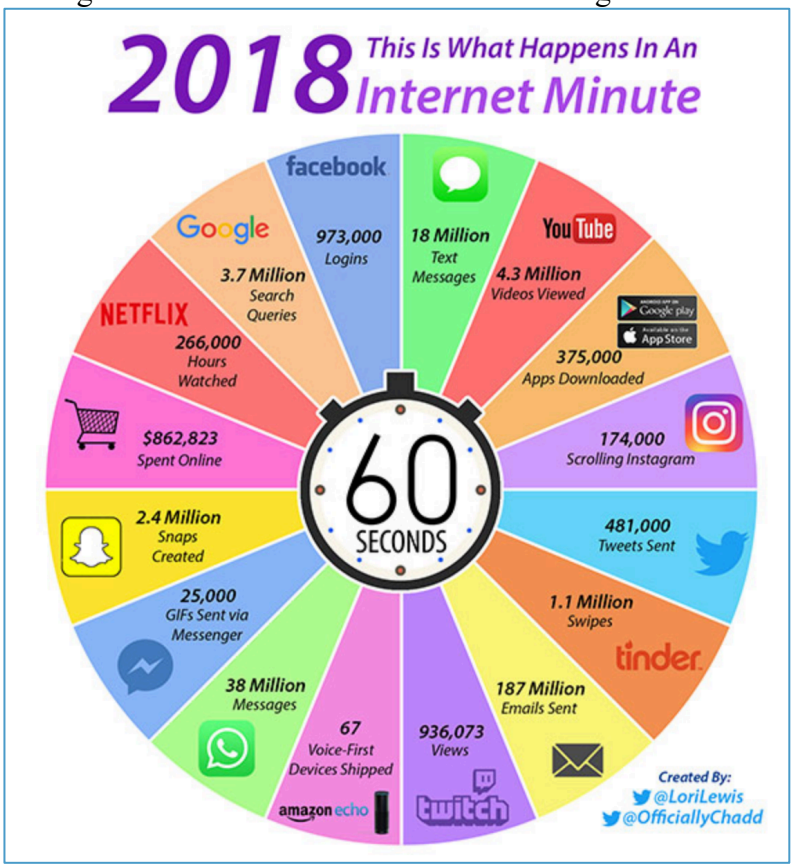
- sein Kaufverhalten,
- seine finanzielle Situation,
- seinen Bildungsgrad und Beruf,
- seine religiöse und sexuelle Orientierung,
- seine nationale Abstammung und Hautfarbe,
- seine Krankheiten,

[11] http://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/swr/smart-tv-22042015-100.html

12 https://safeaddress.de/blog/adress-und-datenhandel-ueberblick/

- eventuelle Haustiere und
- eventuelle sportliche Tätigkeiten.

Aber natürlich sind es vor allem die vielen kostenlosen und sogar bezahlten Internet-Angebote, die unser Verhalten tracken.
Folgende Grafik zeigt recht anschaulich, in welcher Frequenz häufig genutzte Internet-Dienste weltweit genutzt werden. Fast alle diese Dienste werden auch dafür genutzt unser Verhalten und unsere Vorlieben zu analysieren und mit den gewonnenen Erkenntnissen uns alle in irgendeiner Form zu manipulieren.



https://www.allaccess.com/merge/archive/28030/2018-update-what-happens-in-an-internet-minute#sthash.IKyiTou1.uxfs

Schauen wir uns zunächst ein paar solcher kommerziellen Firmen etwas genauer an, deren Geschäftsmodel es ist, mit unseren Daten Geld zu verdienen.

Die Firma Facebook

Eines der bekanntesten globalen Unternehmen, das mit unseren Daten Milliarden verdient, ist Facebook. Alleine diese Facebook-Facts macht die Größe dieses Unternehmens deutlich [13] (Anfang 2020):

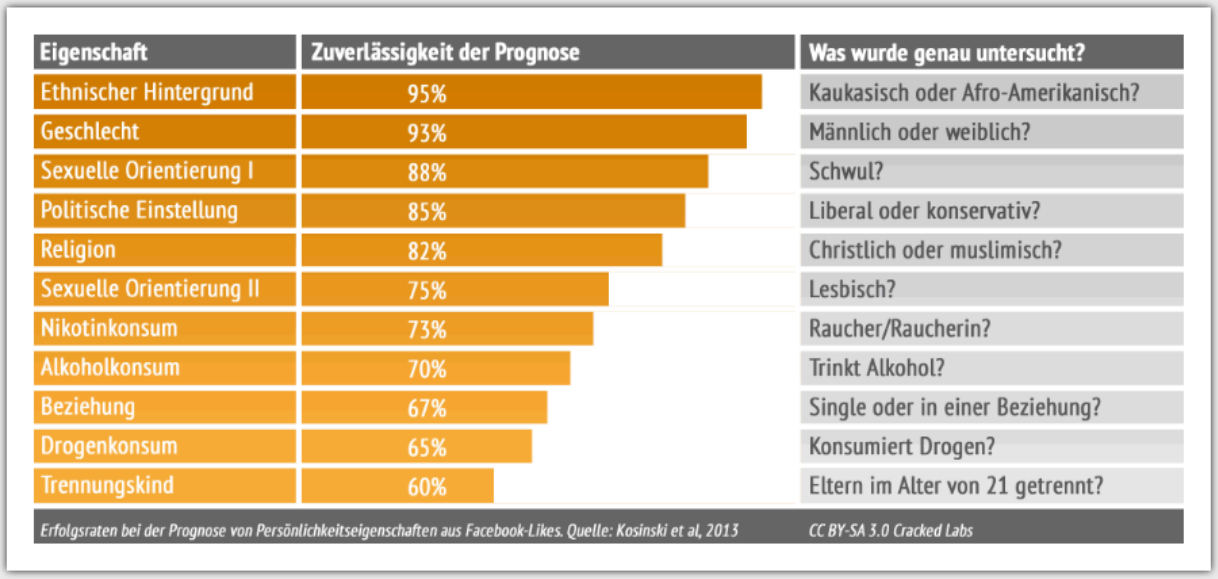
- 2,9 Milliarden Menschen nutzen mindestens einen Facebook Dienst im Monat (FB, IG, WA, …)
- 2,3 Milliarden Menschen nutzen mindestens einen dieser Dienste pro Tag
- In Europa gibt es 394 Millionen aktive Facebook Nutzer – 294 Millionen davon sind jeden Tag auf Facebook aktiv
- Es gibt 140 Millionen aktive Unternehmen auf Facebook (Basis: Small Businesses)
- 4 Millionen Unternehmen werben mit Instagram-Story-Ads
- 21,1 Milliarden Umsatz im letzten Quartal (25%+ zum Vorjahr)

Viele Webseiten haben mittlerweile den Facebook-Like-Knopf auf ihren Seiten einprogrammiert. Um der Seite anzuzeigen, dass man sie mag werden pro Tag 7 Milliarden mal dieser Knopf gedrückt (das sind über 80.000 Likes pro Sekunde!)[14]. Unabhängig davon, ob man überhaupt ein Konto bei Facebook

[13] https://allfacebook.de/toll/state-of-facebook

[14] http://www.doz.com/media/one-minute-internet

hat, können unter andere folgende persönliche Eigenschaften mit einer gewissen Zuverlässigkeit allein auf Basis dieser Facebook-Likes berechnet werden[15],[16]:



Erfolgsraten bei der Prognose von Persönlichkeitseigenschaften aus Facebook-Likes. Quelle: Kosinski et al, 2013

Quelle: Wolfie Christl, Cracked Labs (November 2014): Durchleuchtet, analysiert und einsortiert. Abgerufen am: 10.04.2015, 11:55 von http://crackedlabs.org/studie-kommerzielle-ueberwachung, Lizenz: CC BY-SA 3.0 Cracked Labs (http://creativecommons.org/licenses/by-sa/3.0/deed.de)

Aber auch wenn Sie diesen Like-Knopf nicht drücken, kann es sein, dass Facebook trotzdem weiß, dass Sie gerade diesen Artikel lesen oder sich für ein bestimmtes Produkt interessieren da viele Web-Seiten und Smartphone-Apps diese Information direkt von Ihrem Smartphone oder PC an Facebook liefern.

Aber Facebook wertet nicht nur die Anzeige und das Anklicken von Like-Knöpfen aus. Über die vielen weiteren Kooperationen mit anderen Datensammlern und ausgeklügelten Analyse-Werkzeugen, mit deren Hilfe Facebook aus den Daten der Facebook Nutzer und deren „Freunde“ Informationen errechnen, kennt Facebook 98 Attribute von jedem Einzelnen[17].

Facebook hat sogar ein Patent zum Abhören über das Smartphone-Mikrofon[18]. Facebook erklärt allerdings, das Patent richte sich gegen Konkurrenten und solle nie zum Einsatz kommen.

Und Facebook bekommt nicht nur Daten über uns durch unsere Online-Aktivitäten. Facebook hat Schnittstellen eingebaut, mit deren Hilfe Partnerfirmen auch „Offline-Conversations“ auf Facebook hoch laden können[19]. Und dieses Interface wird von sehr vielen Firmen genutzt.

15 http://crackedlabs.org/studie-kommerzielle-ueberwachung

http://www.pnas.org/content/suppl/2013/03/07/1218772110.DCSupplemental/pnas.201218772SI.pdf

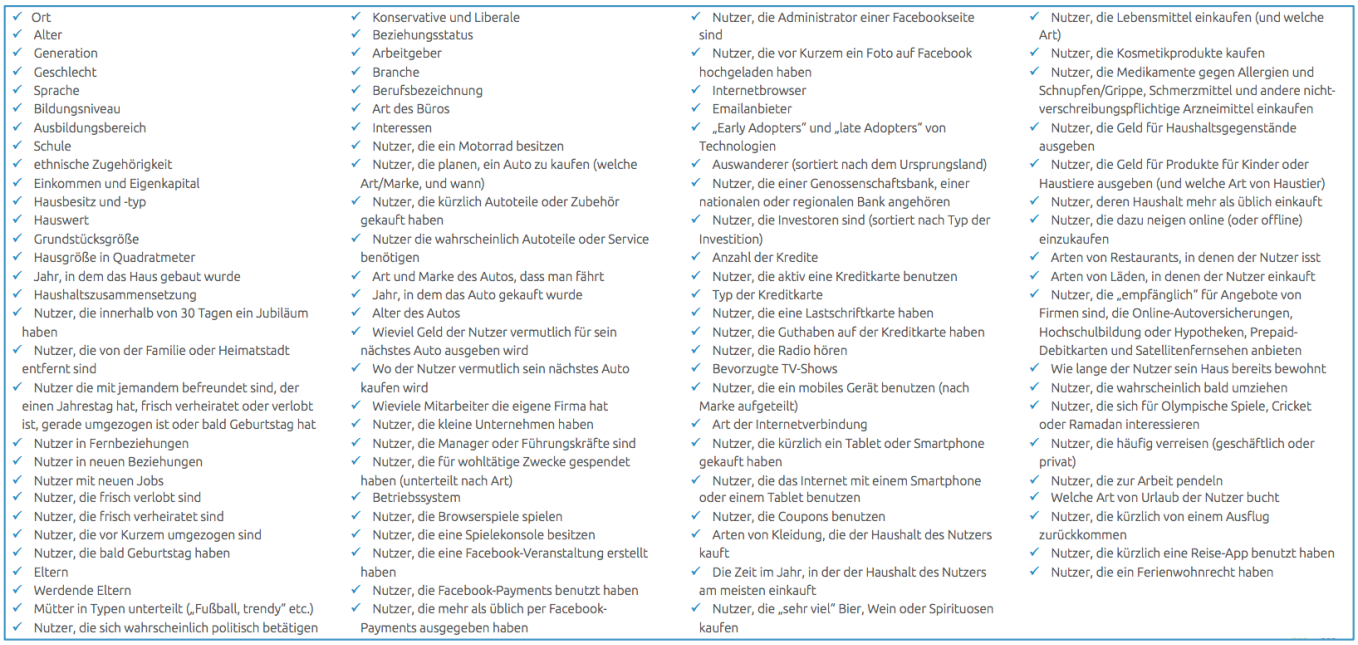
16 http://www.pnas.org/content/pnas/110/15/5802.full.pdf

17 https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/

18 https://www.sueddeutsche.de/digital/audio-ueberwachung-facebook-will-das-patent-zum-abhoeren-1.4034080

19 https://www.facebook.com/business/help/1278167592274041

Mehr Details zu den Daten, die Facebook sammelt sind unter dem Blog „What should you think about when using Facebook?“ [20] und in dem Bericht „Facebook Doesn’t Tell Users Everything It Really Knows About Them“[21] aufgeführt.



- Ort
- Alter
- Generation
- Geschlecht
- Sprache
- Bildungsniveau
- Ausbildungsbereich
- Schule
- ethnische Zugehörigkeit
- Einkommen und Eigenkapital
- Hausbesitz und -typ
- Hauswert
- Grundstücksgröße
- Hausgröße in Quadratmeter
- Jahr, in dem das Haus gebaut wurde
- Haushaltszusammensetzung
- Nutzer, die innerhalb von 30 Tagen ein Jubiläum haben
- Nutzer, die von der Familie oder Heimatstadt entfernt sind
- Nutzer die mit jemandem befreundet sind, der einen Jahrestag hat, frisch verheiratet oder verlobt ist, gerade umgezogen ist oder bald Geburtstag hat
- Nutzer in Fernbeziehungen
- Nutzer in neuen Beziehungen
- Nutzer mit neuen Jobs
- Nutzer, die frisch verlobt sind
- Nutzer, die frisch verheiratet sind
- Nutzer, die vor Kurzem umgezogen sind
- Nutzer, die bald Geburtstag haben
- Eltern
- Werdende Eltern
- Mütter in Typen unterteilt („Fußball, trendy“ etc.)
- Nutzer, die sich wahrscheinlich politisch betätigen
- Konservative und Liberale
- Beziehungsstatus
- Arbeitgeber
- Branche
- Berufsbezeichnung
- Art des Büros
- Interessen
- Nutzer, die ein Motorrad besitzen
- Nutzer, die planen, ein Auto zu kaufen (welche Art/Marke, und wann)
- Nutzer, die kürzlich Autoteile oder Zubehör gekauft haben
- Nutzer die wahrscheinlich Autoteile oder Service benötigen
- Art und Marke des Autos, dass man fährt
- Jahr, in dem das Auto gekauft wurde
- Alter des Autos
- Wieviel Geld der Nutzer vermutlich für sein nächstes Auto ausgeben wird
- Wo der Nutzer vermutlich sein nächstes Auto kaufen wird
- Wieviele Mitarbeiter die eigene Firma hat
- Nutzer, die kleine Unternehmen haben
- Nutzer, die Manager oder Führungskräfte sind
- Nutzer, die für wohltätige Zwecke gespendet haben (unterteilt nach Art)
- Betriebssystem
- Nutzer, die Browserspiele spielen
- Nutzer, die eine Spielekonsole besitzen
- Nutzer, die eine Facebook-Veranstaltung erstellt haben
- Nutzer, die Facebook-Payments benutzt haben
- Nutzer, die mehr als üblich per Facebook-Payments ausgegeben haben
- Nutzer, die Administrator einer Facebookseite sind
- Nutzer, die vor Kurzem ein Foto auf Facebook hochgeladen haben
- Internetbrowser
- Emailanbieter
- „Early Adopters“ und „late Adopters“ von Technologien
- Auswanderer (sortiert nach dem Ursprungsland)
- Nutzer, die einer Genossenschaftsbank, einer nationalen oder regionalen Bank angehören
- Nutzer, die Investoren sind (sortiert nach Typ der Investition)
- Anzahl der Kredite
- Nutzer, die aktiv eine Kreditkarte benutzen
- Typ der Kreditkarte
- Nutzer, die eine Lastschriftkarte haben
- Nutzer, die Guthaben auf der Kreditkarte haben
- Nutzer, die Radio hören
- Bevorzugte TV-Shows
- Nutzer, die ein mobiles Gerät benutzen (nach Marke aufgeteilt)
- Art der Internetverbindung
- Nutzer, die kürzlich ein Tablet oder Smartphone gekauft haben
- Nutzer, die das Internet mit einem Smartphone oder einem Tablet benutzen
- Nutzer, die Coupons benutzen
- Arten von Kleidung, die der Haushalt des Nutzers kauft
- Die Zeit im Jahr, in der der Haushalt des Nutzers am meisten einkauft
- Nutzer, die „sehr viel“ Bier, Wein oder Spirituosen kaufen
- Nutzer, die Lebensmittel einkaufen (und welche Art)
- Nutzer, die Kosmetikprodukte kaufen
- Nutzer, die Medikamente gegen Allergien und Schnupfen/Grippe, Schmerzmittel und andere nicht-verschreibungspflichtige Arzneimittel einkaufen
- Nutzer, die Geld für Haushaltsgegenstände ausgeben
- Nutzer, die Geld für Produkte für Kinder oder Haustiere ausgeben (und welche Art von Haustier)
- Nutzer, deren Haushalt mehr als üblich einkauft
- Nutzer, die dazu neigen online (oder offline) einzukaufen
- Arten von Restaurants, in denen der Nutzer isst
- Arten von Läden, in denen der Nutzer einkauft
- Nutzer, die „empfänglich“ für Angebote von Firmen sind, die Online-Autoversicherungen, Hochschulbildung oder Hypotheken, Prepaid-Debitkarten und Satellitenfernsehen anbieten
- Wie lange der Nutzer sein Haus bereits bewohnt
- Nutzer, die wahrscheinlich bald umziehen
- Nutzer, die sich für Olympische Spiele, Cricket oder Ramadan interessieren
- Nutzer, die häufig verreisen (geschäftlich oder privat)
- Nutzer, die zur Arbeit pendeln
- Welche Art von Urlaub der Nutzer bucht
- Nutzer, die kürzlich von einem Ausflug zurückkommen
- Nutzer, die kürzlich eine Reise-App benutzt haben
- Nutzer, die ein Ferienwohnrecht haben

Source: https://netzpolitik.org/2016/98-daten-die-facebook-ueber-dich-weiss-und-nutzt-um-werbung-auf-dich-zuzuschneiden/

Ein Werbetreibender kann bei Facebook sogar aus über 52.000 Kategorien seine Zielgruppe auswählen[22],[23].
Facebook bietet allerdings online einige Funktionen an, mit denen man seine bei Facebook gespeicherten Daten einsehen kann[24].
Umgekehrt kann ein Facebook-Nutzer neuerdings (Anfang 2020) in Facebook auch sehen, welche Daten Facebook über ihn von anderen Quellen bekommen hat. In Facebook kann der Benutzer unter „Einstellungen“ auf „Deine Facebook-Informationen“ klicken, auf der nächsten Seite auf „Aktivitäten außerhalb von Facebook“ und schließlich auf „Deine Aktivität außerhalb von Facebook“. Dann bekommt er endlich aufgelistet, welche Websites und Apps Daten an Facebook weitergegeben haben. Dort kann man zwar die Daten löschen, aber Facebook informiert damit gleichzeitig, dass danach weiterhin Daten auch aus anderen Quellen gesammelt werden.
Einen sehr interessanten Einblick, in die Interna des Unternehmens Facebook haben unter anderem die Studien von „Facebook Algorithmic Factory“ ergeben[25].

[20] https://veekaybee.github.io/facebook-is-collecting-this/

[21] https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them

[22] https://www.propublica.org/datastore/dataset/facebook-ad-categories

[23] https://www.propublica.org/article/breaking-the-black-box-what-facebook-knows-about-you

[24] https://www.facebook.com/help/131112897028467?helpref=page_content

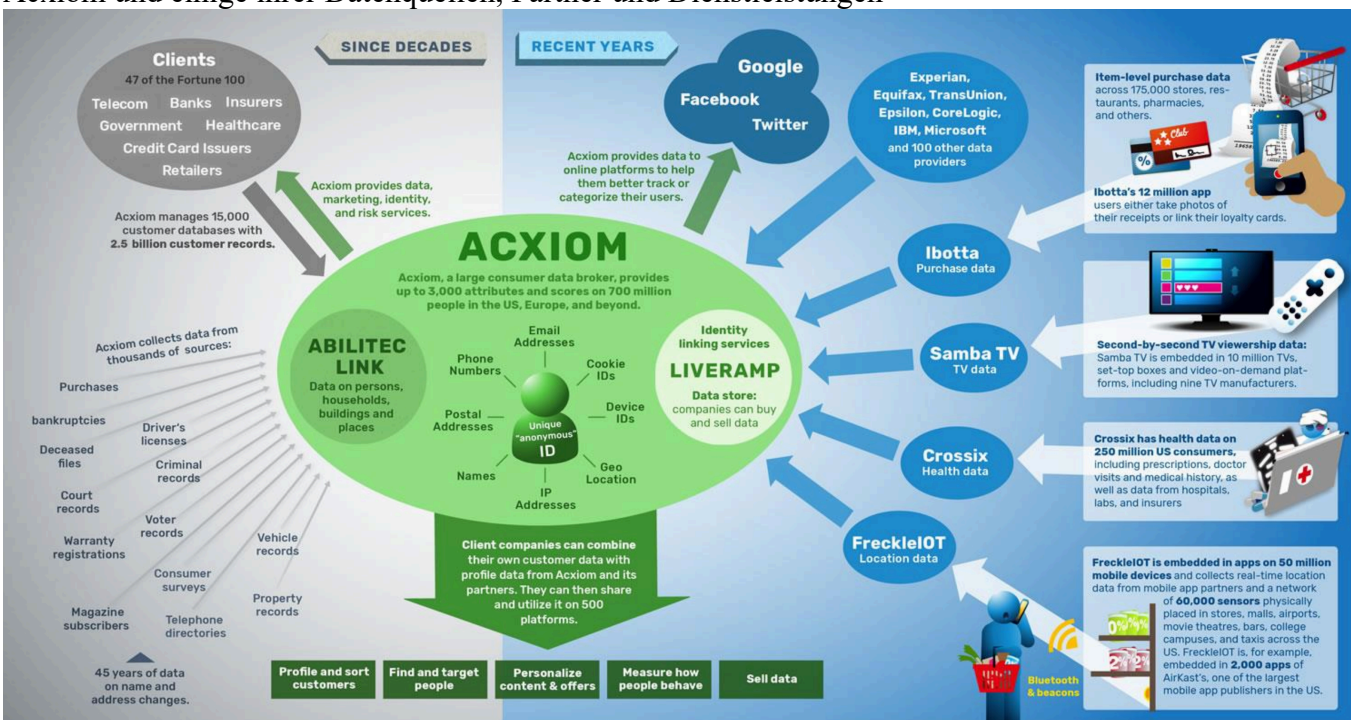
[25] https://labs.rs/en/category/facebook-research/

Die Firma Acxiom

Hier ein Zitat aus http://crackedlabs.org/studie-kommerzielle-ueberwachung:

„Die US-Firma Acxiom verfügt über umfangreiche Dossiers mit bis zu 3.000 einzelnen Eigenschaften von etwa 700 Millionen Menschen – von Ausbildung, Wohnen, Beschäftigung, Finanzen, Eigentum und Wahlverhalten bis zu „Bedürfnissen“ und „Interessen“ im Bereich Gesundheit oder etwa der „Neigung zum Glücksspiel“26. Das Unternehmen betreibt 15.000 Kundendatenbanken von globalen Top-Unternehmen, kooperiert mit Google, Facebook und Twitter und hat seit dem Kauf des Online-Spezialisten Liveramp laut Eigenangabe drei Milliarden Kundendatensätze „ins Web gebracht“. Acxiom ist auch in Deutschland tätig und besitzt laut der Wochenzeitung Die Zeit Daten von über 44 Millionen Deutschen[27]“.

Acxiom und einige ihrer Datenquellen, Partner und Dienstleistungen



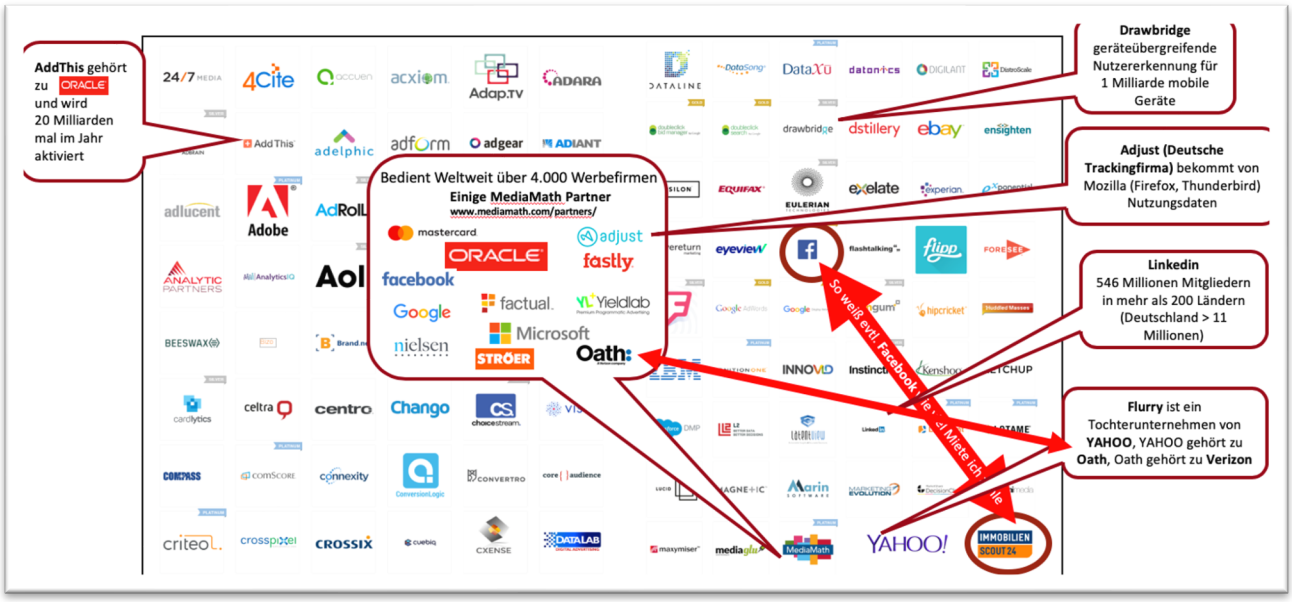
https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Wie verflochten nicht nur Acxiom, sondern alle diese Datenhändler untereinander sind, zeigt das folgende Chart, das einige ausgewählten Partner-Firmen von Liveramp[28], einer Tochterfirma von Acxiom zeigt:

[26]http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[27] http://www.zeit.de/2013/28/acxiom/komplettansicht

[28] https://liveramp.uk/partners



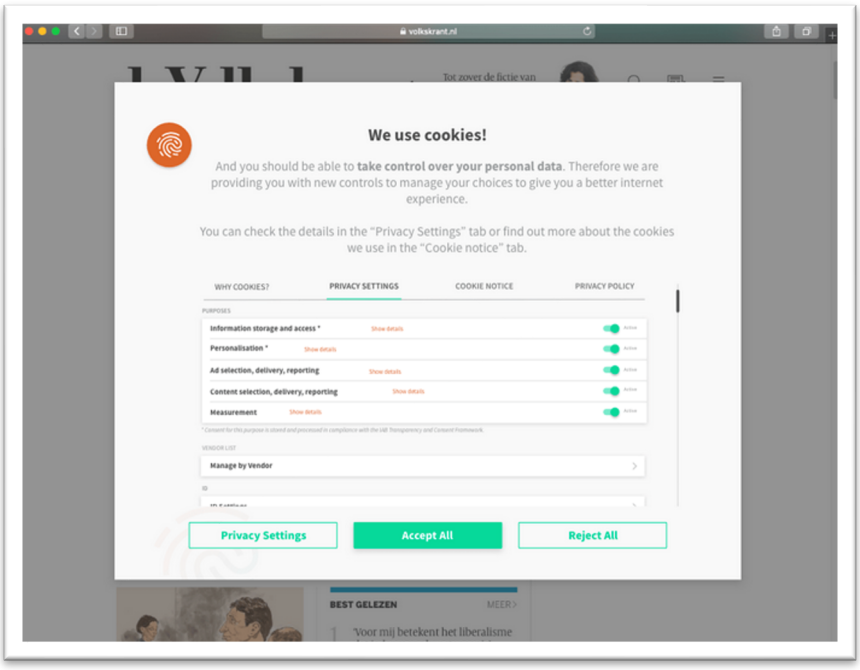
(© 2020 Comidio GmbH und https://liveramp.uk/partners)

So Kooperiert Acxiom seit Jahren mit ImmobilienScout24. Die in ImmobilienScout24 gesammelten Daten über das Interesse oder Kauf bzw. Miete von Wohnungen gehen direkt an Acxiom. Da Facebook Daten von Acxiom einkauft, „weiß" Facebook, für welche Art von Wohnung oder Immobilie man sich interessiert, oder sogar welche Miete man zahlt.
Die Übersicht zeigt auch sehr anschaulich, dass es nichts nützt sich gegen ein paar wenige Tracker zu schützen. Somit nützt es wenig, wenn wir den besten Trackingschutz im Browser haben, wenn die Smartphone-App oder unser kostenloser E-Mail-Provider weiterhin unsere Daten sammelt und weitergibt. Da diese Datenhändler untereinander Informationen über uns austauschen, bekommen kooperierende Datenhändler auch dann unsere Daten, wenn wir uns nur teilweise schützen.

Acxiom kümmert sich sogar um das Consent-Management anderer Webseiten und Apps

Im Jahr 2019 hat Liveramp die Firma Factor gekauft (faktor.io)[29]. Factor ist ein Unternehmen, das sich auf „Consent-Management" spezialisiert hat. Unter „Consent-Management" versteht man, das Einholen eins Einverständnisses (Consent) des Benutzers, dass man seine Daten sammeln und verwenden darf. Das sind z.B. diese bekannten Meldungen im Browser oder auch Apps, die unser Einverständnis dafür möchten, dass hier Cookies verwendet werden dürfen. Da Consent-Management die letzten Jahre recht komplex geworden ist, lagern viele Unternehmen das Einholen dieses Einverständnisses an darauf spezialisierte Firmen aus.

[29] https://liveramp.com/blog/liveramp-acquires-faktor/



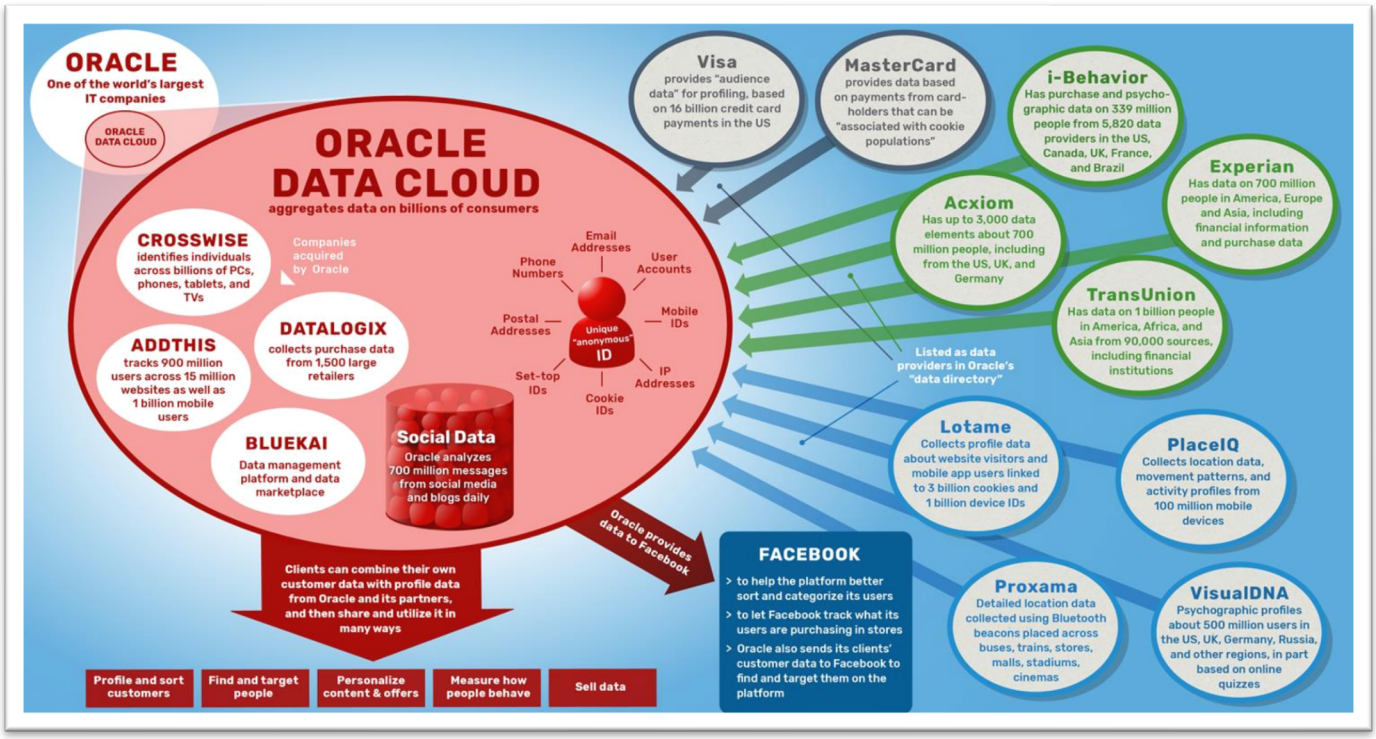
https://liveramp.com/our-platform/preference-consent-management/privacy-manager/

Mit dieser Firmenübernahme hat der Datensammler Acxiom Zugriff auf alle Webseiten, die das Consent-Management von Factor nutzen.

Die Firma Oracle

Die Firma Oracle, die ursprünglich ihr Geld mit einer relationalen Datenbank verdient hat, hat die letzten Jahre viele Firmen aufgekauft, deren Geschäftsmodel der kommerzielle Datenhandel ist. So ist Oracle mit seinen vielen Tochterfirmen mittlerweile zu einem der größten Datenhändler für Konsumenten-Daten geworden. Insgesamt bietet der Datenmarktplatz von Oracle "mehr als 30.000 Datenattribute von zwei Milliarden Verbraucherprofilen".
Während Datalogix Daten über Milliarden von Kauftransaktionen über 50 Lebensmittelketten und 1.500 große Einzelhändler sammelt, verfolgt der Sozial-Network-Aktivitäten-Markierungsdienst „AddThis“ 900 Millionen Nutzer auf 15 Millionen Websites sowie 1 Milliarde mobile Nutzer. „AddThis“ ist nicht nur eine Tochterfirma von Oracle, „AddThis“ kooperiert unter anderem auch mit Aciom um Daten auszutauschen.
Die Oracle-Tochter „Crosswise“ sammelt Aktivitätsdaten über Milliarden von Geräten und identifiziert, welche PCs, Telefone, Tablets und Fernseher von einem einzelnen Verbraucher benutzt werden. Darüber hinaus aggregiert und analysiert Oracle "700 Millionen soziale Nachrichten täglich " aus sozialen Medienetzwerken, Message Boards, Blogs, Verbraucherbewertungsseiten und Videoplattformen[30].

[30] https://crackedlabs.org/en/corporate-surveillance



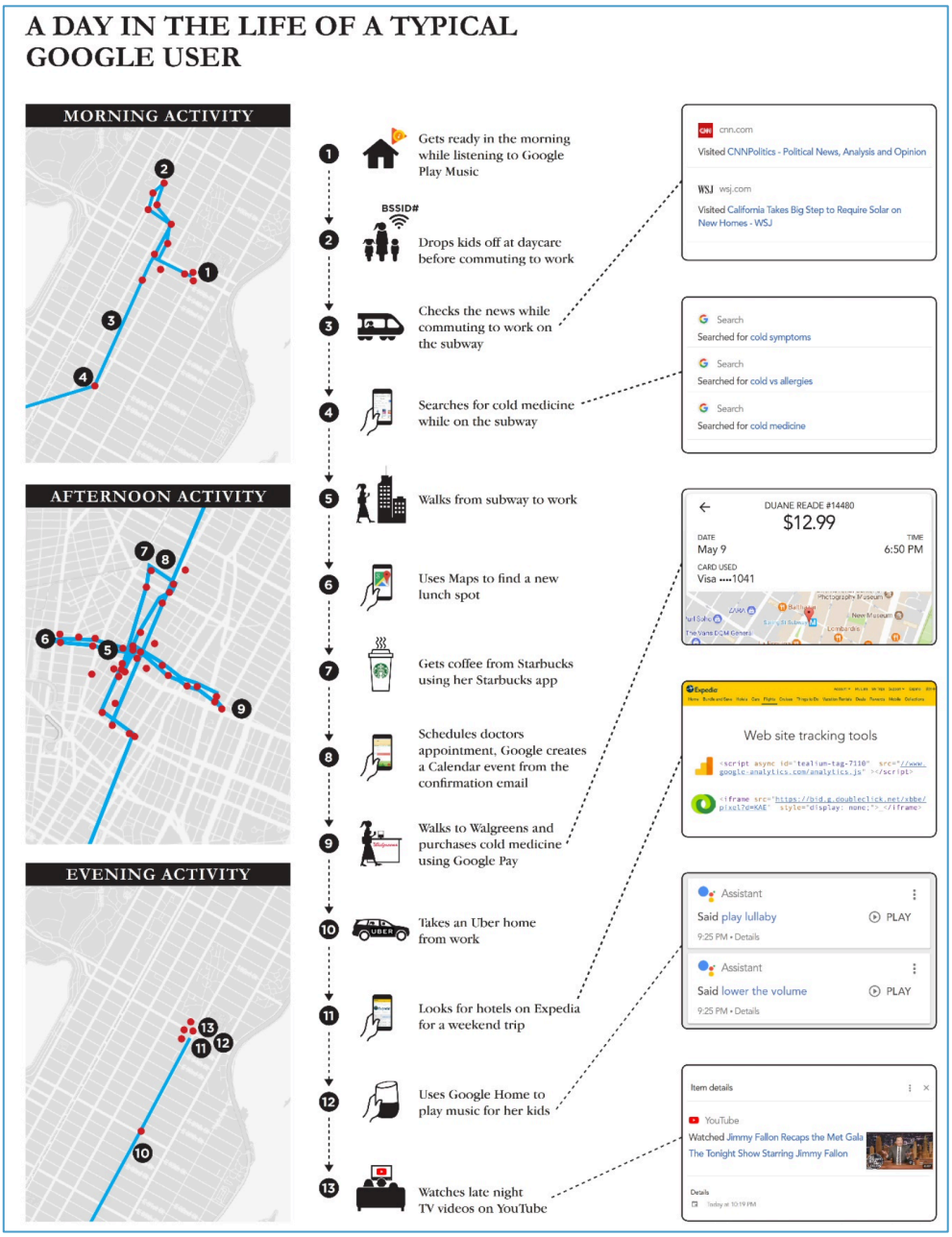
https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Die Firma Alphabet (Google)

Die Firma Alphabet (vormalig Google) ist eines der größten kommerziellen Daten-Tracker und Daten-Händler Unternehmen. Mit einer Marktkapitalisierung von 980,5 Mrd. USD (20.02.2020) glaubt auch der Markt an große Gewinne mit dem Sammeln von Daten.
Wie weit dieses Unternehmen mittlerweile schon sämtliche Teile unseres Lebens überwacht, aufzeichnet und für kommerzielle Ziele nutzt, zeigt der Bericht „Google data collection research“[31].
Wer denkt, dass Google lediglich unsere Online-Aktivitäten verfolgt, der hat sich geirrt. Nicht nur als Besitzer eines Android-Smartphones und bei Nutzung der vielen Google-Dienste hat Google Zugriff auf viele unsere Offline-Aktivitäten (siehe Grafik). Durch Ankauf weiterer Daten von anderen Dienstleistern, die auch Daten von unserem Kaufverhalten, Einkommen, Lebensverhältnisse usw. haben, ist Google rundum über uns informiert. So wurde 2018 öffentlich, dass Google sogar die Transaktionsdaten unserer Kreditkarte von Mastercard bekommt[32]. Aber auch da ist Google nicht alleine. Man sollte davon ausgehen, dass fast alle Daten die irgendwann, irgendwie von irgendwem, auch wenn diese angeblich anonym erfasst werden, an andere Firmen weiterverkauft werden, und durch Zusammenführung mit anderen Daten auch wieder de-anonymisiert werden können. Das ist manchmal illegal, aber leider auch oft legal.

[31] https://digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/

[32] https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales



https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

Die Firma Segment

Einen besonderen Stellenwert nimmt die Firma Segment ein (https://segment.com/). Diese hat den Markt von über 100 solcher Tool-Anbieter noch mal in einen Service zusammengefasst, sodass ein Web-Entwickler diese Services nicht einzeln in seine Webseite integrieren muss. Somit kann ein Web-Entwickler die gewonnen Daten ohne Aufwand an über 100 Firmen gleichzeitig weitergeben. Die Übersicht dieser

„Dienstleister“ gibt auf der Seite von Segment unter https://segment.com/integrations einen guten Überblick über den Markt dieser „Dritt-Anbieter“.
Der Anwender stellt manchmal verwundert fest, dass er im Browser plötzlich Werbung aus einer Produktkategorie angezeigt bekommt, nach der er sich Vortags im Internet erkundigte. Das sind Auswirkungen von Online-Tracking. Der Anwender war zuvor auf einer anderen Webseite die solche Tracker enthielt. Diese Tracker sammeln Nutzerprofile und verkaufen diese an Werbetreibende. Folgende Tausenderkontaktpreise sind für solch gezielten Adressinformationen üblich, wobei im Internet eine „Adresse“ auch der Fingerabdruck des Browsers sein kann:

	Adressen	Beschreibung	Preis pro T.
Die Zeit	55.900	Shopkäufer und Buchserienkäufer	€ 210,00
RTL Club	510.000	aktive Kunden	€ 180,00
Elderly & Disabled	110.000	Spender	€ 175,00
Tag des Herrn	52.400	Abonnenten katholische Wochenzeitung	€ 170,00
Lehrer	246.100	mit Privatanschrift	€ 170,00
Lehrer	367.700	mit Schulanschrift	€ 170,00
Die Zeit	374.000	aktuelle Leser und ehem. Abonnenten	€ 160,00
Passive Ältere	3.051.100	Adressen gesamt	€ 155,00
Versa Distanzhandel	55.700	aktive Käufer 0-6 Monate (Beate Uhse)	€ 150,00
Gewinnspielteilnehmer	215.500	Gewinnspielteiln. Drogerieartikel	€ 150,00
Große Tageszeitung	2.155.000	Werbedatei einer großen Tageszeitung	€ 110,00

CC BY-SA 3.0 Cracked Labs

Beispiele für von *AZ Direkt/Bertelsmann* im Online-Katalog angebotene Adressen (11/2014)

Oder der Gesamtkatalog der Bertelsmann Tochter Arvato:
http://www.az-direct.com/site/blaetterkatalog/listinfos/
Solche zielgerichtete Werbung wird oftmals als harmlos eingestuft und von vielen Internet-Nutzern sogar gewünscht.

Welchen Schaden können Tracker-Daten anrichten?

Neben der zielgerichteten Werbung werden diese über den Internet-Nutzer gewonnen Informationen auch für Dinge genutzt, die dem Nutzer sogar schaden können. Hier ein paar Beispiele, für welche Zwecke diese persönlichen Informationen gerne auch verwendet werden:

- „Bonitätsbewertung mittels Online-Daten“ wird gerne von Shops genutzt. Beispielsweise bietet das Unternehmen ZestFinance dazu Bonitätsinformationen an[33].
- „Personalentscheidungen auf Basis Big Data Auswertungen“ werden gerne von Personalabteilungen genutzt. Das Unternehmen Cornerstone hält dafür Ihre Daten bereit[34], und

33 http://www.zestfinance.com

34 http://www.cornerstoneondemand.com

ConnectCubed[35] kann sogar die Leistungsfähigkeit der zukünftigen Mitarbeiter voraussagen[36].

- „Preisdiskriminierung“ ist heute schon Realität[37]. Hierbei fordert ein Anbieter für die gleiche Leistung von Interesssenten und Kunden unterschiedliche Preise je nach deren Bildungsstand, Wohnort, Clubzugehörigkeit etc. Google hat auf eine Art der Preisdiskriminierung ein Patent angemeldet[38]. Firmen wie [39]HCL und SO1 [40] nutzen moderne KI (künstliche Intelligenz) Methoden, um aus Informationen des Kaufinteressenten den optimalen Preis zu errechnen. Auf der „University of Minnesota“ gibt es sogar einen eigenen Studiengang „Marketing Analytics Program“ in dem speziell diese Methoden gelehrt werden[41].

  Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) hat jedoch in einer groß angelegten Studie keinen Beleg dafür gefunden, dass „..für ein Laptop, eine Waschmaschine oder eine Reise scheinen die Deutschen bei demselben Anbieter einen identischen Preis zu zahlen – unabhängig vom Wohnort, von Datenschutzeinstellungen oder vom Log-In mit einem Nutzerkonto..“ [42],[43]

- „Krankheitsprognosen aus Konsumverhalten“ werden von Versicherungen getestet[44].

- Da man mit Profildaten sehr viel Geld verdienen kann, kann man dieses Geld auch wieder dafür einsetzen, Medien zu beeinflussen. So schreibt netzpolitik.org über Google: „Mit 150 Millionen Euro will der US-Konzern Innovationen im europäischen Journalismus fördern. Seit Anfang 2016 beschenkt er deshalb hunderte Medienunternehmen, Verlage, Start-Ups, Einzelpersonen und Universitäten in Europa“.

[35] http://connectcubed.com/

36 http://connectcubed.com

37 http://www.zeit.de/wirtschaft/2014-10/absolute-preisdiskriminierung

38 http://www.tagesspiegel.de/medien/digitale-welt/verbraucherschutz-ein-individueller-preis-fuer-jeden/8353500.html

[39] https://www.hcltechsw.com/wps/portal/about/welcome

[40] https://www.so1.ai/

[41] https://www.d.umn.edu/unirel/homepage/11/retailmarketing.html

[42] https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/Schlussbericht_Empirie.pdf?__blob=publicationFile&v=1

[43] https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2021/0311_Studie_personalisierte_Preise.html

44 http://www.wsj.com/articles/SB10001424052748704648604575620750998072986

https://netzpolitik.org/2018/news-initiative-wohin-googles-millionen-fuer-die-medien-in-deutschland-fliessen/

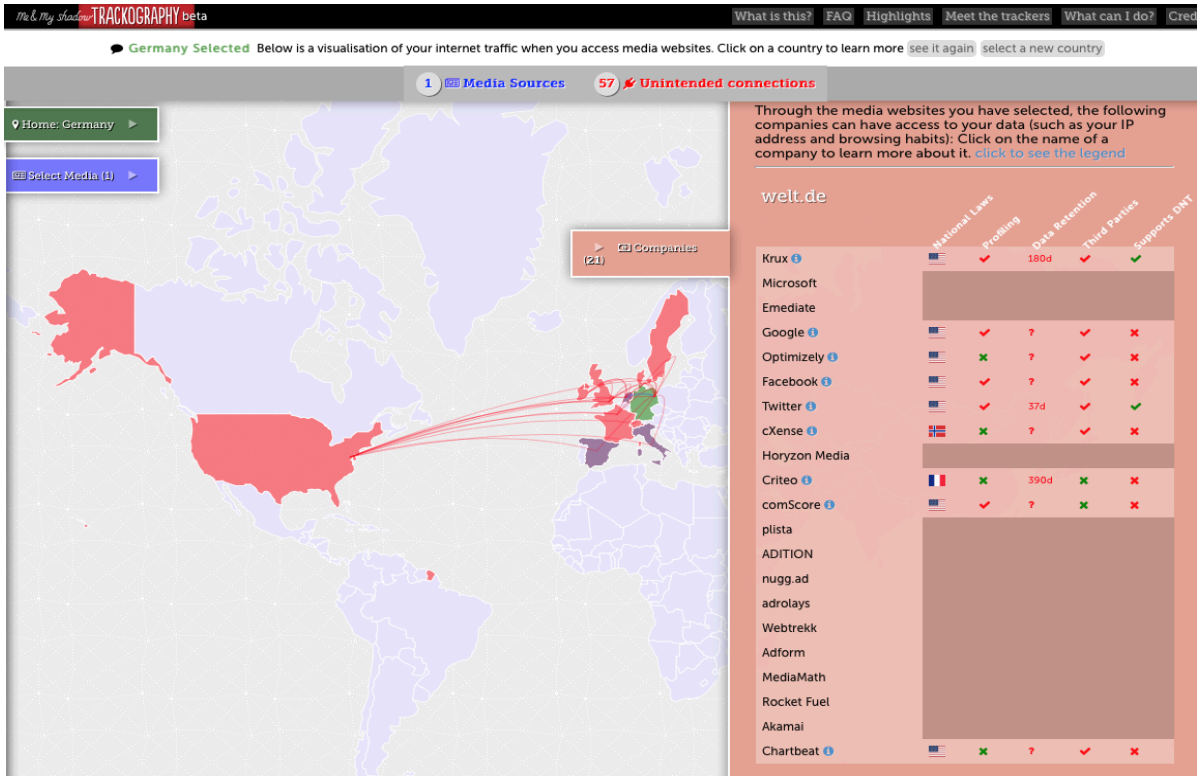
Es kann aber auch durchaus sein, dass der Nutzer (oder dessen Kinder) auch noch in 20 oder 30 Jahren mit Daten aus seinem Leben konfrontiert werden, die er selbst schon längst vergessen hat. Denn diese Daten-Sammel-Firmen vergessen nie etwas. Vor allem Kinder und Jugendliche, die heute meist sehr unbekümmert Datenspuren hinterlassen, können in vielen Jahren mit diesen Informationen konfrontiert werden[45]. Eventuell sogar ohne dass sie es merken, wenn sie z.B. eine Versicherung abschließen und dafür mehr bezahlen müssen als andere, oder eine Job-Bewerbung mit fadenscheinigen Gründen abgelehnt wird.

Mancher mag denken: „wie gut, dass ich in Deutschland lebe, da gibt es die besten Datenschutzgesetze“. Leider nützen die deutschen Datenschutzgesetze hier nur wenig. Sobald eine deutsche Tageszeitung im Internet aufgerufen wird, werden automatisch viele Daten-Tracker Programme mit aufgerufen. Das ist so in den Webseiten fast aller Medienunternehmen, auch bei deutschen Zeitungen und Zeitschriften, programmiert worden. Das Internet Tool „Trackography”[46] zeigt sehr gut aufbereitet, in welche Länder Nutzerdaten fließen und welchen rechtlichen Bestimmungen diese Länder unterworfen sind. Natürlich fließen die meisten Daten in die USA, da Facebook und Google am meisten genutzt werden und auf den meisten Medienseiten in irgendeiner Weise eingebunden sind.

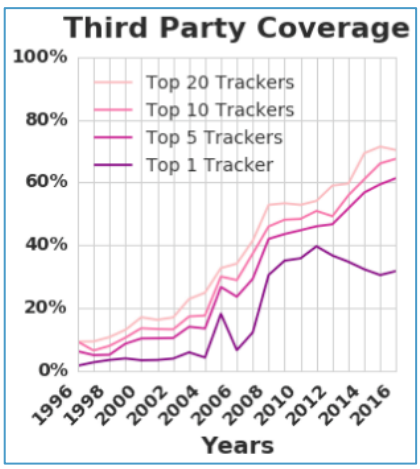
Hier ein Beispiel des Medienportals der Zeitschrift „welt.de“; 21 weitere Firmen greifen ebenfalls gleichzeitig auf diese Nutzer-Tracking-Daten zu, die wiederum in die Länder Finnland, Dänemark, Italien, USA, Spanien, Italien, Niederlande, Großbritannien, Frankreich und in die Schweiz weitergeleitet werden (Stand 2021).

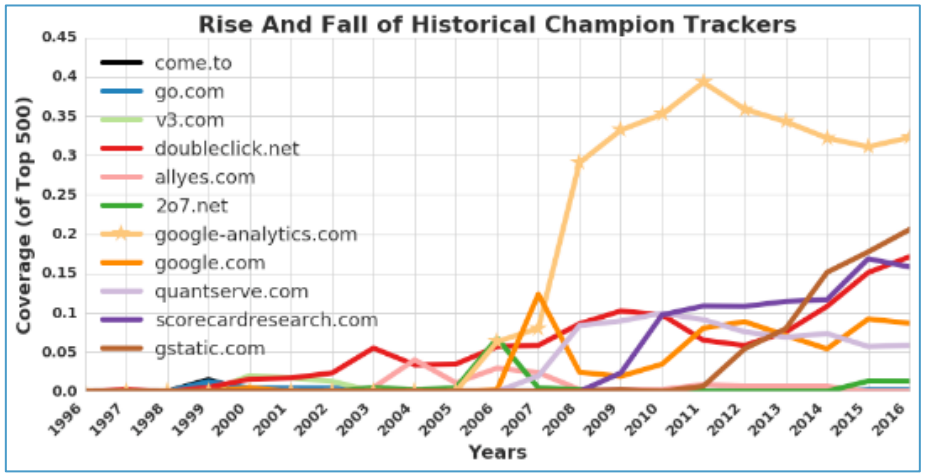
45 https://openstandard.mozilla.org/whos-collecting-kids-personal-data-lots-of-people/

46 https://trackography.org



Aber Nutzerdaten können auch in Länder gehen, die keine Datenschutzgesetze haben, wie z.B. nach Indien oder China. Was dort mit diesen Daten geschieht, ist meist nicht mehr nachvollziehbar.
Des Weiteren sollte man auch nie vergessen, dass alle diese von Daten-Trackern gesammelten Daten auch gerne von Kriminellen und Geheimdiensten in diesen Ländern abgefischt werden.
Aber nicht nur beim Browsen im Internet sammeln kommerzielle Firmen Daten über uns. Gerade erst hat Microsoft die Datensammelwut von Windows 10 erläutert[47].
Wie sich das Tracking im Internet über die letzten 20 Jahre entwickelt hat, haben Forscher der University of Washington analysiert[48]:





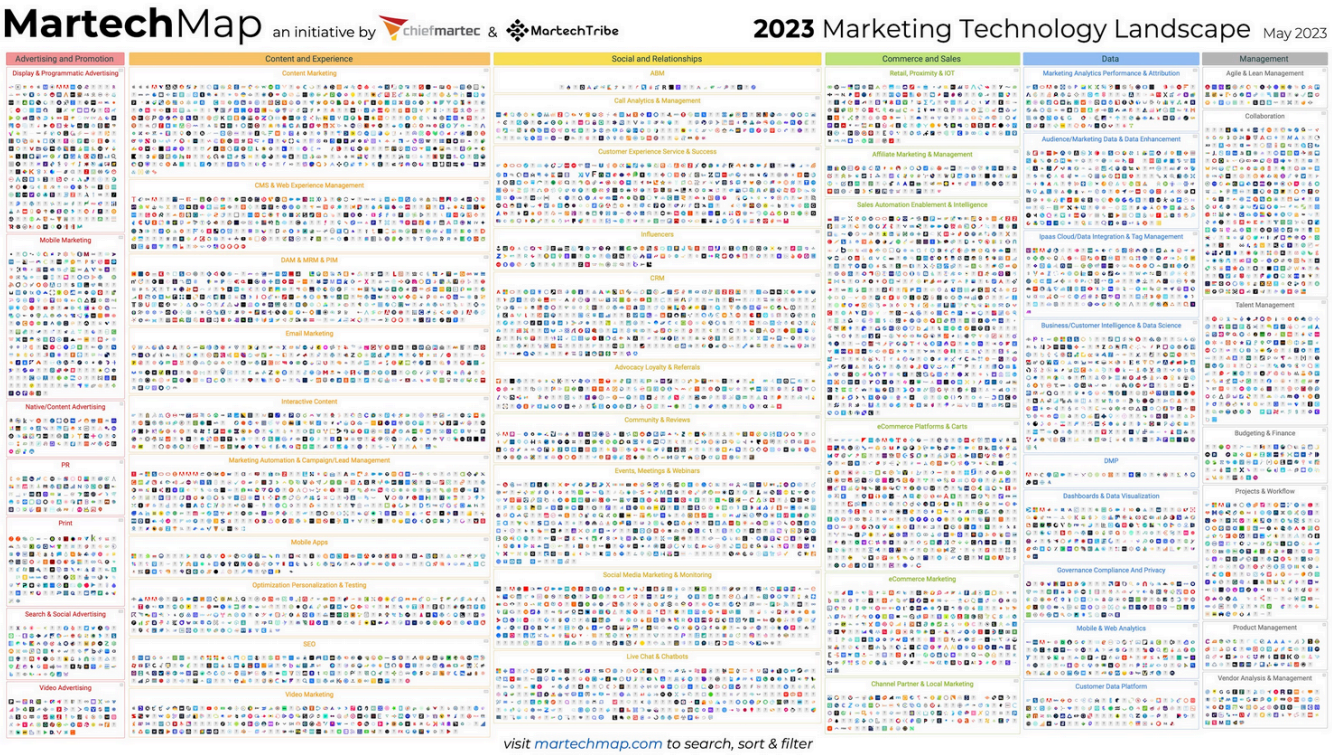
[47] https://www.heise.de/newsticker/meldung/Creators-Update-Microsoft-erlaeutert-die-Datensammelwut-von-Windows-10-3675978.html

[48] https://trackingexcavator.cs.washington.edu/InternetJonesAndTheRaidersOfTheLostTrackers.pdf

https://trackingexcavator.cs.washington.edu/InternetJonesAndTheRaidersOfTheLostTrackers.pdf

Werbung im Internet

Wie aus obiger Tabelle erkennbar ist, kann Internet-Werbung auch für die Angriffsart „Adware“ (Malvertising) genutzt werden.
Werbung im Internet ist ein Milliardenmarkt. Nicht nur die Marktführer Google und Facebook verdienen sich mit diesem Geschäft (und unseren Daten) eine goldene Nase. Allein im letzten Quartal 2019 hat alleine Facebook 21 Milliarden US$ fast ausschließlich durch Werbeeinnahmen generieren können.
Egal was wir im Internet machen, ob Videos über Youtube schauen, ob eine Apps auf dem Smartphone benutzen oder im Internet eine kostenlose Ausgabe einer Zeitschrift lesen, alles wird mit Werbung finanziert.
Mit Werbung finanziert? Um es genauer zu sagen, mit unseren Daten finanziert. Die Werbung, die wir sehen, ist nur die Spitze des Eisbergs. Zwischen dem Abrufen einer Seite oder dem Anklicken einer App werden komplexe Abläufe angestoßen, die beim Anbieten der Werbefläche und des Profils des Benutzers anfangen, über Versteigerungs-Plattformen dieser beiden Werte einen Käufer unter den Werbetreibenden finden, letztendlich die Werbung auf dem Bildschirm anzeigen, oder auch nur den Anbieter des Nutzerprofiles vergüten. Und das alles geschieht in Millisekunden unbemerkt vom Nutzer.
Diese (unvollständige) Grafik von über 11.000 Marketing Technology-Firmen zeigt, wie komplex und unübersichtlich der Markt mittlerweile geworden ist:



Quelle: https://chiefmartec.com/2023/05/2023-marketing-technology-landscape-supergraphic-11038-solutions-searchable-on-martechmap-com/

Eine Studie ergab, dass es ca. 81.000 Online Tracking Dienste gibt! Aber nur 123 dieser Dienste den Markt dominieren [49]. Alle diese Dienste haben sich erst über die letzten Jahre etabliert und werden unter anderem über Werbung bezahlt. Der „Chief Marketing Technologist Blog“[5051] beschreibt sehr detailliert wie der Markt in die verschieden spezialisierten Firmen aufgeteilt ist.
Viele Nutzer sind der Meinung, dass Zielgerichtete Werbung doch nichts verwerfliches sein kann und viele Nutzer haben nichts gegen Werbung im Internet. Aber Werbung hat auch Nachteile und birgt sogar Gefahren:

- Um Werbung möglichst den Interessen des Nutzers anzupassen, benötigt man Wissen über die Interessen des Nutzers. Und dieses Wissen über den Nutzer kann und wird auch zum Nachteil des Nutzers verwendet. Siehe Kapitel „Welchen Schaden können Tracker-Daten anrichten?“.

- Während eine durchschnittliche Wikipedia-Seite, also eine Seite ohne Tracker und ohne Werbung, ca. 20 Zugriffe auf den Server benötigt, um alle Daten in den Browser zu laden, benötigt eine Boulevard-Zeitschrift mitunter 200-400 Zugriffe auf bis zu 100 verschiedene Servern. Dabei werden nicht nur Werbe-Banner zusätzlich geladen, sondern auch eine riesige Menge zusätzlicher Tracker-Codes. Dieser zusätzliche Overhead verzögert den Seitenaufbau und generiert gerade bei einem Internet-Zugang, den man für den verbrauchten Trafik bezahlen muss (also bei jedem mobilen Zugriff), auch zusätzliche Kosten für den Nutzer.

- Wenn man eine Webseite abruft oder eine App startet, dann interessiert man sich für den angebotenen Inhalt. Auf diesen möchte man sich konzentrieren. Werbung lenkt vom eigentlichen Inhalt ab, und oft muss man Werbung auch noch mühselig wegklicken. Dies generiert in der Summe einen nicht unerheblichen ökonomischen Schaden.

- Über Werbenetzwerke werden auch Schädlinge verteilt[52],[53]. Dieses Vorgehen wird Malvertising[54] genannt.

Malvertising, also das Versenden von Malware über Werbe-Netzwerke, ist besonders effektiv, da der Angreifer sich gut verstecken kann und die Zielgruppe seines Angriffs sehr genau adressieren kann. Er kann solche Schädlinge z.B. nur an eine bestimmte Berufsgruppe oder an besonders zahlungskräftige Personen verteilen; oder nur an jeden, der eine bestimmte Browser-Version mit einem bekannten „Exploit“ beinhaltet (ein Bug, der sich besonders dafür eignet, illegal in ein System einzudringen[55]). 2015 wurden alleine im Firefox Browser über 7.000 Bugs festgestellt, davon über 100 sicherheitskritische Bugs. Dazu muss ein Angreifer noch nicht einmal einen teuren Zero-Day-Exployt[56] einkaufen. Ein weiterer Vorteil für Angreifer bietet Malvertising dadurch, dass der Angreifer keine eigene Infrastruktur für

[49] http://www.sueddeutsche.de/digital/internet-dienste-dominieren-das-online-tracking-1.2998244

[50] http://chiefmartec.com/2015/01/marketing-technology-landscape-supergraphic-2015/

[51] http://chiefmartec.com/2016/03/marketing-technology-landscape-supergraphic-2016/

[52] http://thehackernews.com/2014/06/deviantart-malwaretising-campaigns-lead.html

[53] https://www.bleepingcomputer.com/news/security/russian-methbot-operation-makes-up-to-5-million-per-day-from-click-fraud/

[54] https://en.wikipedia.org/wiki/Malvertising

[55] https://en.wikipedia.org/wiki/Exploit_(computer_security)

[56] https://de.wikipedia.org/wiki/Exploit#Zero-Day-Exploit

die Verteilung des Schädlings benötigt. Das übernimmt das Werbenetzwerk für ihn. Des Weiteren erlauben Werbenetzwerke, die beliebige Verteilung von Codes: Flash, JS, Java, animierte GIFs…
Das ist möglich, da in der Regel niemand in der Auslieferkette des Werbebanners die Daten auf Schadsoftware kontrolliert.
Wie einfach es ist, einen solchen Malvertising Schädling zu entwickeln und in Umlauf zu bringen, haben Thorsten Schröder & Frank Rieger auf der re:publica 2016 demonstriert[57]. Auf dem Markt gibt es Werkzeuge (z.B. Metasploit), mit deren Hilfe es auch ohne tiefgreifende technische Kenntnisse möglich ist, Schadsoftware automatisch zu generieren.
Mit Malvertising werden selbst renommierte Webseiten zum Gehilfen krimineller Angreifer. Über die Server von AOL, BBC, MSN wurden schon Erpressungs-Trojaner mit Hilfe von Werbeeinblendungen verteilt. Von Angriffen dieser Art Schädlinge können alle Betriebssysteme und auch Smartphones betroffen werden. Selbst MACs, die in der Regel weniger von Angriffen bedroht sind, können mit Malvertising geschädigt werden[58].

Echtzeit-Versteigerung von Werbeflächen

Es ist heute üblich, die Werbeanzeige unsichtbar und noch während die Webseite geladen wird innerhalb weniger Millisekunden automatisch zu versteigern. Das Verfahren wird „Real Time Bidding“ (RTB) genannt. Um jedoch Werbung wirklich zielgerichtet zu automatisieren, hat sich für den dafür notwendigen Gesamtprozess der Begriff „Programmatic Advertising“[59] etabliert.
Dazu wird über ein riesiges und kaum durchschaubares Geflecht von Dienstleistern die Werbefläche und das Profil des Nutzers der Webseite in den Werbe-Versteigerungs-Netzwerken angeboten, und der Höchstbietende darf auf genau diesem einen Browser seine Werbung anzeigen.
Im Fachjargon ausgedrückt: dieses Real Time Bidding, auch Real-Time-Advertising (RTA) genannt, ist ein Verfahren, mit dem Werbetreibende (z.B. eine Zeitschrift im Internet) bei der Auslieferung von Online-Werbemitteln automatisiert und in Echtzeit (engl. real time) auf Werbeplätze bzw. „Ad Impressions“ im Internet bieten können. Pro Ad-Impression[60] wird das Werbemittel des jeweils Höchstbietenden ausgeliefert[61].

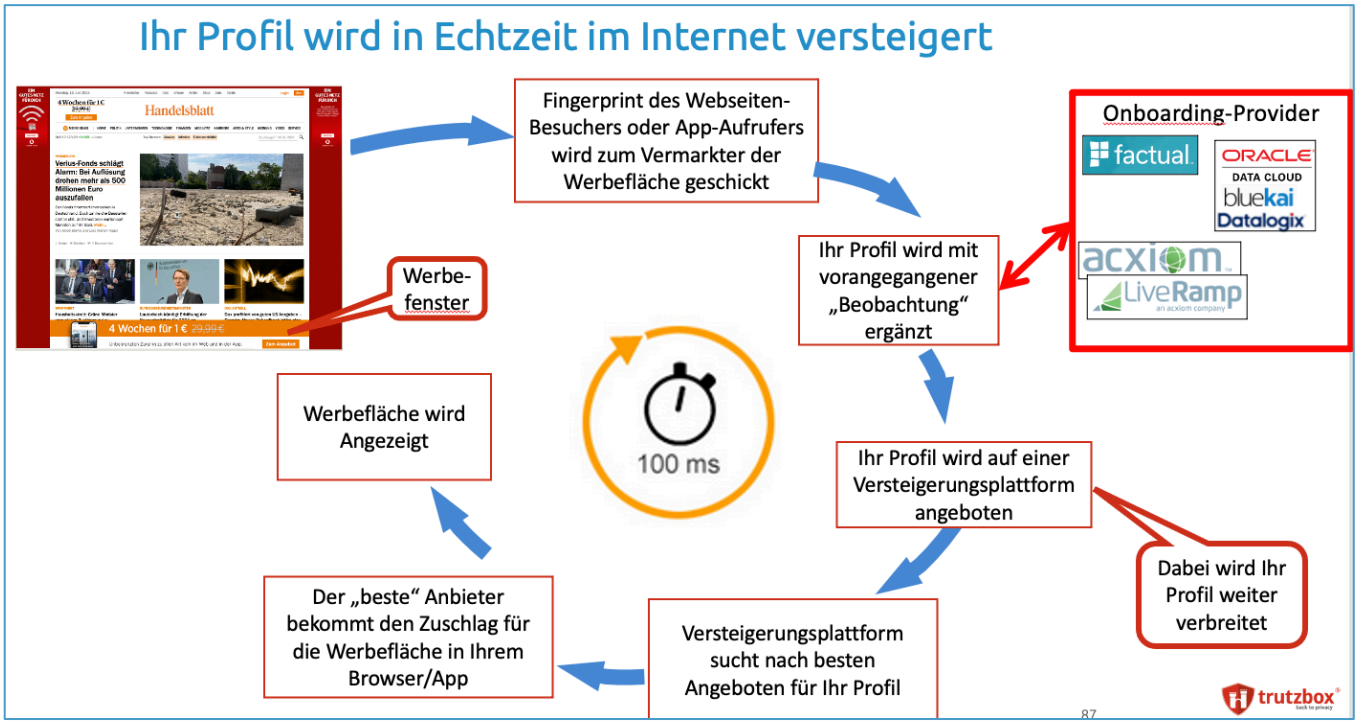
[57] https://www.youtube.com/watch?v=zJUmjtjCtY8

[58] https://blog.confiant.com/confiant-malwarebytes-uncover-steganography-based-ad-payload-that-drops-shlayer-trojan-on-mac-cd31e885c202

[59] https://de.wikipedia.org/wiki/Programmatic_Advertising

[60] https://de.wikipedia.org/wiki/Ad_Impression

[61] https://de.wikipedia.org/wiki/Real_Time_Bidding



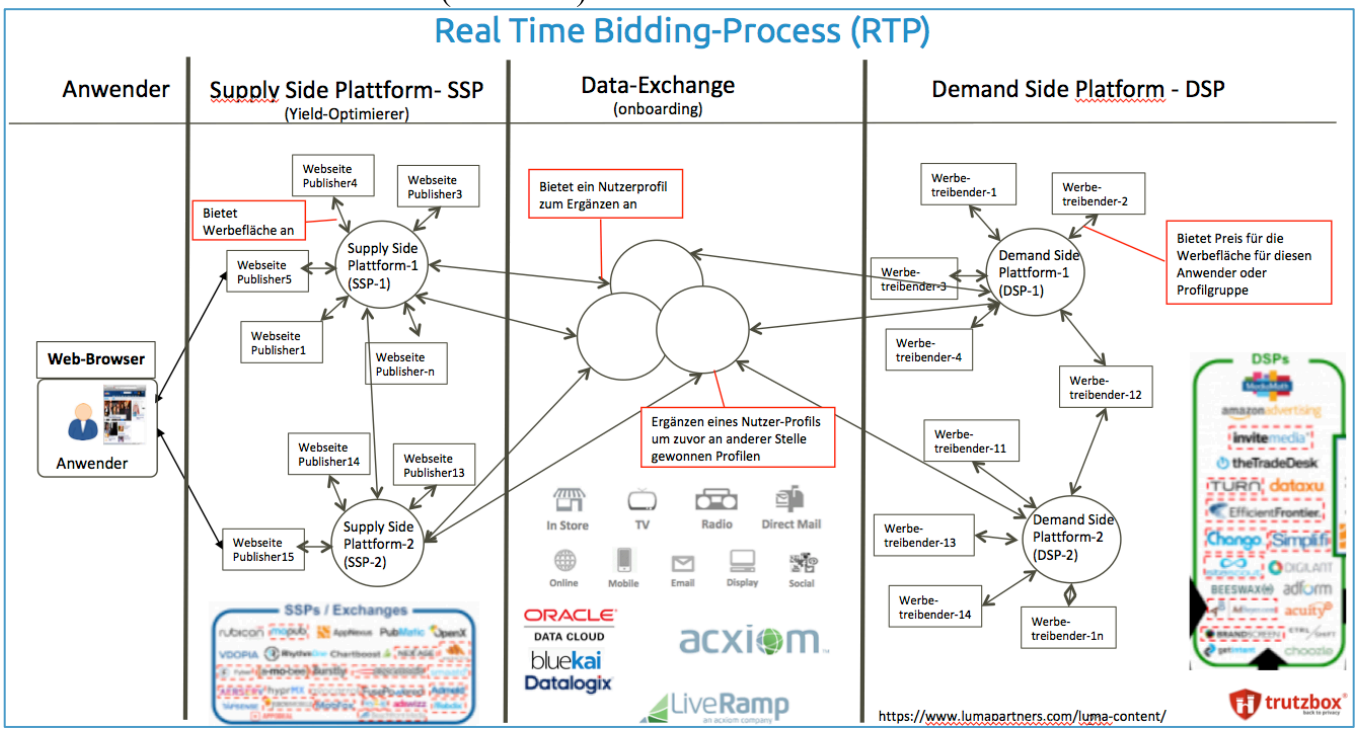
(© 2023 Comidio GmbH)

Da der gebotene Preis für eine Werbefläche vom Profil des Nutzers abhängt, wird dem Benutzer das Profil der besuchten Seite zugeordnet. Falls der Nutzer vom gleichen Tracker „wiedererkannt wird“, dann wird sein Profil jetzt um die besuchte Seite ergänzt.
Die Werbefläche und das Profil des Besuchers wird zunächst einer „Sell Side Platform“ (SSP) höchstbietend zur Versteigerung angeboten. Sell Side Platform (SSP) oder auch Supply Side Plattform ist ein Begriff aus dem automatisierten Handel im Onlinemarketing. Es bezeichnet eine Technologie, die es einem Publisher erlaubt, sein Inventar für ihn möglichst gewinnbringend Ad-Exchanges und Werbetreibenden anzubieten[62].
Aber auch das Bieten eines Preises für dieses Profil und Werbeplatzes funktioniert automatisch: jetzt sendet die SSP eine Anfrage an eine „Demand Side Platform“ DSP sowie die angebundenen Ad Networks. In einem DSP haben sich Werbetreibende angeschlossen, die für ihre Kunden Werbung schalten möchten. Sie bedienen die Nachfrageseite und agieren als Dienstleister für Advertiser und Agenturen[63].
Diesen DSPs werden ein Werbeplatz sowie das Nutzerprofil angezeigt. In Bruchteilen einer Sekunde überprüft das System automatisch, ob das angezeigte Nutzerprofil zu den Zielgruppenparametern passt, die der Werbetreibende zuvor festgelegt hat und gibt ein entsprechend hohes oder niedriges Gebot ab. Die SSP sammelt alle Gebote, und das Werbebanner des Höchstbietenden wird schließlich angezeigt. Zwischen SSP und DSP sind gelegentlich weitere Dienstleister geschaltet, die beispielsweise das „Onboarding“ übernehmen.

[62] http://www.digitalwiki.de/ssp-sell-side-platform/

[63] http://www.digitalwiki.de/dsp-demand-side-platform/

Onboarding bezeichnet den Prozess, ein bestehendes Nutzerprofil um weitere Profile aus anderen Daten zu erweitern und somit wertvoller zu machen. Dies können auch Daten aus dem realen Leben eines Nutzers sein, die zuvor beispielsweise bei einem nicht anonymen Einkauf von einem Nutzer gewonnen wurden. Wie das technisch funktioniert wird im Kapitel „Wie werden Internet-Tracking Daten mit gesammelten Daten aus dem Alltag verknüpft?“ beschrieben. Ein Unternehmen, das Advertiser und Publisher verbindet ist z.B. die Firma Awin (awin.com).



(© 2015 Comidio GmbH)

Diese Beschreibung ist eine recht vereinfachte Darstellung der Prozesse und Mitspieler in dem komplexen Prozess des Online-Marketings. In der Realität spielen viele weitere Faktoren eine Rolle, wie z.B. Klicks, Leads, Sales und Orders. Es haben sich hunderte von zusätzlichen Dienstleistungs-Unternehmen etabliert, die sich auf die Erfolgsmessung von Optimierung von Online-Marketing spezialisiert haben. Diese Beschreibung soll lediglich einen ersten Eindruck vermitteln, was sich hinter den Kulissen eines Werbebanners, einem „Werbe-Vorfilm“ in Youtube oder einer Werbe-Mail abspielt.
Ein grosses Problem bei dieser Versteigerung von Werbefläche ist auch, dass dabei unserer Daten vielen Firmen angeboten werden. Somit bekommen unsere Daten nicht nur die Firma, die den Zuschlag für die 5 Sekunden Werbung erhält, sondern alle Firmen die an der Versteigerung teilnehmen. Und das sind meist wieder Firmen, die dadurch ihren Datenbestand über uns ergänzen können. Das führt dann zu einer „Diffusion“ unserer Trackingdaten. Die Streuung wurde in einer recht interessanten Studie mit dem Titel „Diffusion of User Tracking Data in the Online Advertising Ecosystem“[64] untersucht.

Facebook und Google behaupten immer wieder, dass sie unsere Profildaten weder verkaufen, noch sonst wie an Dritte weitergeben. Da beide Firmen jedoch bei einer Versteigerung von Werbeflächen unsere

[64] https://www.petsymposium.org/2018/files/papers/issue4/popets-2018-0033.pdf

Profile den Bietern preisgeben, stimmt diese Aussage nicht. Deswegen hat ein Konsortium mehrerer Firmen ein Klageverfahren in USA gegen Google angestoßen. In der Klageschrift gibt es eine Grafik die der Heiseverlag unter dem Artikel „Verräterische -Datenflüsse - Googles Geschäftsmodell unter Druck“ veröffentlichte. Die Grafik zeigt auch die Daten, die Google weitergibt. Dabei sind neben Daten, die eindeutig die Person identifizieren können, auch sehr private Daten, wie Abstammung, sexuelle Orientierung, finanzielle Verhältnisse, Krankheiten und Beziehungsstatus.

(https://www.heise.de/select/ct/2021/10/2109613171135837656)

Das gleiche Thema hatte im April 2021 auch das Wall Street Journal beschrieben.[65]

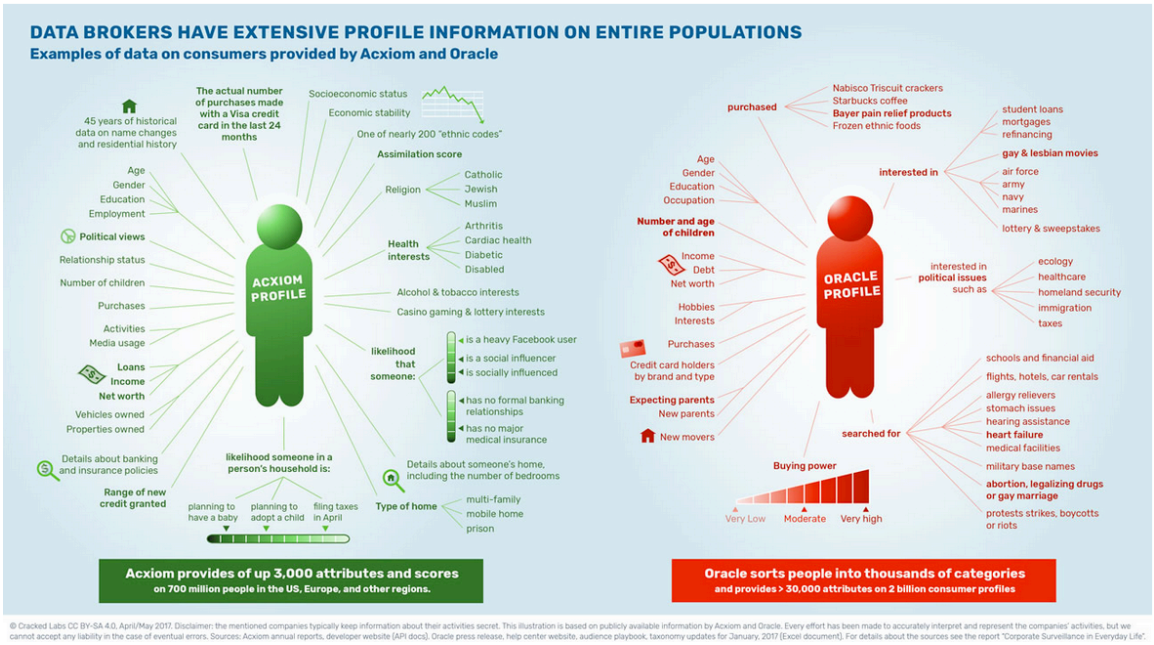
[65] https://www.wsj.com/articles/u-s-senators-ask-digital-ad-auctioneers-to-name-foreign-clients-amid-national-security-concerns-11617393964

Eine recht gute Marktübersicht über DSP-, SSP-Anbieter, die auch in Deutschland vertreten sind und Publisher welche SSP nutzen, gibt „programmatic beef“[66].
Vor allem Onboarding-Dienstleister haben im Zusammenspiel hier eine entscheidende Rolle. Sie verknüpfen die aktuell gewonnen Profile mit den schon zuvor gewonnen Profilen aus anderen Datenquellen. Diese können auch aus dem täglichen off-Line Leben stammen. Z.B. Kunden-Bindungs-Karten (Loyalty-Karten), Geo-Datenbanken usw. werden hier untereinander verknüpft. In der LUMAscape Übersicht sind die Firmen mit Audience/Market Data & Data Enhancement bezeichnet:

aus http://www.lumapartners.com/resource-center/lumascapes-2/

Die beiden größten Unternehmen, die sich in den letzten Jahren auf das „anzapfen“, „veredeln“ und den Verkauf von Verbraucher-Daten etabliert haben, sind Oracle und Acxiom. Dabei sammelt und veredelt Acxiom vor allem Daten aus der Onlinewelt, während sich Oracle zusätzlich auch auf das Sammeln von Profile-Daten der realen (offline) Welt konzentriert.

[66] http://www.programmaticbeef.de/wordpress/marktuebersicht/



Source: crackedlabs.org/en/corporate-surveillance

Neben der technischen Systeme für Real-Time-Bidding, kostet Programmatic Advertising zusätzlich Geld für die Bedienung der Systeme, Testbudgets, Designer, Programmierer für aufwändige Banner, Videoproduzenten Abrechnungs- und auch noch technische-Dienstleister[67].
Die wichtigste Erkenntnis für den Anwender ist: selbst wenn der Tracker an vorderster Front im Browser (der den Fingerabdruck des Nutzers ermittelt) verspricht, sich an alle gesetzlichen Regeln zu halten und die Daten zu anonymisieren, er diese „anonymen Daten“ oft an andere Verwerter weiter gibt, diese Daten immer und immer wieder um weitere Daten ergänzt werden und dadurch über viele Umwege de-anonymisiert werden können.
Dass die Zusammenarbeit der Werbe- mit der Tracking-Industrie erst am Anfang steht, zeigen die Themen, die bei für diese Branche organisierten Treffen „Tracks-Summit“ besprochen werden: https://www.tracks-summit.de/.

Diese Industrie behauptet immer, dass die kostenlosen Internet-Dienste, die wir alle täglich nutzen, nur durch Werbung finanzierbar wären. Diese Aussage ist allerdings bereits eine reine Werbe-Aussage, denn wenn man sich die Gewinn-Verteilung dieser Tracking-Industrie anschaut, dann wird offensichtlich, dass nur ein sehr kleiner Teil bei den Diensten, die wir gerne kostenlos nutzen, hängen bleibt. Die meisten Gewinne verbleiben bei den großen internationalen Tracking-Firmen, die im Hintergrund agieren. Nur ein winziger Bruchteil dieser Milliardeneinnahmen geht z.B. an die deutsche Medienindustrie.
Und Werbung wird dann gefährlich, wenn sie als solche nicht mehr erkennbar ist. Also versteckte Werbung, auch Schleichwerbung genannt. Und die gibt es im Internet mittlerweile überall, obgleich laut §5a VI Gesetz gegen den unlauteren Wettbewerb (UWG), Schleichwerbung in Deutschland verboten ist.
In diesem Video erklärt Johnny Rayn recht gut wie Echtzeit-Versteigerungen von Werbeflächen im Internet funktionieren: https://vimeo.com/317245633.

Die Initiative „StopSpyingOnUs ist der Meinung, dass „…mittels Real-Time Bidding ("Echtzeitbieten") und durch das Googles Werbesystem 'Authorized Buyers' die personenbezogenen Daten der Nutzer an

[67] http://www.programmaticbeef.de/wordpress/butter-ans-beef-was-kostet-programmatic-advertising/

Hunderte, wenn nicht Tausende von Unternehmen übertragen werden können“ und wirbt um Unterstützer, die mit ihnen gegen diese Machart vor gehen: https://www.liberties.eu/de/campaigns/stopspyingonus-fixad-tech-kampagne/307.

Werbung ist Bestandteil unseres Lebens und wichtig für Unternehmen. Aus diesem Grund verhindert die TrutzBox in den Standard-Einstellungen auch keine Werbung. Aber Werbung muss nicht gleich Tracking sein. Dass der Nutzer von Firmen beobachtet, profiliert wird und mit diesen Profilen gehandelt wird, das möchten die meisten Internet-User nicht, und das verhindert die TrutzBox. Siehe dazu auch den Artikel der Firma EmVolution „warum Werbeprofile der Kuhhandel des 21 Jahrhunderts sind“[68].

[68] https://blog.emvolution.me/2016/07/warum-werbeprofile-der-kuhhandel-des-21-jahrhunderts-sind/

Geheimdienste

Neben diesen Daten-Sammel-Firmen haben auch **Geheimdienste** großes Interesse an jeglichem Datenverkehr. In den meisten demokratischen Ländern dürfen Geheimdienste eigentlich nur im Ausland aktiv werden, da im eigenen Land andere staatliche Stellen zuständig sind. Im eigenen Land dürfen Geheimdienste allerdings auch „Ausländer" überwachen. Wer allerdings Ausländer ist, und wie Kommunikation von „Ausländern" überhaupt erkannt werden soll, ohne den gesamten Datenverkehr zu überwachen, bleibt ungeklärt. Somit zeigt die Praxis, dass sich Geheimdienste im eigenen Land entweder nur eingeschränkt an Gesetze halten bzw. diese nach ihren Bedürfnissen auslegen. Und sie lassen sich kaum kontrollieren, da alle Aktivitäten ja geheim sind. Selbst parlamentarische Untersuchungsausschüsse haben es schwer, Informationen über geheimdienstliche Aktivitäten zu erhalten. Somit ergibt es sich, dass sich Geheimdienste sowohl im eigenen Land als auch im Ausland oft wenig an rechtliche Beschränkungen halten.[69]
Ein Artikel von Netzpolitik.org bringt es auf den Punkt[70]:

„Auf Deutsch: Der Geheimdienst hält sich nicht an das Gesetz – oder hat zumindest eine sehr eigene und geheime Interpretation davon. Das reiht sich nahtlos ein in weitere eigentümliche Rechtsauffassungen wie Weltraumtheorie (Satelliten sind im Weltraum, also gelten beim Abhören keine deutschen Gesetze), Funktionsträgertheorie (Grundrechtsträger können ihre Grundrechte in bestimmter Funktion verlieren) und geheime, illegale Datenbanken." (Grundrechtstrp://www.zeit.de/politik/deutschland/2014-11/bnd-bundesnachrichtendigeheime, illegale Datenbanken."

Aus einem geheimen Gutachten der ehemaligen Bundesdatenschutzbeauftragten Andrea Voßhoff geht hervor, dass der deutsche Bundesnachrichtendienst (BND) im Verdacht steht, bei Abhöraktionen systematisch gegen Bestimmungen des Datenschutzes verstoßen zu haben[71],[72].
Geheimdienste zapfen das Internet an zentralen Internet-Daten-Austauschpunkten an, oder sogar Überseekabel[73] über die der weltweite Internetverkehr abgewickelt wird. Allein der amerikanische Geheimdienst NSA betreibt Datenaustauschpunkte, die weltweit an ca. 150 Standorten positioniert sind[74].

[69] http://www.spiegel.de/politik/deutschland/ueberwachung-neue-spionageaffaere-erschuettert-bnd-a-1030191.html

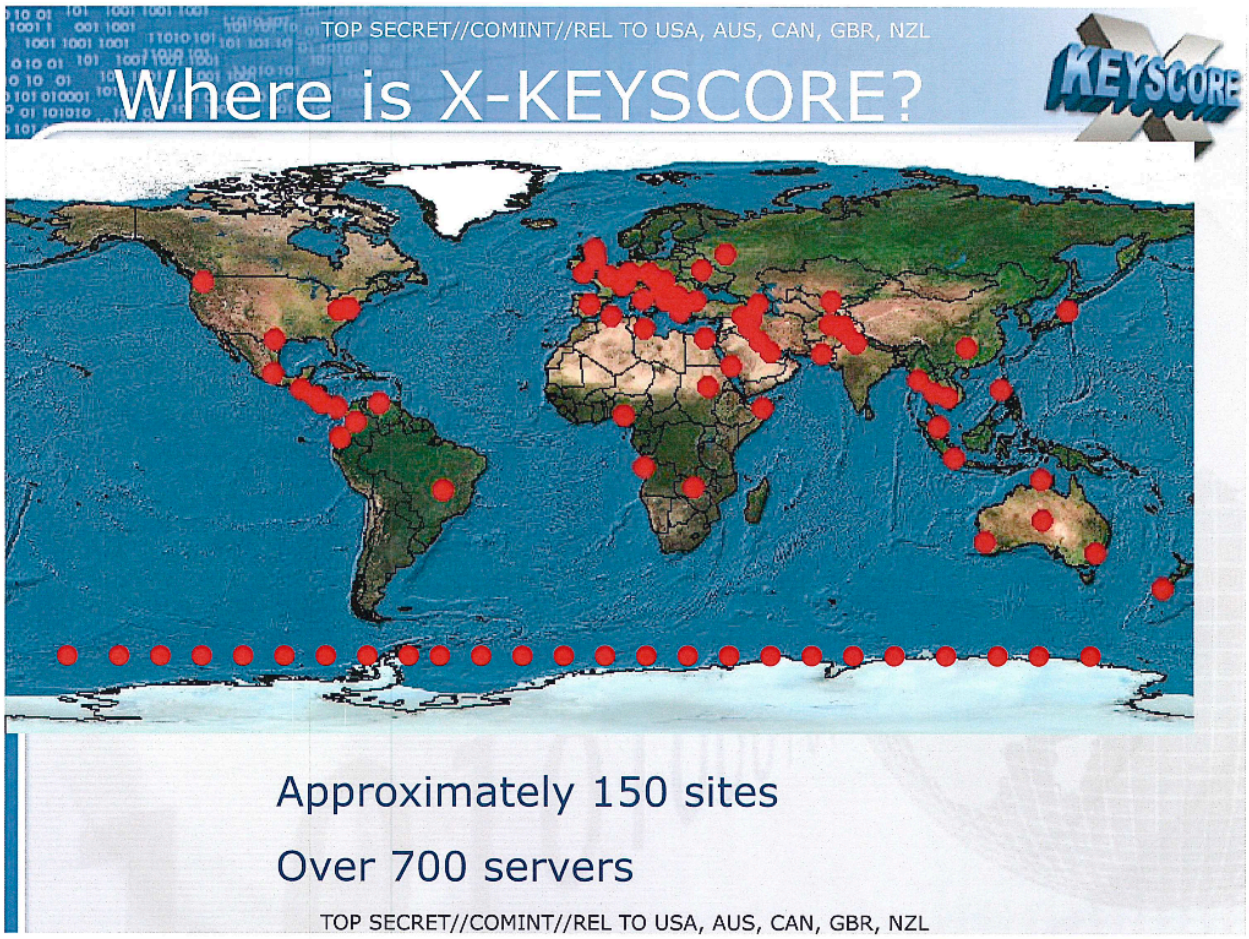
[70] https://netzpolitik.org/2015/geheimer-pruefbericht-wie-der-bnd-die-gesetzlich-vorgeschriebene-20-prozent-regel-hintertreibt/

[71] https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/#Sachstandsbericht

[72] http://www.spiegel.de/politik/deutschland/bundesnachrichtendienst-soll-massiv-gegen-datenschutz-verstossen-haben-a-1110579.html

[73] http://www.zeit.de/digital/internet/2016-06/ueberwachung-henrik-moltke-deep-cables-berlin

[74] https://upload.wikimedia.org/wikipedia/commons/4/48/XKeyscore_presentation_from_2008.pdf



Folie einer NSA-Präsentation zu XKeyscore

Dort filtern sie mehr oder weniger den gesamten weltweiten Internet-Verkehr nach für sie interessanten Inhalten. Ausgeklügelte Software wie XKeyscore[75],[76] filtert den Internet-Verkehr (Internet-Browser-Daten, E-Mail, Chat…) nach bestimmten Stichwörtern. Tauchen „verdächtige Begriffe“ oder Bilder auf, werden die Kommunikationspartner automatisch auf ein bestimmtes „Verdächtigungs-Level“ gesetzt, um dann zielgerichtet detaillierter überwacht zu werden. Dabei ist selbst die SSL-Verschlüsselung nicht vor NSA-Spionage sicher[77].

„The Guardian“ berichtete, dass 10/2014 sagenhafte 1,2 Millionen Menschen auf dieser NSA Beobachtungsliste standen[78]. Die NSA hat bei ihren Spionageaktivitäten vor allem auch Deutschland im Visier. Dazu setzt sie präparierte Hardware ein. Das können von amerikanischen Unternehmen gelieferte Internet-Router sein, die in den deutschen Internet-Backbones installiert werden und dann dem Geheimdienst alle gewünschten Daten zuspielen[79],[80].

[75] http://technische-aufklaerung.de/ta034-spionagesoftware-xkeyscore/

[76] http://www.heise.de/newsticker/meldung/NSA-Ausschuss-BND-hat-XKeyscore-ohne-Sicherheitskonzept-genutzt-3118257.html

[77] http://www.zeit.de/digital/datenschutz/2013-09/nsa-gchq-private-internet-verschluesselung

[78] http://www.theguardian.com/us-news/2014/oct/11/second-leaker-in-us-intelligence-says-glenn-greenwald

[79] https://tarnkappe.info/sentry-eagle-nsa-sabotiert-gezielt-deutschland/

[80] https://firstlook.org/theintercept/2014/10/10/core-secrets/

Aber auch deutsche Regierungsinstitutionen sind bemüht, die Überwachung in Deutschland zu vereinfachen bzw. alles zu verhindern, was die Überwachung erschweren könnte. So setzt auch der Deutsche Geheimdienst seit Juni-2016 das NSA-Werkzeug XKeyscore ein. Und mit der Reform des BND-Gesetzes werden dem Deutschen Geheimdienst weitere Befugnisse zugestanden[81].
Der Trend, jegliche Kommunikation zu digitalisieren und mit Hilfe von Internet-Technologie zu übertragen, macht auch vor dem privaten Telefonnetz nicht halt. War es sowohl bei dem alten analogen als auch bei dem ISDN Netz noch problemlos möglich, Gespräche abzuhören, so wäre eine standardmäßige Ende-zu-Ende Verschlüsselung bei der heutigen Internet-Telefonie ganz einfach realisierbar. Aber die deutschen Behörden arbeiten erfolgreich daran, dies zu verhindern[82].

Geheimdienste haben durch ihre rechtliche Sonderstellung und fast unbegrenzten finanziellen Mitteln alle technischen Möglichkeiten, die für sie interessanten Informationen aus der riesigen Menge der Internet-Daten herauszufiltern, um bei Bedarf eine konkrete Person im Detail zu beobachten[83]. So geschah es im April 2014, dass der Dienstleister Levision seinen sicheren E-Mail Dienst „Lavabit“ abschalten musste. Der amerikanische Geheimdienst NSA hatte ihn zur Herausgabe privater Schlüssel gezwungen (Edward Snowden war Kunde von Lavabit)[84]. Kurz danach stellte auch der VPN Anbieter Cryptoseal aus den gleichen Gründen sein Angebot ein[85.] Amerikanische IT-Dienstleister, die vom amerikanischen Geheimdienst zur „Zusammenarbeit“ gezwungen werden, sind zusätzlich verpflichtet, diesen Sachverhalt geheim zu halten.

Allerdings überwachen auch Geheimdienste anderer Länder einen Großteil des gesamten Internet-Verkehrs. Da die Chinesische Firma Huawei Technologies auch Technology für Unterwasser-Kabel herstellt, ist China in der Lage darüber Internet-Daten anzuzapfen[86]. Die folgende Grafik gibt einen Überblick über die Unterwasser-Kabel Infrastruktur.

[81] http://www.zeit.de/digital/datenschutz/2016-06/bnd-bundesnachrichtendienst-gesetz-reform

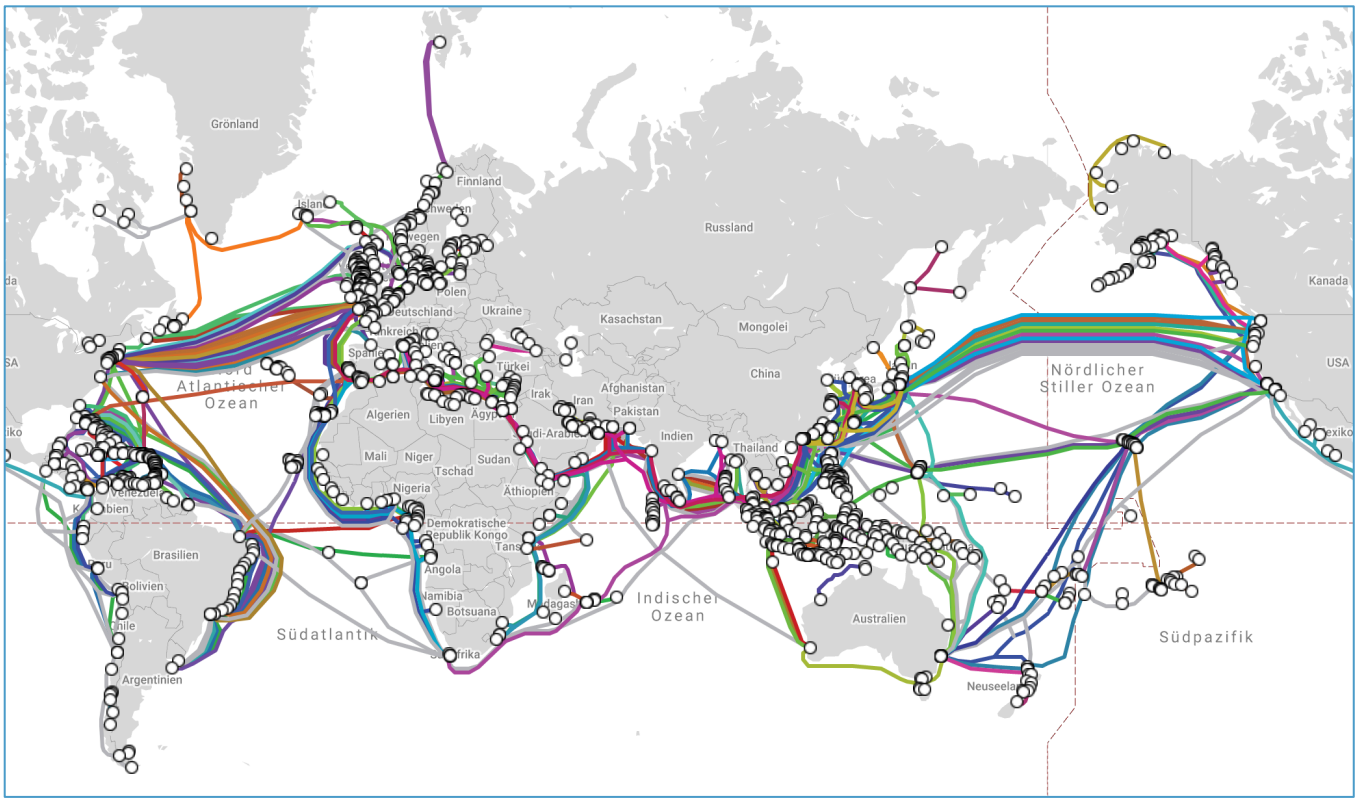
[82] http://www.br.de/fernsehen/das-erste/sendungen/report-muenchen/dossiers-und-mehr/internet-telefonie-lauschangriff100.html

[83] http://they-know.org/de

[84] http://www.zdnet.de/88165404/lavabit-snowdens-e-mail-service-schliest-und-warnt-vor-us-anbietern/

[85] http://www.heise.de/newsticker/meldung/NSA-Affaere-Cryptoseal-folgt-Lavabit-und-schliesst-VPN Angebot-1983157.html

[86] https://www.bloomberg.com/opinion/articles/2019-04-09/china-spying-the-internet-s-underwater-cables-are-next



https://www.submarinecablemap.com/

Und es sind nicht nur Geheimdienste die ohne Verdacht massenweise die gesamte Bevölkerung eines oder sogar viele Staaten ausspähen. Erst kürzlich wurde aufgedeckt, dass die US-Antidrogenbehörde DEA von 1992 bis 2013 Milliarden von Telefonverbindungsdaten gesammelt und gespeichert haben. Und diese Daten wurden nicht nur dazu benutzt um Drogendealern auf die Spur zu kommen[87].

Leider kann es dabei auch passieren, dass bei all diesen Ausspähungsaktivitäten jemand auf einem falschen „Verdächtigungs-Level“ landet, was für den Betreffenden sehr unangenehm werden kann. Er wäre nicht der Erste, der völlig unschuldig morgens um 4:00 Uhr von einer Staffel schwarz gekleideter Männer aus dem Bett geklingelt wird, bei dem dann sämtliche Rechner und verdächtige Papiere beschlagnahmt werden, und der für Tage unschuldig in einem Untersuchungsgefängnis landet. Auch wenn sich herausstellt, dass die Flughafenpläne und die Webseiten über Waffengesetze, die er sich anschaute, nur seiner besseren Orientierung an seinem nächsten Urlaubsziel galten: diesen Tag werden er und seine Familie nicht vergessen. Und es kann viele Monate dauern, bis er die beschlagnahmte Hardware, die er unter Umständen für seine Arbeit unbedingt benötigt, komplett analysiert von Computer-Forensikern zurückbekommt. Auch wenn dies für den Einzelnen persönliches Pech bedeutet, kann es alles in allem noch das kleinere Übel sein.

Ein reales Beispiel, bei denen staatliche Behörden auch nicht vor Rechtsbeugung zurückschreckten und unrechtmäßig Verdächtige nicht mehr auf einen Rechtsstaat hoffen konnten, zeigt die Entführung Abu

[87] http://www.zeit.de/digital/datenschutz/2015-04/metadaten-geheime-vorratsdatenspeicherung-usa-dea

Omars[88] Dieser wurde von der CIA, mit Unterstützung der italienischen Polizei, entführt und gefoltert. Da dies einer der wenigen Fälle ist, bei dem man die Täter ermitteln konnte (CIA), ist es umso überraschender, dass kein Täter verurteilt worden ist.
Hier ein paar Beispiele, was sonst noch so passieren kann bzw. schon eingetreten ist, wenn Geheimdienste (oder ihre Mitarbeiter) die Macht ihres Wissens ausnutzen:

- **Manipulation des Wirtschaftsgleichgewichts**: Jack Welch, langjähriger CEO von General Electric, soll einmal gesagt haben: "Wer mein Telefon abhört, kann sehr viel Geld verdienen" (weil er z.B. mit diesen Infos frühzeitig die richtigen Aktien kaufen könnte). Da Tausende Geheimdienstmitarbeiter Zugriff auf unbegrenzte Daten haben und die Aufdeckungsgefahr bei wirtschaftlichem Missbrauch sehr gering ist, ist davon auszugehen, dass solcher Missbrauch auch real stattfindet.

- **Politiker (oder andere Entscheidungsträger) können erpresst werden**. Wir wissen, dass die NSA die Telefone nicht nur deutscher Politiker überwacht hat. Wer sagt uns, dass sie dort nicht Informationen erhalten haben, mit denen sie die deutsche Politik beeinflussen können? J. Edgar Hoover, dem ersten Direktor des FBI, gelang es über die Amtszeiten von acht US-Präsidenten, diese Position zu halten. Unter anderem auch deswegen, weil er geschickt Informationen über seine politischen Gegner ausnutzte, die er in seiner Position als FBI-Direktor ermitteln konnte.

- **Entscheidungen von Politikern (oder anderen Amtsträgern) können manipuliert werden**; z.B. indem man ihnen, unter falschem Absender, gefälschte Informationen zukommen lässt, die sie als authentisch einschätzen. Derartige Fehlentscheidungen können fatale Konsequenzen haben, weil damit sogar Kriege provoziert werden können.

- **Wissen ist Macht – Das Facebook Experiment**: Bei den USA Kongresswahlen 2010 gab Facebook ausgewählten Nutzern den Hinweis, dass heute Wahltag ist. Dadurch stieg die Wahlbeteiligung um 0,39% (60.000 Wähler)[89]. Wem genau hatte Facebook diesen Hinweis angezeigt?[90]

- Durch **Manipulation von Internet-Backbone Routern** können Cyber-Angriffe gefahren werden, die z.B. die Stromversorgung ganzer Länder lahmlegen. Die Angreifer können sich dabei sogar "hinter" einem anderen Land verstecken. So sieht es für Security-Analysten, die nicht wissen, dass Internet-Router manipuliert worden sind, so aus, als käme dieser Angriff ursächlich aus einem ganz anderen Land.

- Allein aufgrund von Überwachungsdaten können sogar **Menschen getötet werden**. Und das gefährdet nicht nur politische Aktivisten in totalitären Staaten. Nein, auch demokratische Länder tun das. Michael Hayden, ehemaliger Direktor der NSA und des CIA, bestätigte einmal in einem Interview: "Wir töten Menschen auf Basis von Metadaten"[91].

[88] http://www.swr.de/swr2/programm/sendungen/wissen/die-cia-vor-gericht/-/id=660374/nid=660374/did=14823688/1wyj4my/index.html

[89] https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering

[90] http://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006?rev=1462799465508

91 http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/

https://www.youtube.com/watch?v=UdQiz0Vavmc

- Damit Geheimdienste und andere staatliche Überwachung überhaupt in der Lage sind Schadcode zum Zwecke der Überwachung auf ein Gerät zu bringen, müssen Software-Lücken des Geräts bekannt sein. Und damit besteht von diesen **Staatlichen Organisationen kein Interesse daran, solche Softwarelücken schließen** zu lassen. Irgendwann werden solche Softwarelücken aber auch Hackern bekannt, die diese dann ausnutzen.
  So wurde 2016 das Angriffswerkzeug „EternalBlue“, das von der NSA zur Überwachung entwickelt wurde, von Hackern entwendet und damit großflächige Angriffe gefahren, die unter den Namen WannaCry, NotPetya und Baltimore bekannt wurden[92]. Mit diesen Angriffen wurden ganze Städte, Krankenhäuser und Firmen lahm gelegt.

Bei Geheimdiensten wird es immer das Problem „Wer überwacht die Überwacher?“ geben. Natürlich muss Sicherheit auch immer Freiheiten einschränken. Sicherheit mit mehr Überwachung zu gewährleisten, ist ein einfacher Weg für die Politik, da dadurch in Einzelfällen evtl. sogar Verbrechen verhindert werden können oder zumindest die Aufklärung unterstützt werden kann. In einer Demokratie sollte sich allerdings ein gesunder Kompromiss etablieren. Eine Übermacht der Geheimdienste ist ein Schritt in den „Überwachungsstaat“[93].

Geheimdienste haben allerdings nicht mehr nur das Ziel, Informationen zu sammeln und auszuwerten. Mittlerweile werden Geheimdienste direkt in die Kriegsführung miteinbezogen. Vor allem der amerikanische Geheimdienst NSA ist in der Lage, ganze Infrastrukturen zu zerstören. Solche Infrastrukturen könnten das Kommunikationssystem oder Stromnetz eines Landes sein, sodass kein Internet, keine Bank und auch kein Rettungsdienst mehr funktioniert. Das besonders Perfide daran ist, dass es damit möglich ist, die Schuld eines Angriffs anderen in die Schuhe zu schieben. Dazu muss ein Angreifer nicht vor Ort sein; den wahren Angreifer zu verschleiern[94]. funktioniert von einem anderen Land aus oder sogar von jedem beliebigen Punkt auf der Erde. Das besonders hinterhältige hieran ist, dass es damit auch noch einfach möglich ist, die Schuld anderen, z.B. unbequemen Kritikern, in die Schuhe zu schieben.
"Devise sei dabei stets, die eigenen Aktionen plausibel leugnen zu können. Dazu sei es üblich, Unbeteiligte ohne ihr Wissen einzuspannen, um den wahren Urheber zu verschleiern. Als Folge entwickelt die USA nach den ABC-Waffen (Atom-, biologische und chemische Waffen) nun digitale D-Waffen.”[95]

Es sollte nie vergessen werden, dass Überwachung letztendlich von Menschen verursacht und indirekt auch durchgeführt wird. Zumindest haben bestimmte Menschen immer Zugriff auf Überwachungsdaten, und da Menschen mit diesen Informationen auch ihre persönlichen Ziele verfolgen können, wird das auch geschehen. "Macht ohne Missbrauch verliert ihren Reiz." sagte angeblich einmal Groucho Marx. Dadurch, dass sich bei Geheimdiensten an zentraler Stelle sehr „wertvolle“ Daten und Informationen ansammeln, sind Geheimdienste auch eines der begehrtesten Angriffsziele für kriminelle Hacker. Dass Hacker es geschafft haben Daten von Geheimdiensten abzugreifen, wird selten öffentlich bekannt; aber dies ist schon vorgekommen, sogar in Deutschland[96].

[92] https://www.spiegel.de/netzwelt/web/schadsoftware-vom-us-geheimdienst-entwickelt-von-erpressern-genutzt-a-1269343.html

[93] https://www.youtube.com/watch?v=iHlzsURb0WI&feature=youtu.be

[94] http://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html

[95] http://www.heise.de/security/meldung/NSA-bereitet-eigene-Angriffe-im-Netz-vor-2519532.html?wt_mc=nl.heisec-summary.2015-01-19

[96] http://www.mz-web.de/mitteldeutschland/verfassungsschutz-sachsen-anhalt-geheimdienst-gehackt-23979024

Es gibt einen sehr empfehlenswerten interaktiven Film mit dem Namen „Netwars / out of CTRL", der im Detail über diesen digitalen Krieg aufklärt[97].
Wie weit derzeit alleine die NSA in ihrer Entwicklung schon gekommen ist, zeigen die Enthüllungen von Edward Snowden, die Heise in über 1.000 Eintragungen auf einer Zeitachse dokumentiert hat[98].

Internet-Kriminelle

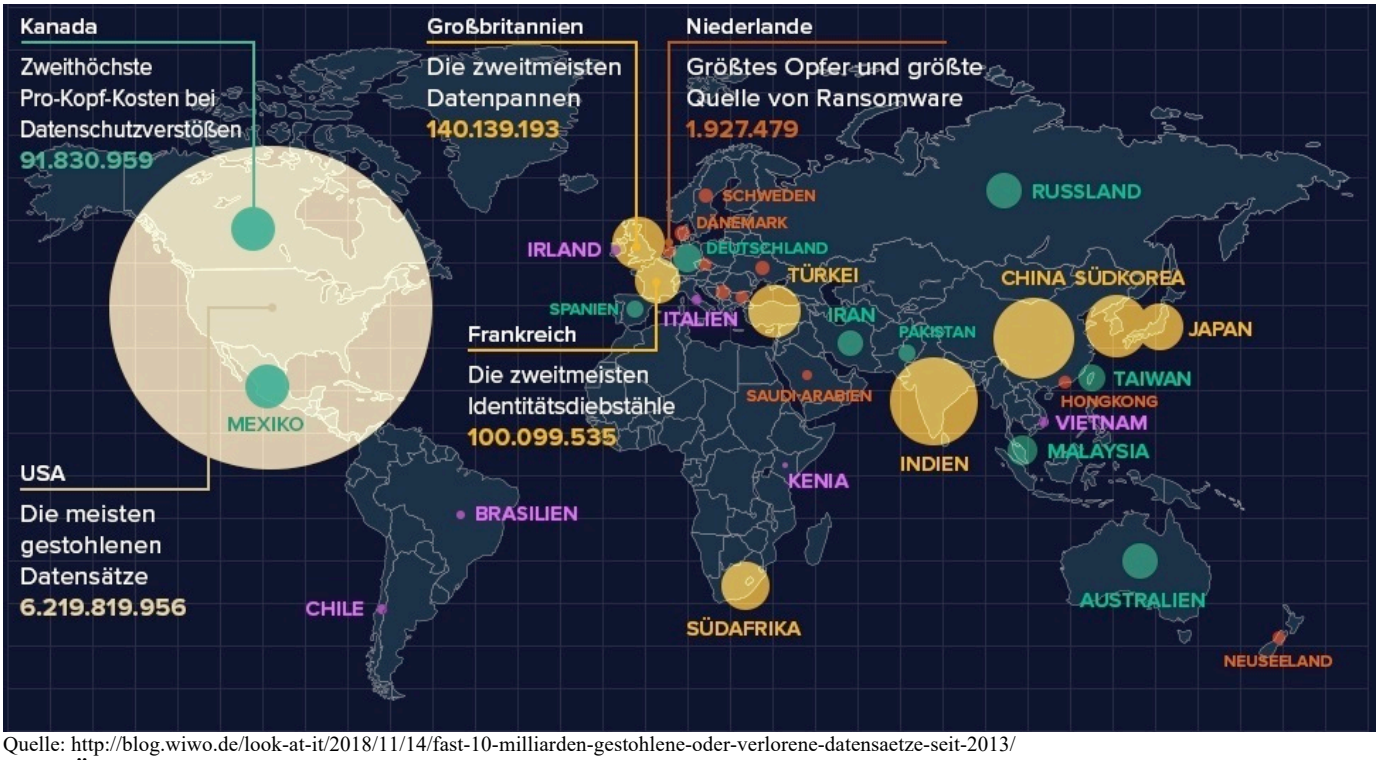
Die dritte Gruppe, die alles dafür tut, Nutzerdaten zu manipulieren, umfasst Internet-Kriminelle, die Nutzern irgendwelche schädlichen Programme unterschieben. Dies dient i.d.R. dem Zweck, sich die Passwörter des jeweiligen Nutzers zu erschleichen, um dann dessen Rechner oder sogar dessen Identität zu usurpieren. Mit Hilfe dieser Informationen können Internet-Kriminelle z.B. auf Kosten anderer einkaufen oder Geld von Bankkonten abheben. Oft werden solche sensiblen Nutzerdaten millionenfach im Internet verkauft.
Internet-Kriminelle können mit abgefangenen oder mit manipulierten Daten aber auch dadurch Geld verdienen, dass sie diese Informationen nutzen, um wirtschaftliche Vorteile z.B. an der Börse zu erlangen[99]. Oder sie erpressen andere mit den gewonnen Informationen.
Nicht nur private Internet-Benutzer sind gefährdet. Viel lukrativer ist es für Hacker, sich in Unternehmen einzuschleichen und diese mit geheimen Unternehmensinformationen zu erpressen oder diese Informationen an Wettbewerber zu verkaufen. Der Deutsche Vertreter der digitalen Unternehmen, die BITKOM schätzt, dass jedes zweite deutsche Unternehmen mindestens einmal in den letzten zwei Jahren Opfer Digitaler Wirtschaftsspionage geworden ist. Dies verursacht einen Schaden von rund 51 Milliarden Euro pro Jahr[100].
Das Unternehmen Varonis (varonis.com) hat eine Statistik der fast 10 Milliarden gestohlenen oder verlorenen Datensätze von 2013 – 2018 aufgestellt. Das sind ca., 7 Mio Datensätze , die täglich kompromitiert werden.

97 http://netwars-project.com/de/webdoc

98 http://www.heise.de/extras/timeline

99 https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html

100 http://www.bitkom.org/de/presse/8477_82074.aspx



Quelle: http://blog.wiwo.de/look-at-it/2018/11/14/fast-10-milliarden-gestohlene-oder-verlorene-datensaetze-seit-2013/

Eine Übersicht der größten Sicherheits-Angriffe kann man unter https://haveibeenpwned.com/Pwned-Websites abrufen. Dort kann man auch abfragen, ob die eigene E-Mail-Adresse bei diesen Angriffen schon einmal kompromittiert wurde.

Oder wer die aktuellen weltweiten Angriffe in Echtzeit sehen möchte, der kann unter https://sicherheits-tacho.eu/start/main den „Sicherheitstacho“ der Deutschen Telekom aufrufen.

Alle drei hier beschriebenen Tätergruppen verfügen nicht nur über detailliertes technisches Fachwissen, sondern auch über nahezu unbegrenzte finanzielle Mittel. Diese finanziellen Möglichkeiten nutzen sie fortwährend, um die Methoden weiterzuentwickeln, mit denen sie sich Nutzerdaten erschleichen.

Es gibt zwar Werkzeuge, mit denen man sich einigermaßen gegen diese Eingriffe in die Privatsphäre wehren kann, aber diese sind meist nicht nur für große Firmen entwickelt worden und somit für Privatanwender nicht nur zu teuer, sondern von Laien auch nicht bedienbar. Zwar gibt es auch für Privatanwender technische Möglichkeiten, aber diese decken nicht alle Angriffsarten ab, sind i.d.R. nicht für alle Internet-Geräte verfügbar und oft für Laien wiederum auch nicht bedienbar.

Recht auf „Informationelle Selbstbestimmung“

Nach der Deutschen Rechtsprechung hat jeder ein Recht auf „Informationelle Selbstbestimmung“. Als Recht auf „informationelle Selbstbestimmung“ wird das Recht des Einzelnen verstanden, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Das Recht auf informationelle Selbstbestimmung ist im Grundgesetz nicht explizit geregelt. Das Bundesverfassungsgericht hat es in seinem Volkszählungsurteil aus dem allgemeinen Persönlichkeitsrecht (Art. 2

Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) entwickelt und versteht es als eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts[101].[102]

Nachdem Edward Snowden der Weltöffentlichkeit gezeigt hat, dass alles was spionagetechnisch machbar ist, auch angewandt wird, fragen sich viele, ob diese massenweise Ausspähung überhaupt mit den Menschenrechten vereinbar ist. Diese Frage hat Navi Pillay, eine hohe Beamtin der Vereinten Nationen für Menschenrechte, veranlasst, einen Bericht zum Schutz der Privatsphäre im digitalen Zeitalter vorzulegen[103]. Sie bekräftigt darin, dass die Menschenrechte und insbesondere das Recht auf Privatsphäre "offline" und "online" gleichermaßen gelten. Des Weiteren werden alle Staaten aufgefordert, das Recht auf Privatsphäre auch im Kontext digitaler Kommunikation zu achten und zu schützen, Maßnahmen zu ergreifen, um Rechtsverletzungen zu beenden und zu verhindern, Recht und Praktiken der Kommunikationsüberwachung zu überprüfen und in Einklang mit der internationalen Menschenrechtskonvention zu bringen. Die Staaten werden außerdem aufgefordert, unabhängige und effektive Aufsichtsmechanismen zu etablieren, um eine angemessene Transparenz und Kontrolle staatlicher Überwachung zu gewährleisten.

Ob sich alle Staaten und Unternehmen in den Ländern, die sich der UN Menschenrechtskonvention verpflichtet haben, in Zukunft daran halten werden, kann bezweifelt werden. Zweifel sind auch schon deswegen angebracht, da juristisch nicht klar definiert ist, welche Metadaten personenbezogene Daten sind. Somit kann jeder in diesem juristischen Niemandsland Metadaten sammeln. Auch der deutsche Geheimdienst ist an diesen Metadaten interessiert und beharrt darauf, dass Metadaten keine personenbezogenen Daten sind[104].

Die Comidio Mission

Auf Grund dieser Gegebenheiten hat sich in den letzten Jahren ein riesiges Ungleichgewicht entwickelt. Dieses besteht auf der einen Seite aus den großen, mit den Daten ihrer Nutzer Geld verdienenden Internetfirmen in Verbindung mit maßlosen staatlichen Einrichtungen, die anlasslos alle und jeden überwachen. Auf der anderen Seite stehen die oft hilflose Firmen und Internet-Laien, die sich zwar oft des Problems bewusst sind, aber keine Möglichkeit sehen, diese Angriffe auf Ihre Firmengeheimnisse und Persönlichkeit abzuwehren.
Diesen Internet-Laien, also privaten Anwendern und kleinen Firmen, möchte Comidio Mittel an die Hand geben, mit denen sie ihre gesetzlich zugesicherte Privatsphäre und Anonymität verteidigen können.
Comidio hat die Angreifer in drei Gruppen eingeteilt

1. Gruppe: Kommerzielle Daten-Tracker und Daten-Händler
2. Gruppe: Geheimdienste und andere staatliche Autoritäten
3. Gruppe: Internet-Kriminelle (Hacker, die es auf das Geld des Internet-Nutzers abgesehen haben)

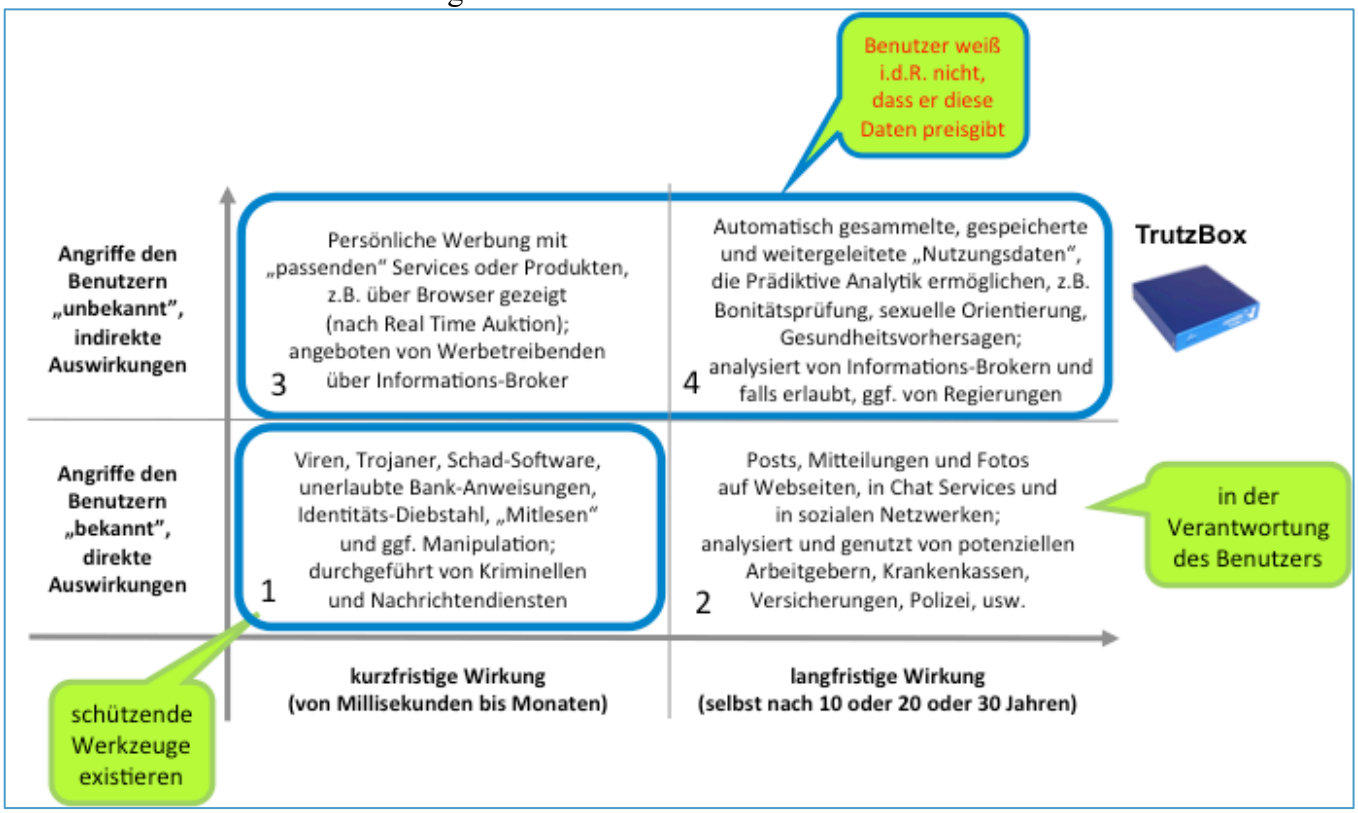
[101] http://www.grundrechteschutz.de/gg/recht-auf-informationelle-selbstbestimmung-272

[102]https://de.wikipedia.org/wiki/Grundrecht_auf_Gew%C3%A4hrleistung_der_Vertraulichkeit_und_Integrit%C3%A4t_informationstechnischer_Systeme

103 http://www.institut-fuer-menschenrechte.de/aktuell/news/meldung/article/navi-pillay-legt-bericht-zum-schutz-der-privatsphaere-im-digitalen-zeitalter-vor.html

104 https://netzpolitik.org/2014/lieber-bundesnachrichtendienst-wir-erklaeren-warum-metadaten-sehr-wohl-personenbezogene-daten-sind/

Die Angreifer in diese drei Gruppen einzuteilen ist sinnvoll, da sie einerseits unterschiedliche Bedrohungen darstellen und andererseits mit jeweils eigenen technischen Mitteln und juristischen Möglichkeiten arbeiten.
Während die 1. Gruppe „Kommerzielle Daten-Tracker und Daten-Händler“ das Nutzer-Surfverhalten immer und jederzeit beim Browsen im Internet heute schon protokolliert, passiert es glücklicherweise nicht so oft, dass der Nutzer von jemandem aus der 3. Gruppe „Internet-Kriminelle (Hacker, die es auf das Geld des Internet-Nutzers abgesehen haben)“ geschädigt wird. Wenn ein Nutzer gehackt wird, merkt er es in der Regel sehr bald, und die Hacker haben danach kein Interesse mehr an ihm. Die 1. und 2. Gruppe spionieren von allen Internet-Nutzern Daten aus und speichern diese für immer. Die daraus gewonnen Informationen können dem Nutzer auch noch nach Jahrzehnten Probleme bereiten. Und in der Regel merkt er gar nicht, dass er ausspioniert wird und weiß nicht, was mit seinen Daten passiert.
Häufig gibt er auch noch freiwillig persönliche Daten der Öffentlichkeit preis; z.B. bei Facebook, Twitter, LinkedIn und anderen sozialen Netzwerken.
Man kann aber auch auf seiner eigenen Homepage persönliche Daten veröffentlichen. Natürlich freuen sich alle drei Gruppen auch über diese Daten. Allerdings, hier entscheidet der Nutzer selbst darüber, was er freiwillig preisgibt. Er sollte sich aber auch bei diesen Daten immer bewusst sein, dass das Internet nichts vergisst. Selbst wenn man persönliche Daten in sozialen Netzwerken löscht, entzieht man sie damit nur der Öffentlichkeit – der Anbieter hat sie in der Regel immer noch im Zugriff.
Die Auswirkungen von Angriffen kann man nach vier Quadranten unterteilen. Waagerecht ist aufgetragen, wie lange sich der Angriff auf die Nutzerpersönlichkeit auswirken kann, in der Senkrechten, ob der Internet-Nutzer etwas von dem Angriff bemerkt:



Auswirkung 1: aus Angriffen durch alle Arten von Viren, Trojanern und durch anderer Malware, mit deren Hilfe kriminelle Hacker die User-IDs und Passwörter abfangen. Aber auch Behörden nutzen diese Technologien, um damit eine Art „Digitale Hausdurchsuchung“ durchzuführen, oder den Internet-Nutzer zunächst eine Zeitlang zu observieren. Zur Abwehr gibt es zahlreiche Viren-Schutzprogramme, die mehr oder weniger gut funktionieren.
Auswirkung 2: betrifft alle Daten, die der Nutzer freiwillig im Netz, z.B. bei Social Media Diensten wie Facebook, Linkedin usw. speichert. Für diese Daten ist er selbst verantwortlich. Er sollte sich bewusst sein, dass diese Daten auch gegen ihn verwendet werden können. Das Positive an dieser Kategorie ist, dass er es selbst in der Hand hat, was er über sich preisgibt.
Auswirkung 3: Daten-Sammel-Firmen nutzen die Daten entweder selbst oder verkaufen sie an andere Unternehmen. Insbesondere Online-Werbeunternehmen sind sehr an diesen Daten interessiert, vor allem wenn sie recht aktuell sind. Die Werbefirmen steuern damit zielgerichtet, recht zeitnah nach der Ermittlung der Daten, Werbebotschaften auf Webseiten ein, die der Nutzer besucht. Er kann sich zwar gegen die Erhebung dieser Daten und gegen solche Werbebotschaften mit Browser-Plugins wehren[105], aber diese Werkzeuge sind nicht für alle Geräte und Browser verfügbar und darüber hinaus von den Laien auch kaum bedienbar.
Auswirkung 4: Dies ist die gefährlichste Kategorie. Die hier von Daten-Sammel-Firmen und Behörden erhobenen Informationen werden nie gelöscht. Der Internet-Nutzer merkt gar nicht, dass diese Daten gespeichert werden. Und diese Daten können ihm auch noch viele Jahre später Probleme bereiten. Die Methoden, mit denen diese Daten gesammelt werden, sind die gleichen wie in Kategorie 2 und 3. Aber der Nutzer hat derzeit kaum eine Chance, sich gegen diese Kategorie zur Wehr zu setzen.
Bei den unteren beiden Kategorien 1 und 2 weiß der Nutzer i.d.R. von der Gefahr und den Auswirkungen und hat heute schon Mittel und Möglichkeiten, Schäden abzuwehren.
Jedoch hat er derzeit kaum eine Chance, sich gegen die beiden Kategorien 3 und 4 in der obersten Reihe zu schützen.
Comidio hat sich zum Ziel gesetzt, jedem Internet-Nutzer Mittel in die Hand zu geben, um sich vor allem gegen die beiden Kategorien 3 und 4 zu wehren!

105 Z.B. mit Werkzeugen wie AddBlockerPlus, Ghostery, AVG-DoNotTrackMe, NoScript, lightbeam…

Wie kommen Angreifer an Daten des Internet-Nutzers?

Um das Leben der drei Gruppen, die Nutzerdaten abgreifen möchten, möglichst schwer zu machen, muss erst einmal genauer heraus gearbeitet werden, welche Techniken diese Gruppen nutzen, um Daten des Internet-Nutzers mitzulesen und zu manipulieren.

1. Gruppe: Kommerzielle Daten-Tracker und Daten-Händler

Ein Webseiten Entwickler möchte natürlich seine Webseiten möglichst benutzerfreundlich gestalten. Dazu werden ihm im Internet viele Hilfen für die Gestaltung und Programmierung von Webseiten angeboten. Der Großteil dieser Code-Bibliotheken ist kostenlos und wird mittlerweile häufig genutzt. Kaum ein Entwickler programmiert seine Webseiten nur noch mit seinem eigenen Programm-Code.
Allerdings haben die Anbieter dieser Hilfs-Software nicht nur das Wohl des zukünftigen Anwenders und des Entwicklers im Auge, sondern auch ihr eigenes. Sehr oft verstecken sich Daten-Tracker in diesem Code, und meist interessiert es die Entwickler gar nicht, was sie da in Webseiten einbauen.
Des Weiteren gibt es viele Hersteller von Webseiten-Tools, deren Werkzeuge es erlauben, im späteren Betrieb der Webseite durch Schaltung von Werbung Geld zu verdienen oder Statistiken über die Nutzung der Seite anzulegen. Leider werden alle Informationen, die dann bei der Benutzung der Webseite gesammelt werden, auch dem Anbieter dieser Werkzeuge zur Verfügung gestellt.

Allein Google bietet den Entwicklern von Webseiten als auch den Betreibern der Webseiten viele Möglichkeiten an, ihre Webseite zu „optimieren“[106],[107]:

- Benutzerdefinierte Suche
- Enterprise Search
- Google Earth Enterprise
- Website-Übersetzer
- AdWords
- DoubleClick
- AdMob
- Google Analytics
- Google Fonts
- Google hosted libraries
- Google Public DNS
- Blogger.com
- Blogspot.com

106 http://www.heise.de/ct/14/11/links/134.shtml

107 https://developers.google.com/apis-explorer/#p/

- Google Sites
- Google Groups
- Google Cloud Platform
- Freebase
- Zagat
- Panoramio
- safebrowsing

Fast schon grotesk ist es, dass Google eine Browser-Erweiterung für jedermann anbietet, die Google-Analytics deaktiviert[108]. Für die vielen anderen Mechanismen, mit denen Google den Nutzer ausspioniert, gibt es das nicht.
Tim Libert (https://timlibert.me) hat eine Studie[109] veröffentlicht, in der er nicht nur eine Million Webseiten auf Datentracker hin analysiert hat, sondern auch, in wieweit diese von der NSA genutzt werden:

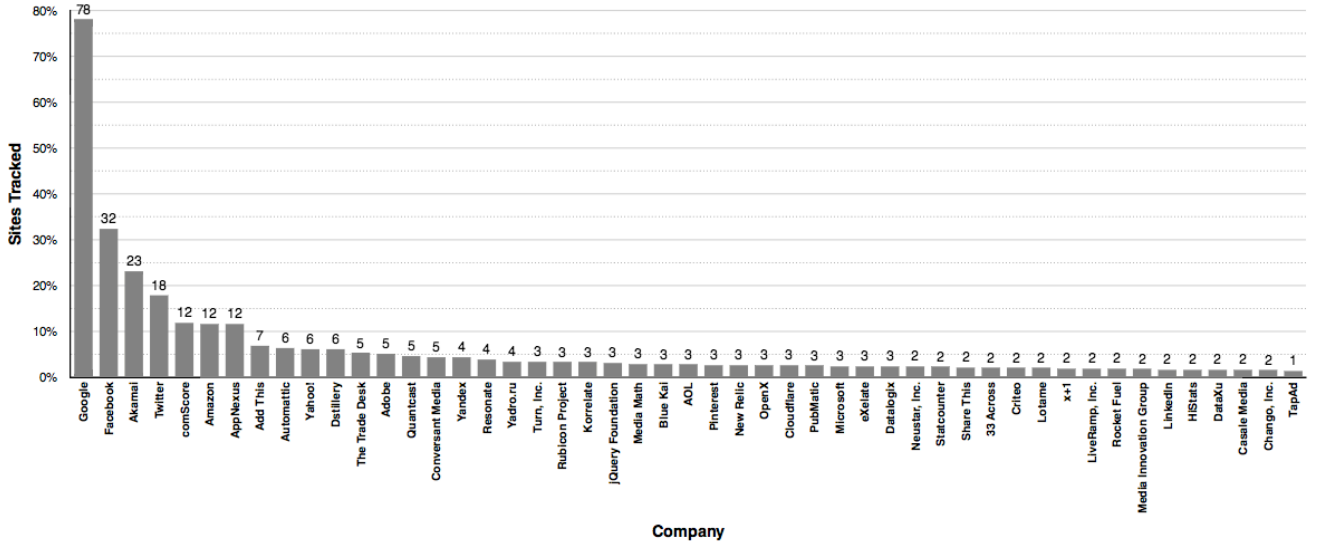


Figure 1: *Percentage of Sites Tracked by Top 50 Corporations*

Aus der Studie geht hervor, dass über 78% der analysierten Seiten einen Tracker von Google haben. In der Studie wird außerdem noch vermutet, dass auf jeder fünften Webseite diese kommerziellen Tracker von Geheimdiensten wie z.B. die NSA genutzt werden, um Internetnutzer zu überwachen. Dadurch soll es der NSA auch möglich sein, Nutzer, die sich durch das Tor-Netzwerk schützen oder im „Dark-Internet surfen“, zu de-anonymisieren.
Eine weitere Seite, dasfilter.com hat ebenfalls eine Statistik über die Web-Sites mit den meisten Trackern erstellt[110]:

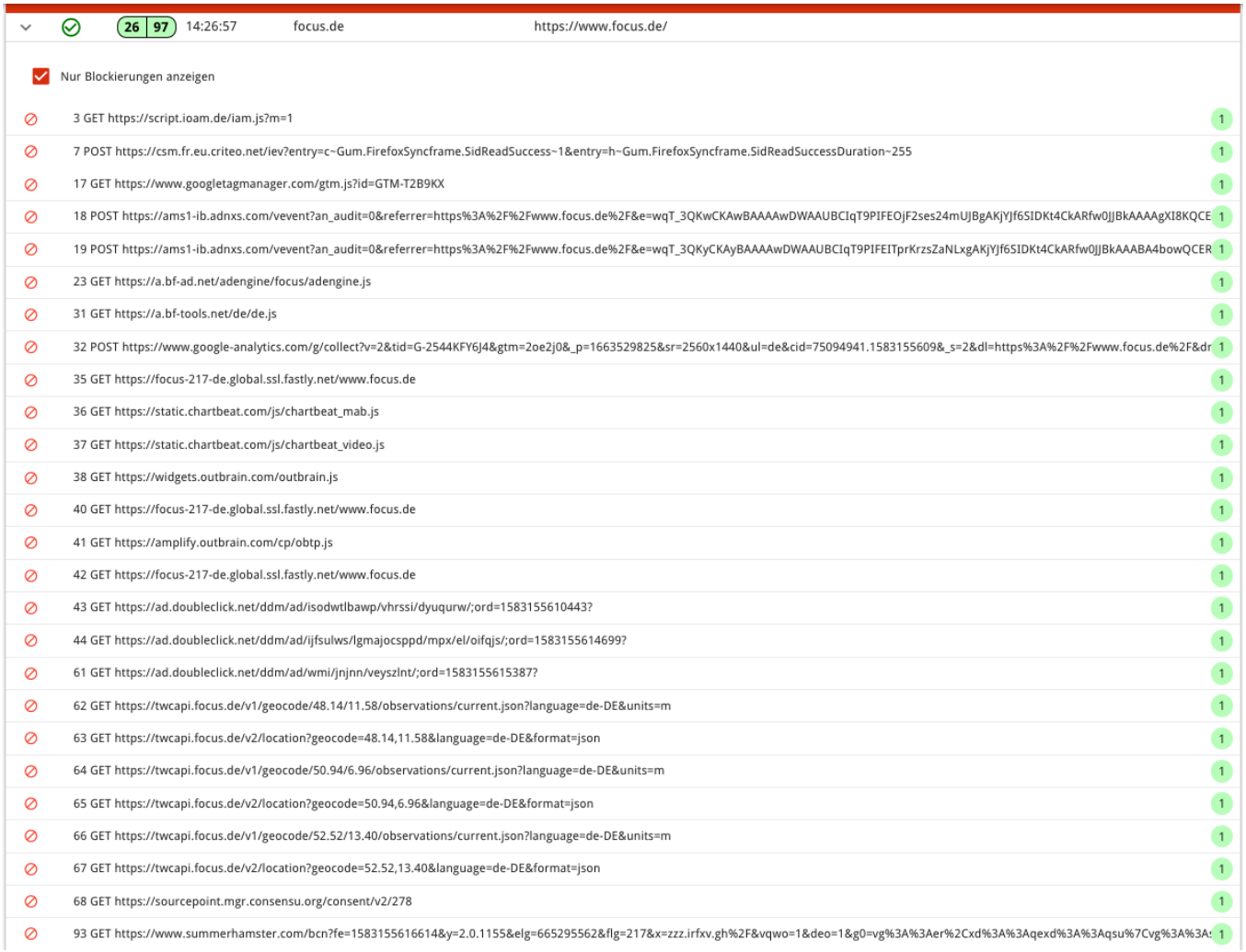
108 https://tools.google.com/dlpage/gaoptout?hl=de

109 https://timlibert.me/pdf/Libert-2015-Exposing_Hidden_Web_on_Million_Sites.pdf

110 http://dasfilter.com/internet/eine-top-22-der-vertracktesten-seiten-wer-laesst-die-meisten-daten-sammeln

Und neben Google gibt es schätzungsweise über 81.000 weitere Unternehmen, die auf ähnliche Weise das Nutzer-Surfverhalten beobachten und mit diesen Daten Geld verdienen[111].
Hier ein Beispiel:
Wenn der Nutzer die Webseite der Zeitschrift Focus aufruft (focus.de), weiß Google bereits, dass jemand auf dem Rechner des betroffenen Nutzers gerade Focus liest (doubleclick und google-analytics). Wenn er dann auf focus.de einen konkreten Artikel anklickt, sieht er einen Facebook „Teilen“ Knopf oder LikeMe-Knopf. Abhängig davon, wie dieser Knopf auf der Webseite programmiert wurde, weiß jetzt auch Facebook, dass sein Rechner die Seite von focus.de aufgerufen hat. Und das ohne, dass der Nutzer diesen Knopf betätigt, und ohne dass der Nutzer überhaupt Mitglied bei Facebook sein muss.
Das Blocking-Protokoll der Comidio TrutzBox TrutzBrowse Funktion zeigt die Details der Tracker, hier am Beispiel eines Artikels von focus.de (abgerufen am 2.3.2020):

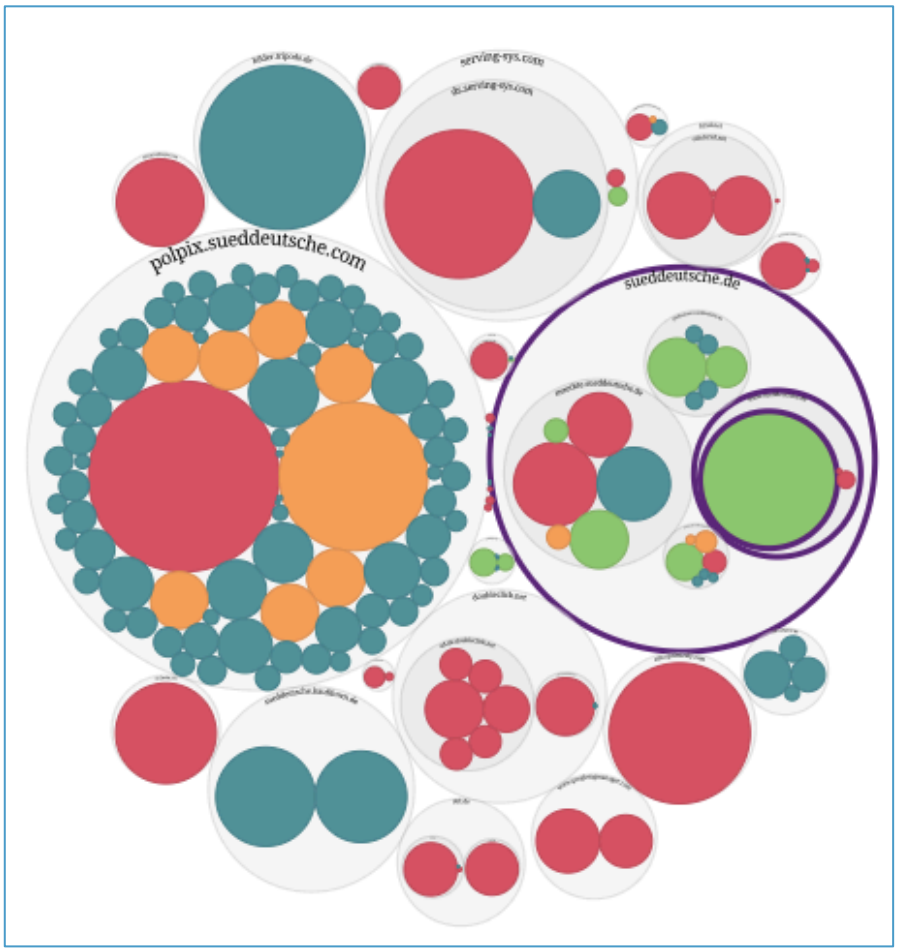
[111] http://www.sueddeutsche.de/digital/internet-dienste-dominieren-das-online-tracking-1.2998244



(© 2020 Comidio GmbH)

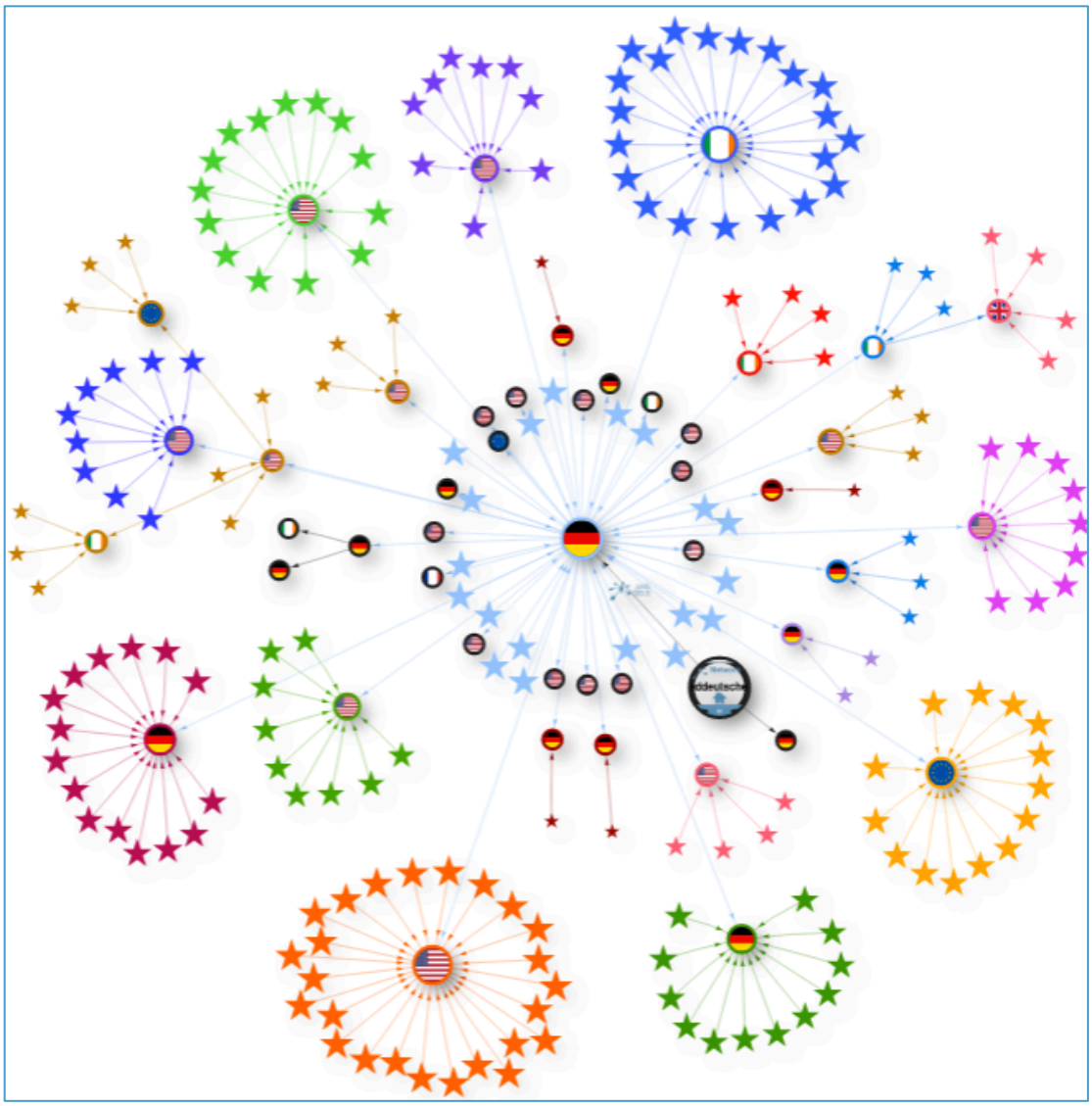
Jetzt wissen neben den Firmen Google und Summerhamster auch die Firmen Ioam und einige weitere Datensammler, dass der Internetnutzer sich für ein bestimmtes Thema interessiert. Facebook (und auch Google) bekommen sogar die Information, über welchen Link er auf diese Seite gelangt ist, also welcher Artikel aufgerufen wurde. Und wenn er bei Facebook Mitglied ist und irgendwann in den letzten drei Monaten eingeloggt war, weiß Facebook auch noch wer der Nutzer ist, der gerade einen Artikel auf focus.de abruft (das gleiche gilt auch für Google).

Die Webseite http://datenblumen.wired.de (link funktioniert leider nicht mehr) veranschaulicht auch sehr gut, wie eine Webseite aufgebaut ist, und an welche Daten-Tracker diese Webseite die Daten des Anwenders ebenfalls weiterleitet:



Die Datenblume für sueddeutsche.de

In welche Länder der Datenverkehr bei Abruf einer Seite geleitet wird, veranschaulicht die Analysesoftware von sendsdata.to sehr gut:



Datentransfer von sueddeutsche.de visualisiert mit Hilfe von sendsdata.to (abgerufen am 17.1.2019)

Wie kommen Unbefugte an das Nutzerverhalten?

Zwar könnte der Internet-Service-Provider seine Kunden überwachen. Da er direkt alle Daten zwischen dem Benutzer und dem Internet auf beiden Seiten der Verbindung (Internet-Router auf Kundenseite und auf Provider-Seite) kontrolliert, hat er alle Möglichkeiten, die Aktivitäten seiner Kunden einzuschränken, ihre Daten mitzuhören, oder sogar zu manipulieren. Und das geschieht dann natürlich auch[112]. Allerdings gibt es im Internet eine ganze Industrie, die sich auf das Tracken von Daten spezialisiert hat. Auf der Seite dieser Industrie bieten Unternehmen Webseiten Betreibern und Programmierern Tools

[112] http://www.sueddeutsche.de/digital/datenschutz-privatsphaere-kostet-extra-1.2355175

und Dienstleistungen, mit deren Hilfe sie die Nutzung ihrer Webseiten kontrollieren können. Die Anbieter solcher Werkzeuge, ganz vorne dabei die Firma Google, bekommen bei Nutzung dieser Werkzeuge meist Nutzungsprofile automatisch mitgeliefert.
Da man sich bei den meisten Webseiten nicht einloggen, also seine persönlichen Daten nicht eingeben muss, ist der Webserver genötigt zu erkennen, dass der gleiche Client (Browser), der gestern bestimmte Zugriffsmuster hinterlassen hat, jetzt wieder auf bestimmte Webseiten zugreift (evtl. auf andere Seiten als gestern). Mit diesen Informationen werden die Nutzerprofile kontinuierlich erweitert und verbessert.
Früher wurden dazu ausschließlich Cookies auf dem Client gespeichert. Cookies sind kleine Dateien, in denen der Daten-Tracker eine eindeutige Kennung über die Websitzung speichert, und die später jederzeit wieder ausgelesen werden kann. Diese Cookies können auch von fremden Webseiten gelesen werden.
Da aber immer mehr Nutzer dazu übergehen, Cookies im Browser abzuschalten, oder sogar Webseiten meiden, die Cookies verwenden, rückt man heutzutage von dieser Technologie eher ab.
Stattdessen benutzt man mehr und mehr den „Fingerabdruck“ des Browsers. Dazu wurde in den letzten Jahren eine Vielzahl von Techniken entwickelt:

- Flash- Local-Storage Objekte,
- localStorage,
- Web Storage,
- WebSQL,
- Web-Beacons,
- FileWriter API oder
- HTTP-ETags

Oft wird die Möglichkeit genutzt, den Webserver möglichst eindeutige Daten vom Browser erfragen (Browser-Profile) zu lassen; z.B.

- aktuelle Bildschirm-Auflösung,
- aktuell benutztes Betriebssystem,
- Browser-Hersteller und -Version,
- wie viele Browser-Tabs geöffnet sind,
- ob Cookies erlaubt sind,
- welche Sprache eingestellt ist,
- welche Schriften geladen sind,
- und vieles mehr.

In der Regel genügen 6 Angaben, um einen Internet-Client weitgehend zuverlässig von Milliarden anderer Internet-Nutzern eindeutig zu unterscheiden. Mit Fingerprint-Werkzeugen wie

- http://ip-check.info,

- https://audiofingerprint.openwpm.com,
- http://analyze.privacy.net/Default.asp
- http://browserspy.dk/useragent.php
- http://www.ericgiguere.com/tools/http-header-viewer.html
- http://www.rexswain.com/httpview.html
- http://livehttpheaders.mozdev.org oder auch mit
- https://panopticlick.eff.org
- http://www.dein-ip-check.de
- https://amiunique.org/
- https://coveryourtracks.eff.org/
- http://noc.to/
- https://fingerprint.pet-portal.eu
- https:// browserleaks.com

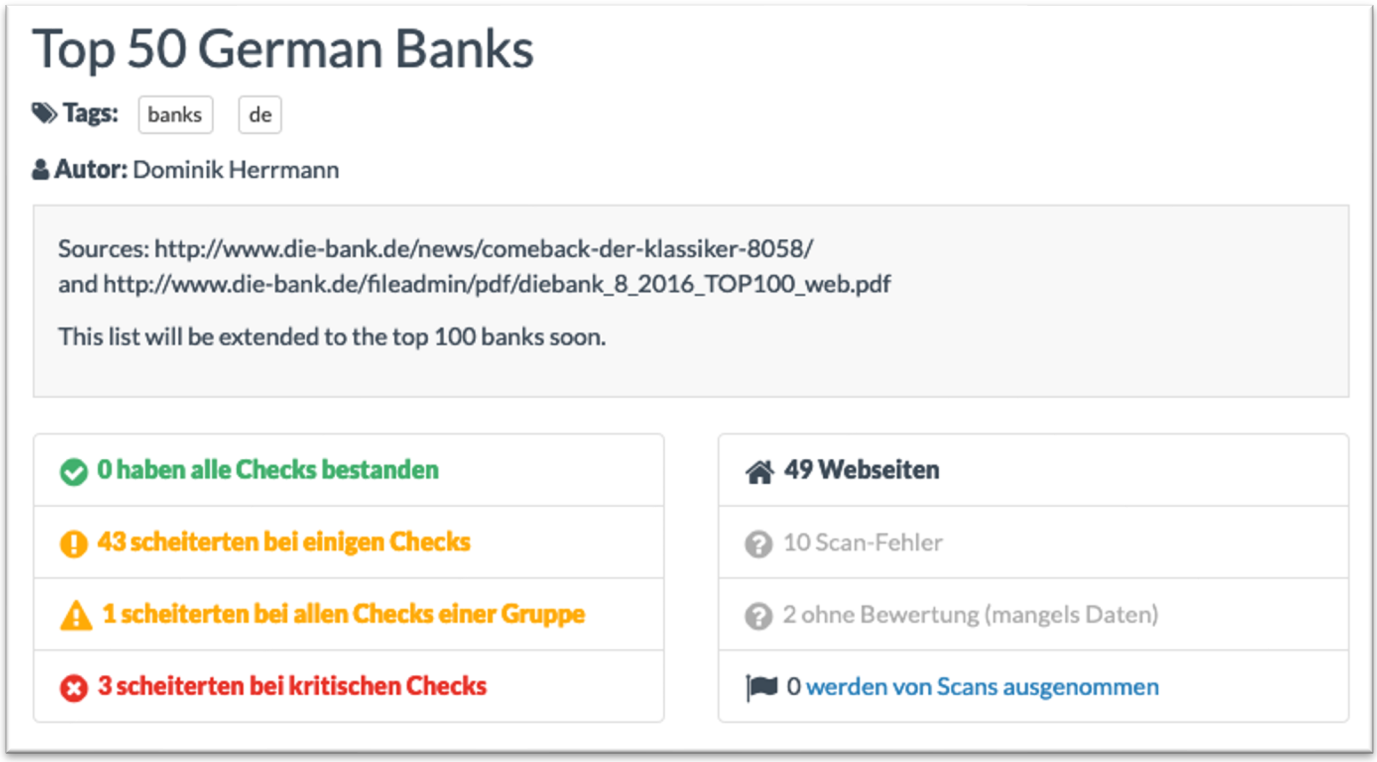
kann jeder selbst herausfinden, welche Daten der Server von seinem Browser auslesen kann, um ihn möglichst zuverlässig wiederzuerkennen. Wenn der Internet-Nutzer dann verschiedene Webseiten aufruft, kann der Daten-Tracker erkennen, dass es sich wieder um denselben Nutzer handelt, der jetzt eine andere Seite ansteuert. Damit kann der Daten-Tracker ein Web-Profil des Nutzers erstellen. Und da er auch noch nachvollziehen kann,

- wie lange der Nutzer auf einer Seite war,
- auf welche Links er geklickt hat,
- zu welchen Uhrzeiten,
- von welchem ungefähren Standort usw.

kennt der Daten-Tracker mit diesen gesammelten Daten nach ein paar Tagen bereits grundsätzlich die Nutzerinteressen. Darüber hinaus kann er auch schon bald besser als der Nutzer selbst voraussagen, was dieser demnächst tun wird oder an was er sonst noch Interesse haben könnte (vgl. Amazon).
Immer wieder argumentieren Tracking-Firmen, dass sie ja nur anonym die Daten sammeln. Dass es aber relativ einfach ist, aus diesen sogenannten „anonymen“ Daten, die realen Personen, die diese Daten-Spuren hinterlassen ausfindig zu machen, zeigt die Analyse der Sendung Panorama 3 „Nackt im Netz: Millionen Nutzer ausgespäht“:
http://www.ardmediathek.de/tv/Panorama-3/Panorama-3-die-ganze-Sendung/NDR-Fernsehen/Video?bcastId=14049184&documentId=38689544

Sicherheit von Web-Seiten prüfen

Mit Hilfe der Webseite https://privacyscore.org (Compare Websites with PrivacyScore) kann man Webseiten prüfen, wie sicher diese sind. Die Entwickler dieser Seite haben auch eine Funktion eingebaut, über die man eine ganze Liste von Links prüfen lassen kann. Einige interessante Gruppen von Web-Seiten können dort schon abgerufen werden. Z.B. Top 50 German Banks:



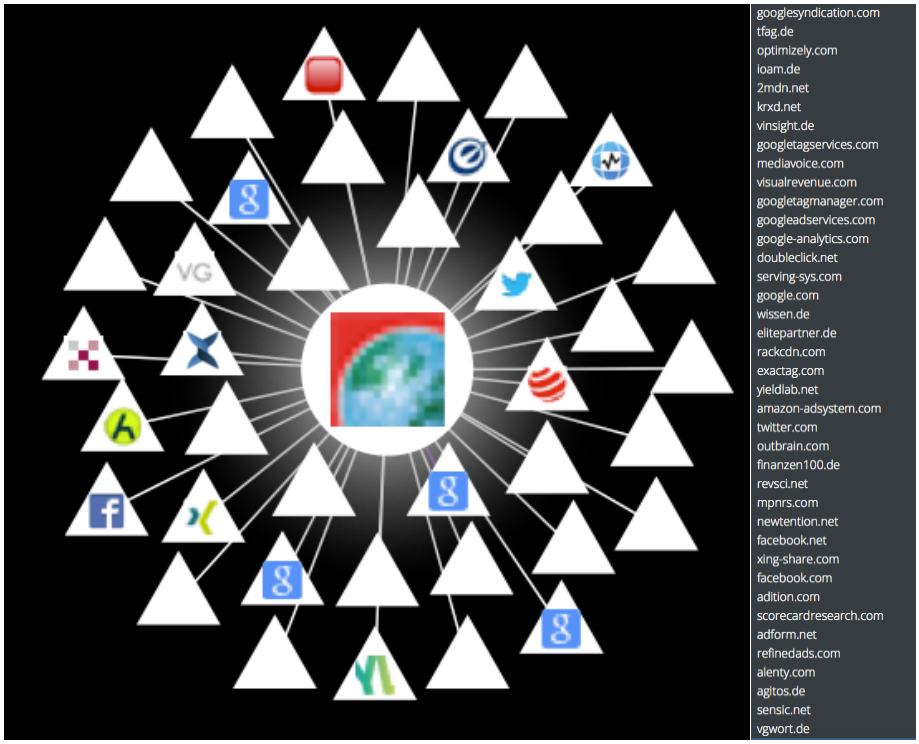
https://privacyscore.org/list/47/?categories=privacy,ssl,security,mx (abgerufen am 2.3.2020)

Web-Server übergreifendes Tracking

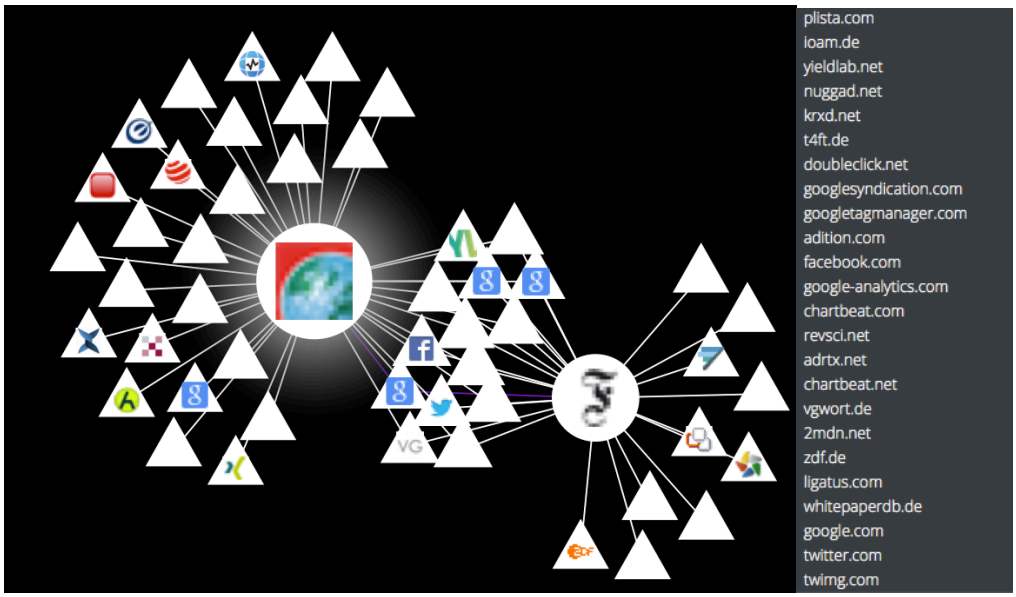
Für einen Tracker ist es wichtig, einen Anwender über Wochen, Monate oder sogar über Jahre in seinem Benutzerverhalten „beobachten" zu können. So wird aus den aufgerufenen Internetseiten ein immer detaillierteres Benutzerprofil. Das wird am einfachsten möglich, wenn der gleiche Tracker in vielen Webseiten einprogrammiert wurde. Wie ein Daten-Tracker seitenübergreifend arbeitet, zeigen die Plugins „disconnect" (Track the trackers)[113] und „lightbeam"[114] sehr anschaulich
Bei Aufruf eines Artikels von der Seite „focus.de" werden weitere 39 Daten-Tracker mitgeladen (hier mit „lightbeam" visualisiert:

113 https://disconnect.me

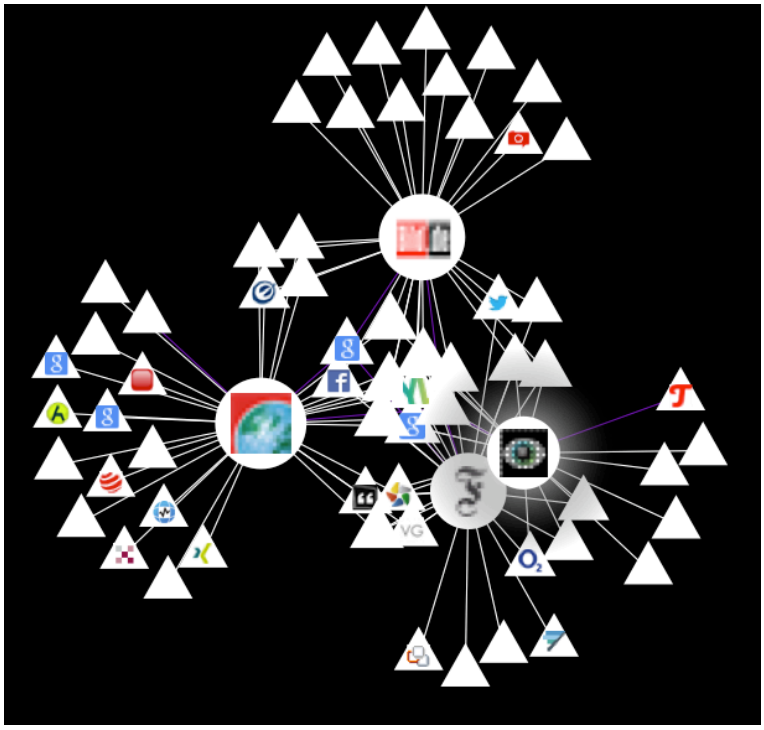
114 https://addons.mozilla.org/en-us/firefox/addon/lightbeam/



Wenn der Internetz-Nutzer anschließend einen „faz.net“ Artikel aufruft, kommen weitere 24 Tracker hinzu:



Wobei 14 dieser Tracker auch schon bei „focus.de“ geladen wurden.
Wenn der Nutzer danach noch einen „bild.de“ mit 30 Trackern (davon 4 gemeinsam mit der FAZ, 5 gemeinsam mit Fokus und 9 mit FAZ und Fokus gemeinsam) und einen „golem.de“ Artikel mit 22 Trackern aufruft, ergibt sich dieses Bild:



Nach diesen vier aufgerufenen Artikeln wissen 69 weitere Sites, welche Webseiten der Internet-Nutzer besucht hat. Darüber hinaus sind die Tracker auch noch untereinander verlinkt, wie man hier am Beispiel von „doubleclick“ (Googles Online-Werbe Unternehmen) sehen kann. Nicht nur alle vier vom Nutzer angesteuerten Seiten, sondern auch „elitepartner“ hat doubleclick verlinkt.

doubleclick.net

focus.de
elitepartner.de
faz.net
bild.de
golem.de

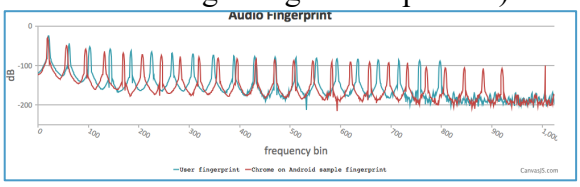
Mit Hilfe dieses Profils (Fingerabdrucks), kann ein Tracker auch noch Monate später erkennen, dass der gleiche Anwender sich jetzt für ein Themengebiet in einer Zeitung oder ein Produkt in Online-Shops interessiert. Die von den Daten-Trackern somit über einen langen Zeitraum ermittelten Datenprofile sind natürlich nur mit einer gewissen Wahrscheinlichkeit korrekt. Aber je eindeutiger das Browser-Profil (Fingerabdruck) des Nutzers ist, umso genauer und wertvoller ist das Verhaltensmuster, das ein Daten-Tracker im Laufe der Zeit über ihn erstellen kann.

Tracking ohne Cookies

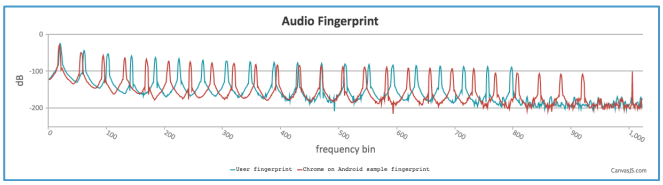
Neben Cookies gibt es einige weitere technische Möglichkeiten, seitenübergreifend den Nutzer wiederzuerkennen[115][116]:

- Flash-Cookies
- diverse HTML5-Speichertechniken
- PNG-Cookie (Cookie-ID in einer speziell angefertigten PNG-Datei gespeichert, die einige Browser via HTML-Canvas wieder auslesen können)
- History-Caching
- AudioContext Fingerprinting[117]
- WebRTC Local IP Discovery

Durch die Kombination mehrerer dieser Techniken entstehen Cookies, die nahezu unlöschbar sind und „Evercookies“ genannt werden[118].
Seit einiger Zeit werden verstärkt auch Browser-Profile mit Hilfe des Canvas-Fingerprinting erkannt [119].
Beim Canvas-Fingerprinting wird unbemerkt ein kleines, nicht angezeigtes Bild mit Hilfe der Grafikkarte des genutzten Rechners erstellt. Aufgrund der genauen Zeit, die für die Darstellung auf dem Bildschirm (Rendern) benötigt wird und die sich auf jedem Rechner geringfügig unterscheidet, kann man den Rechner recht eindeutig wiedererkennen.
Sowohl das AudioContext Fingerprinting als auch das Canvas-Fingerprinting haben den Vorteil, dass zwei verschiedene Browser auf dem gleichen Computer den gleichen Fingerprint liefern. Es nützt hier also auch nichts, verschiedene Browser zum Surfen und Einkaufen im Internet zu nutzen (was fälschlicher Weise einige Ratgeber empfehlen).



Safari



Firefox

Da mobile Devices keine Cookies unterstützen, ist das webseitenübergreifende Tracking auf mobilen Geräten eine besondere Herausforderung. Die Firma Flashtalking hat dazu über ihre Tochterfirma Device9 eine Technology entwickelt, die nach eigenen Angaben „mit einer 98-prozentigen Genauigkeit einzelne User einer In-App Impression und einer Conversion im Mobile Web aber auch andersherum, zuordnen können.“ Dass cookieloses Tracking effektiver sein kann als mit Cookies, hat gerade erst die TUI-Group fest gestellt[120].

---

[115] https://webtransparency.cs.princeton.edu/webcensus/

[116] http://www.heise.de/security/meldung/Das-Zombie-Cookie-1094770.html

[117] AudioContext Fingerprint

[118] http://samy.pl/evercookie/

[119] http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

[120] https://www.tracks-summit.de/news/2016-03-08-mobile-tui-group-testet-cookieloses-tracking/

Ghostery hat eine Auflistung der 50 Sachverhalte verfügbar gemacht[121], die ein Server erfährt, wenn der Nutzer eine Webseite besucht“, und ein Tool (BrowserSpy) [122] gebaut, mit dessen Hilfe jede einzelne Information abgefragt werden kann.

Session Replay

Mittlerweile genügt es den Trackingfirmen nicht mehr nur zu wissen, wer hat welche Web-Seite aufgerufen. Durch intelligenten Code, der in die Web-Seiten eingebaut wird, ist es möglich, dass man jegliche Mausbewegung oder sonstige Eingaben protokollieren und zur Auswertung heran ziehen kann. Das nennt sich „Session Replay“, also das nachträgliche Abspielen aller Nutzeraktionen auf einer Web-Seite. Dafür werden zunächst alle Nutzer-Interaktionen auf der Webseite vom Tracker mit protokolliert. Dabei werden dann auch sensitive Informationen wie Kreditkartennummern, Pins oder Passwörter mit übermittelt.
„freedom-to-tinker.com“[123] hat recht gut aufbereitet wie das funktionier, zeigt ein Beispiel-Video das aufzeigt, wie eine Tracker-Firma nachträglich die Interaktionen des Nutzers sehen kann und hat auch eine Liste von den Webseiten, die solche Technologien einsetzen[124]. Wordpress.com, microsoft.com und adobe.com stehen auf dieser Liste an erster Stelle:

121 https://purplebox.ghostery.com/post/1016024218

[122] http://browserspy.dk

[123] https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/

[124] https://webtransparency.cs.princeton.edu/no_boundaries/session_replay_sites.html

Alexa Rank	Website	Session Replay Company
29	yandex.ru	yandex.ru
35	wordpress.com	yandex.ru
45	microsoft.com	clicktale.net
74	adobe.com	clicktale.net
88	coccoc.com	yandex.ru
102	txxx.com	yandex.ru
124	godaddy.com	clicktale.net
136	uol.com.br	hotjar.com
140	indiatimes.com	hotjar.com
151	avito.ru	yandex.ru
164	outbrain.com	hotjar.com
177	hclips.com	yandex.ru
196	kinogo.club	yandex.ru
202	upornia.com	yandex.ru
209	spotify.com	sessioncam.com
211	livejournal.com	yandex.ru
228	skype.com	clicktale.net
245	softonic.com	hotjar.com
247	files.wordpress.com	yandex.ru
255	instructure.com	hotjar.com
266	wittyfeed.com	hotjar.com
279	rt.com	yandex.ru
282	taboola.com	hotjar.com
284	kinopoisk.ru	yandex.ru
288	tokopedia.com	hotjar.com
289	sh.st	hotjar.com
309	onedio.com	hotjar.com
310	upwork.com	sessioncam.com
316	telegraph.co.uk	sessioncam.com
318	abs-cbn.com	hotjar.com
329	eksisozluk.com	yandex.ru
335	hp.com	clicktale.net
345	seasonvar.ru	yandex.ru
348	sharepoint.com	clicktale.net
359	evernote.com	hotjar.com
370	sberbank.ru	yandex.ru
375	samsung.com	clicktale.net
383	conservativetribune.com	inspectlet.com
387	xfinity.com	userreplay.net
392	digikala.com	mouseflow.com
398	atlassian.net	clicktale.net

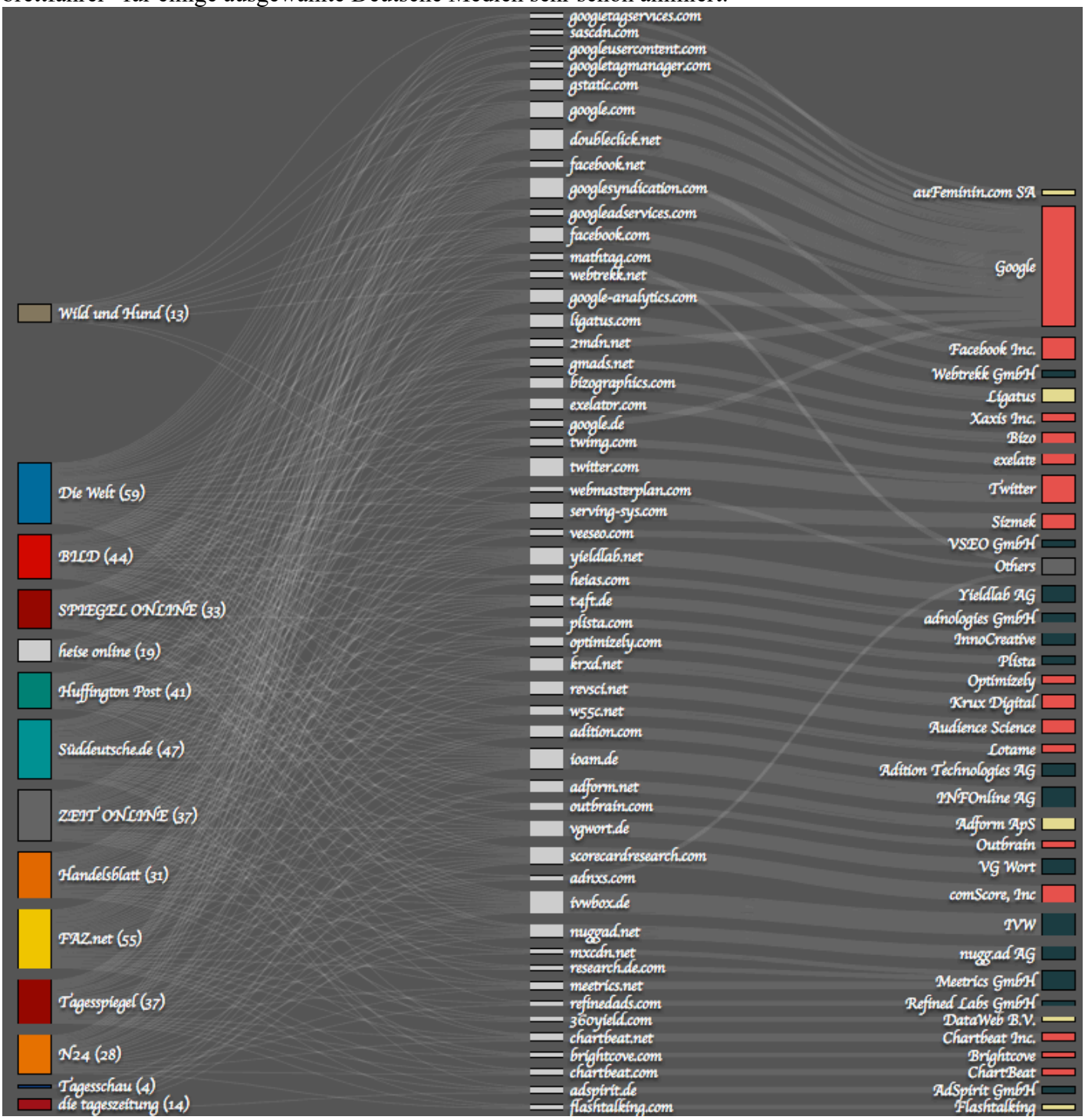
Alexa Rank	Website	Session Replay Company
403	avg.com	hotjar.com
416	leagueoflegends.com	hotjar.com
421	reuters.com	hotjar.com
437	beeg.com	yandex.ru
436	homedepot.com	clicktale.net
439	infusionsoft.com	hotjar.com
456	realclearpolitics.com	hotjar.com
464	udemy.com	hotjar.com
474	mercadolibre.com.ar	hotjar.com
485	hurriyet.com.tr	yandex.ru
485	hurriyet.com.tr	hotjar.com
494	ask.fm	yandex.ru
496	haber7.com	yandex.ru
505	asana.com	hotjar.com
511	hubspot.com	hotjar.com
513	prezi.com	hotjar.com
516	cbsnews.com	decibelinsight.net
520	goal.com	hotjar.com
522	souq.com	inspectlet.com
545	gismeteo.ru	yandex.ru
558	comcast.net	userreplay.net
560	bitbucket.org	clicktale.net
583	wiley.com	hotjar.com
590	lenta.ru	yandex.ru
593	mirror.co.uk	hotjar.com
597	hdzog.com	yandex.ru
602	yandex.ua	yandex.ru
609	asus.com	hotjar.com
610	adbooth.com	hotjar.com
631	ibm.com	hotjar.com
644	onlinevideoconverter.com	yandex.ru
643	rottentomatoes.com	clicktale.net
660	banggood.com	yandex.ru
659	cbssports.com	decibelinsight.net
663	drive2.ru	yandex.ru
677	ria.ru	yandex.ru
681	newegg.com	sessioncam.com
683	norton.com	clicktale.net
686	clickadu.com	hotjar.com
685	lenovo.com	fullstory.com

Dies sind die Top-Web-Seiten, die „Session-Replay“ nutzen

Da die TrutzBox Blockinglisten auch Session Replay Dienstleister beinhalten, werden diese, wie hier am Beispiel der Webseite steuerklassen.com, die das Session Replay Script „yandex“ laden möchte, daran gehindert (abgerufen am 15.1.2020):

⊘	13 GET https://fonts.googleapis.com/css?family=Gloria+Hallelujah&display=swap
⊘	16 GET https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js
⊘	17 GET https://use.fontawesome.com/releases/v5.7.2/css/all.css
⊘	19 GET https://cdnjs.cloudflare.com/ajax/libs/autonumeric/2.0.13/autoNumeric.js
⊘	30 GET https://cdn.jsdelivr.net/npm/yandex-metrica-watch/tag.js
⊘	31 GET https://fonts.googleapis.com/css?family=Gloria+Hallelujah&display=swap
⊘	38 GET https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js
⊘	45 GET https://use.fontawesome.com/releases/v5.7.2/css/all.css
⊘	47 GET https://www.googletagmanager.com/gtm.js?id=GTM-5CFPQHD
⊘	51 GET https://cdnjs.cloudflare.com/ajax/libs/autonumeric/2.0.13/autoNumeric.js
⊘	73 GET https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
⊘	74 GET https://www.google-analytics.com/analytics.js
⊘	75 GET https://www.googletagservices.com/tag/js/gpt.js
⊘	76 GET https://static-de.plista.com/async.js
⊘	77 GET https://static-de.plista.com/async/min.js
⊘	78 GET https://dev.visualwebsiteoptimizer.com/j.php?a=424699&u=https%3A%2F%2Fwww.steuerklassen.com%2F&r=0.2684744672058278

Eine recht vollständige Beschreibung der Daten-Sammler-Techniken ist in https://www.anonym-surfen.de/help/wwwprivacy_technik.html sehr gut beschrieben. http://newsreadsus.okfn.de hat diese „Trittbrettfahrer“ für einige ausgewählte Deutsche Medien sehr schön animiert:



http://newsreadsus.okfn.de/

Die Leser der Zeitschriften links werden mit Hilfe der Firmen rechts „überwacht“.

Wie werden Internet-Tracking Daten mit gesammelten Daten aus dem Alltag verknüpft?

Wie wir gesehen haben, werden wir regelmäßig bei der Nutzung des Internets beobachtet, und die dabei gesammelten Daten werden für immer gespeichert. Aber nicht nur im Internet hinterlassen wir Spuren, für die sich andere interessieren. Bewegungen werden mit Hilfe von Mobilfunk-Stationen und GPS-Tracking Daten erfasst und zentral gespeichert. Beim Einkaufen im Supermarkt nutzen wir eine Loyalty-Karte (z.B. Payback) oder bargeldloses Bezahlen mit Karte, und die Kartenfirmen freuen sich über die so erhaltenen Profile. Es freut sich nicht nur die Bank des jeweiligen Einkäufers, sondern vor allem der Karten-Prozessor, der die Karten-Transaktionen für die Bank und den Shop übernimmt. Wird beim Einkauf eine Loyalty-Karte verwendet, wurde ebenfalls zuvor zugestimmt, dass alle gewonnen Daten gespeichert und vermarktet werden dürfen.
Mit 5-6 Daten über eine Person ist jeder eindeutig identifizierbar, also nicht mehr anonym. Diese Daten können ganz unverfängliche Daten sein, wie benutztes Betriebssystem, ungefähre Lokation in der Sie sich aufhalten, benutzter Browser, Bildschirm Auflösung usw. Aus diesen Attributen wird ein möglichst eindeutiger Hash-Wert gebildet. Sobald Sie auch noch in Facebook, Google, Twitter oder Shop usw. eingeloggt sind, kann dieser Hash-Wert mit Ihrer dort hinterlassenen Identität verknüpft werden. Daraus kann dann ein erweiterter Hash-Wert entstehen, die der Datensammler mit anderen Hash-Werten von Datensammlern aus Ihrem realen Leben abgleicht.
Zu diesem Zweck arbeiten Internet-Datensammler wie Facebook mit anderen Daten-Vermarktern wie Acxiom, LiveRamp (gehört jetzt auch zu Acxiom), Epsilon[125], Datalogix (gehört jetzt zu Oracle) oder Bluekai (gehört jetzt auch zu Oracle) zusammen, um die Profile einer realen Person zuzuordnen und weiter zu vervollständigen.
Nur noch mal zur Erinnerung: Acxiom ist die Firma, die auch eine Zweigstelle in Deutschland hat, die Zugriff auf über 15.000 Datenbanken hat, inklusive Google, Facebook, PayPal, eBay, Yahoo und Twitter..., bis zu **3.000** einzelne Eigenschaften von weltweit etwa **700 Millionen** Menschen, davon auch Daten über 44 Millionen Deutsche hat. Aber auch die Partner-Liste der Firma LiveRamp liest sich wie das Who-is-Who der Online-Industrie[126]. Da sind auch Partner wie Linkedin, Twitter, Adobe, AOL, Facebook, eBay, Google, Instagram, Microsoft, u.a aufgeführt. Die Chance, dass jemand bei nur einem dieser Firmen einen Account hat, ist recht groß. Beide Firmen haben Ihre Netzwerke zum Austausch der Daten zusammen gefügt [127].
Übrigens zum Thema Paypal: vielleicht haben Sie sich schon einmal gefragt, mit was Paypal eigentlich Geld verdient. Nein, nicht nur mit Transaktionsgebühren, die der Shop zahlt. Auch mit Datenhandel. Über 1000 Firmen haben eine elektronische Verbindung zu den Paypal-Datenbanken. In den Paypal „Third-parties-list“ werden diese aufgeführt und dort kann man auch nachlesen, welche Daten an diese Firmen gehen[128]. Besonders Interessant sind die Verbindungen, die in Kapitel 7 unter „Marketing and Public Relations“ aufgeführt sind. Dort kann man alle großen Tracking-Firmen und Datenhändler finden, die von Paypal mit Daten versorgt werden.

[125] http://www.cnet.com/news/who-is-epsilon-and-why-does-it-have-my-data/

[126] http://liveramp.com/partners/

[127] http://adexchanger.com/data-exchanges/everything-you-wanted-to-know-about-liveramp-the-data-connecter-everyone-uses/

[128] https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list

Die Lüge von „anonymen Daten“

Die Juristen unterscheiden mit Recht zwischen „Personen bezogenen“ und „Personen beziehbare“ Daten. Wenn z.B. eine Krankenkasse alle Daten, die sie über einen Versicherten an Dritte weitergeben, vorher aber Vor- und Nachname aus den Datensätzen löschen würde, dann wären diese Daten recht einfach wieder auf einzelne Personen zurück zu führen. Nicht nur weil dann die Adresse des Versicherten weiterhin in den Datensätzen stehen würde. Selbst wenn die Adresse auch noch gelöscht würde, könnte man aufgrund der besuchten Ärzte den Wohnort eng einkreisen und alleine nur durch Beruf, Arbeitgeber, Alter den Versicherten schon auf 2 – 3 Personen einkreisen. An diesem Beispiel sieht man, dass Daten recht schnell wieder auf einzelne Personen zurück zu führen sind.
Sobald Daten zu jemanden gelangen, der diese Daten mit ähnlichen Daten verknüpfen kann, ist es möglich, die Anonymität zu reduzieren. Fachleute sind davon überzeugt, daß es somit gar keine anonyme Daten geben kann.[129].
In unserer digitalen Welt ist es natürlich auch keine Lösung, alle Daten zurück zu halten. Ein gewisser Datenaustausch muss stattfinden. Und ein gewisser Informationsaustausch gab es auch schon immer, auch schon bevor es Computer gab. Ich möchte ja auch, dass mein Hausarzt meine Daten von meinem MRT-Scan bekommt.
Aber niemand möchte, dass eine Datensammelfirma seine sehr privaten Daten sammelt und an jeden weiter gibt, der sie dafür bezahlt. Ohne dass einer Weitergabe zugestimmt wurde. Juristisch wird das nie genau abgrenzbar sein. Somit bleibt nur die Alternative, dass nur diejenigen Daten über mich bekommen sollten, denen ich vertrauen kann. Ansonsten ist Datensparsamkeit eine wichtige Voraussetzung dafür, dass meine persönlichen Daten nicht missbraucht werden können. Also man sollte möglichst Wissen, wer welche Daten von mir bekommt und ansonsten gibt es keine Daten über mich.

Wie können Tracker meine echte Identität herausfinden?

Man könnte annehmen, dass die Tracker im Internet immer nur einen Fingerabdruck des Computers einem Nutzungsprofil zuordnen können. Also gar nicht herausfinden können, welche Person zu diesem Nutzungsprofil gehört. Aber die Tracking-Industrie ist hierzu in der Lage, und das geschieht auch meistens. Die Erweiterung der im Internet anonym gewonnen Profile mit weiteren Daten, geschieht durch „Onboarding“ [130]. Und mit Hilfe dieser Onboarding-Firmen (z.B. die Firma LiveRamp), werden unsere anonym gesammelten Internetprofile mit schon bekannten, nicht anonymen Daten verknüpft. Nicht mehr anonyme Daten können Konten im Internet sein, auf die man sich mit echten Daten einloggt und die evtl. sogar die eigene Adresse besitzen, um Waren an sich liefern zu lassen; oder auch nur die Mailadresse bei Facebook oder die Telefonnummer bei Whatsapp, die sehr einfach mit der jeweiligen Person verknüpft werden kann. Da Whatsapp auch noch die Telefonnummer an alle Facebook-Tochterfirmen weitergibt, hat Facebook weitere Möglichkeiten geschaffen, einen anonymen Nutzer sogar auf einer Nicht-Facebook-Seite zu de-anonymisieren[131].

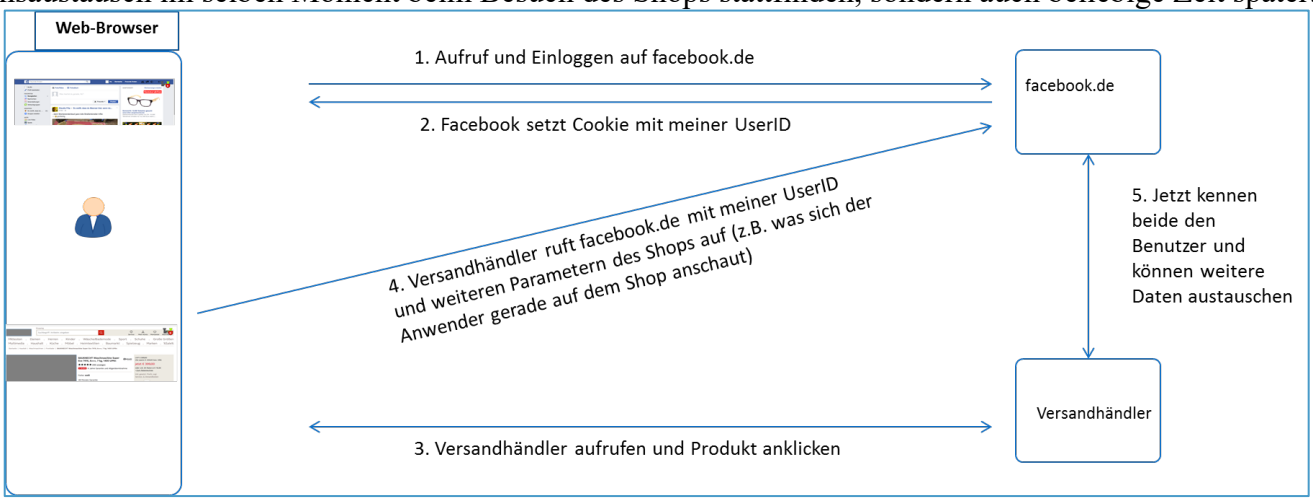
[129] https://netzpolitik.org/2019/weitere-studie-belegt-luege-anonymer-daten/

[130] http://adexchanger.com/data-exchanges/everything-you-wanted-to-know-about-liveramp-the-data-connecter-everyone-uses/

[131] http://mirror.netcologne.de/CCC/contributors/ulm/radio/devradio322_nomusic.mp3

Wie können verschiedene Trackerfirmen ihre Daten untereinander austauschen?

Diese Verbindung von mehr oder weniger anonymen Tracker-Daten, zusammen mit anderen schon zuvor gesammelten Daten (onboarding), lässt letztendlich der Browser zu, nennt sich "cookie syncing"[132] und funktioniert folgendermaßen:
Angenommen, der Browser lädt eine Seite, in der die Tracker-Firma A einen Cookie setzt (hier im Bild ist das facebook.de). Tracker-Firma-A generiert für diesen Nutzer einen eindeutigen Schlüssel. Dieser eindeutige Schlüssel wird auch „Personally Identifiable Information (PII)“ oder auch „Sensitive Personal Information (SPI)“ genannt. Dieser eindeutige Schlüssel des Anwenders wird in dem Cookie der Tracker-Firma-A auf dem PC des Anwenders abgespeichert. Dieser Cookie kann über Monate, sogar über Jahre auf dem PC des Anwenders verbleiben.
Irgendwann einmal ruft der Anwender anonym die Seite eines Internet-Shops (Versandhändler) auf und schaut sich einige Produkte an. Ein Tracker oder die Seite des Versandhändlers selbst ruft nun Tracker-A (facebook.de) auf und übergibt dabei sowohl den facebook-cookie mit meiner eindeutigen Facebook-Id als auch ein eindeutiger Session-Key des Versandhändlers und evtl. weitere Informationen über die Produkte die ich mir auf dem Shop gerade anschaue. Jetzt weiß nicht nur Facebook für welche Produkte ich mich auf dem Shop gerade interessiere, jetzt ist der Facebook-Server in der Lage den Shop-Server zu kontaktieren und mit diesem eindeutigen Session-Key beliebige Daten über alles was Facebook und der Shop schon über mich wissen, auszutauschen. Da sowohl Facebook über Login-Daten, als auch der Shop mit Hilfe des Fingerprints des Browsers, mich auch später wieder identifizieren können, kann Informationsaustausch im selben Moment beim Besuch des Shops stattfinden, sondern auch beliebige Zeit später.



(© 2016 Comidio GmbH)

Mit diesen Mechanismen wird ein anonymer Besucher einer Webseite nicht nur de-Anonymisiert, es ist auch möglich, einem Benutzer mehrere Devices (PC, iPhone, iPad…) zuzuordnen. Es nützt somit auch nichts, z.B. einen PC oder Browser für Einkaufen und Banking zu nutzen und einen anderen für das Surfen im Internet. Diese Tracker-Mechanismen können erkennen, dass der gleiche Nutzer genau diese beiden PCs benutzt. Es nützt auch nichts zwischendurch die Cookies zu löschen, da diese durch die Verwendung von Evercookies, durch cookie-sync wieder hergestellt werden[133].
Die TrutzBox verhindert schon in ihrer Standard-Einstellung diese Art der De-Anonymisierung.

[132] https://freedom-to-tinker.com/blog/englehardt/the-hidden-perils-of-cookie-syncing/

[133] https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf

Beispiel: De-Anonymisierung eines Shop-Besuchers mit Hilfe der TrutzBox nachvollziehen.

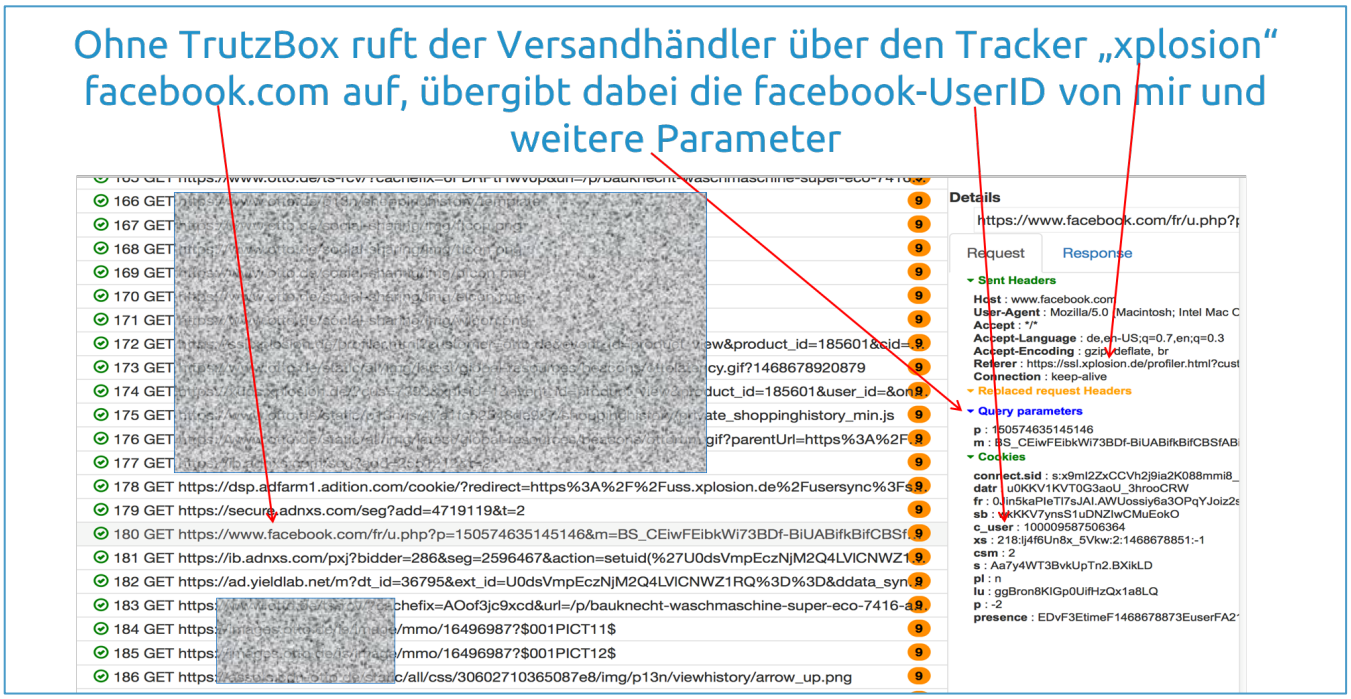
Wer sich jemals über Werbung in Facebook gewundert hat, über Produkte, die man sich irgendwann einmal zuvor auf einer ganz anderen Webseite angeschaut hat, der kann die Ursache am Beispiel eines „Online-Versandhändlers“ im Zusammenspiel mit Facebook folgendermaßen nachvollziehen.
Da die TrutzBox einen solchen Datenaustausch verhindert, muss für einen solchen Test zuvor die Filterfunktion der TrutzBox abgeschaltet werden.
Zuerst in Facebook einloggen. In Facebook kann man sehen, dass ein Cookie geschrieben wird:

(©2016 Comidio GmbH)

Wenn man dann irgendwann den Online-Versandhändler aufruft und ein Produkt anwählt, dann sendet die Versandhändler-Seite über diesen http-get-Befehl an Position 180

GET https://www.facebook.com/fr/u.php?p=150574635145146&m=BS_CWDb0BSUCEi7AWDf-BiUABifkBSU0WifABifABifABfrr

den Facebook-Cookie zurück an Facebook:



(©2016 Comidio GmbH)

Und somit hat der Versandhändler Facebook mitgeteilt, dass sich dieser Facebook-User mit der id: 100009587506364, gerade das Produkt xyz bei dem Versandhändler angeschaut hat. Dabei ist es technisch auch möglich, dass der Versandhändler jetzt über den http-Response auch die Facebook Identität des Versandhändler-Besuchers mitgeteilt bekommt. Da aber auch die Server des Versandhändlers und Facebook miteinander kommunizieren können, ist es ab jetzt möglich, dass auch die Server Daten über diesen einen Benutzer austauschen. Da der Anwender jetzt bekannt ist, können die Server jetzt problemlos diese Daten mit weiteren, dritten Partnern austauschen, auch um Daten, die diese anderen Tracker irgendwann einmal ermittelt haben, ergänzen.
Bei der Übertragung des Cookies an Facebook, kann man im http-header-Feld „Referer“ nicht nur erkennen, dass hier auch die Produkt-Id des Versandhändlers an Facebook übermittelt wird (customer=Versandhaendler&event_id=product_view&product_id=371528), man kann auch sehen, dass diese Versandhändler <-> facebook Verbindung durch ssl.xplosion.de initiiert wird.

Wer ist Xplosion?

Die Firma **Xplosion Interactive** ist ein Tochterunternehmen der Deutschen Telekom[134]**.** Die Domain xploision.de gehört jetzt der Firma emetriq (www.emetriq.com), die hier auf der Webseite des Versandhändlers aktiv ist. Emetriq ist auch ein Tochterunternehmen der Deutschen Telekom, das laut ihrer Webseite „*starke Partner der Digital Advertising Branche zusammen bringt, um über eine strategische Kooperation, der Intelligent Data Alliance (IDA), gemeinsam den größten deutschen Datenpool zu etablieren*“. Die Partnerschaft von xplosion.mit der Firma AdAudience ermöglicht es „*… weite Teile der Daten der über AdAudience organisierten Premium-Vermarkter – Axel Springer Media Impact, G+J Electronic Media Sales (G+J EMS), IP Deutschland, iq digital media marketing, OMS, SevenOne Media und*

[134] http://www.wuv.de/digital/otto_konzern_verkauft_retargeting_firma_an_telekom

TOMORROW FOCUS Media – mit denen von InteractiveMedia zu bündeln und diese für die Vermarktung zugänglich zu machen“[135]. Über diese „*Intelligent Data Alliance (IDA)“* kann man unter www.adaudience.de/ida auch folgende Details nachlesen, die aufzeigen, welche Deutschen Medienunternehmen hierüber Daten austauschen:

- **AdAudience** ist ein Joint Venture, der Vermarkter Axel Springer Media Impact, G+J Electronic Media Sales, IP Deutschland, iq digital media marketing, OMS, SevenOne Media und TOMORROW FOCUS Media. Als Targeting-Spezialist bündelt AdAudience die Online-Reichweite seiner sieben Gesellschafter und ermöglicht zielgruppenspezifische Werbekampagnen über ein einzigartiges Portfolio. Hiermit ist AdAudience einer der führenden Anbieter im Data Driven Advertising. Weitere Informationen finden Sie unter www.AdAudience.de.

- **xplosion interactive** ist Spezialist für datengetriebene Online Advertising-Lösungen. Basierend auf unserer fundierten Daten- und Technologiekompetenz bieten wir unseren Kunden innovative Lösungen zur Erhöhung von Relevanz und Präzision ihrer Digitalkampagnen. Vermarkter und Werbetreibende profitieren dabei von unserem breiten Produktspektrum, das von Retargeting bis hin zu ausgefeilten datengetriebenen Lösungen reicht. Mit unserem Team aus Datenspezialisten und Realtime-Experten ermöglichen wir Unternehmen den Einstieg ins Data Driven Advertising. Unser Kundenportfolio umfasst Top 10-AGOF-Vermarkter sowie führende Werbetreibende auf dem deutschen Markt. Xplosion interactive ist ein Unternehmen der Deutschen Telekom Gruppe.

- **InteractiveMedia – Der Digitalvermarkter** “Stories you love. Data you trust.“: Unter diesem Claim setzt InteractiveMedia seine Kompetenz rund um Daten, Premium-Umfelder sowie Zielgruppen- und Konzeptvermarktung ein, um individuelle Markeninszenierungen über alle digitalen Kanäle hinweg zu realisieren. Rich Media und Native Advertising werden dabei mit klassischen Display-Werbeformaten und neuen Bewegtbildprodukten intelligent verknüpft. Parallel werden kontinuierlich innovative Werbeformate auch für den automatisierten Handel (Stichwort: Programmatic Advertising) entwickelt. Für umfeldorientierte Werbung stellt InteractiveMedia seinen Kunden Premium-Inventar zur Verfügung. Im Bereich Display-Werbung (Online und Mobile) verfügt InteractiveMedia über ein einzigartiges Vermarktungsangebot an renommierten Medienmarken (wie T-Online, gutefrage.net, kicker.de) und Apps sowie thematisch orientierte Verticals. In der Bewegtbildvermarktung nimmt InteractiveMedia, neben dem Angebot an „klassischem“ Online-Video Advertising eine Ausnahmestellung im Zukunftsmarkt SmartTV und IPTV ein. Die InteractiveMedia CCSP GmbH ist ein Unternehmen der Deutschen Telekom Gruppe und Veranstalter des renommierten Kreativwettbewerbs für digitale Werbung „new media award“.

Somit ist auch der Austausch von Tracking-Daten über alle dieser Unternehmen technisch möglich. Durch das Unternehmen „***InteractiveMedia“*** werden auch sowohl SmartTV als auch IPTV (Internet-Fernsehen) mit eingebunden.
Diese Zusammenarbeit lässt sich recht einfach nachvollziehen: nachdem man sich für einen Artikel des Versandhändlers interessiert hat, wird von der Versandhändler-Seite xplosion.de aufgerufen, die einen Cookie mit dem Wert:

„pid_signature=Wd5lwqWbBiwkWC_FHSjlWScDWq5jWqBFWQwFwD5jwCWbwSU8Wsf0E_rr“

[135] http://www.adaudience.de/ida/

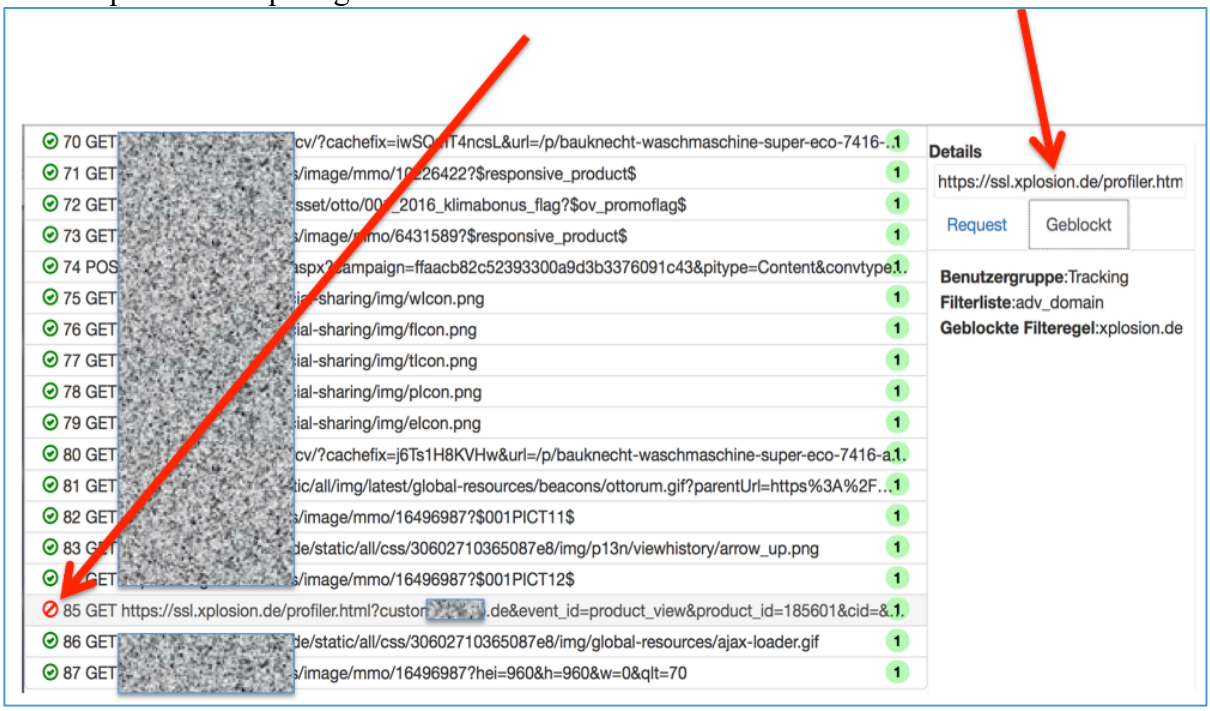
setzt. Wenn man danach einen Artikel auf focus.de liest, wird von der focus.de Seite auch xplosion.de aufgerufen, die wiederum einen Cookie mit dem Wert:

„pid_signature=Wd5lwqWbBiwkWC_FHSjlWScDWq5jWqBFWQwFwD5jwCWbwSU8Wsf0E_rr“

setzt. Durch diese beiden gleichen pid_signatures zeigt uns xplosion.de an, dass hier erkannt wurde, dass der gleiche PC diese beiden unterschiedlichen Seiten aufgerufen hat.
Und auch hier in focus.de wird wieder facebook über den Besuch des Focus-Artikels informiert, indem focus.de den facebook-Cookie mit dem Wert

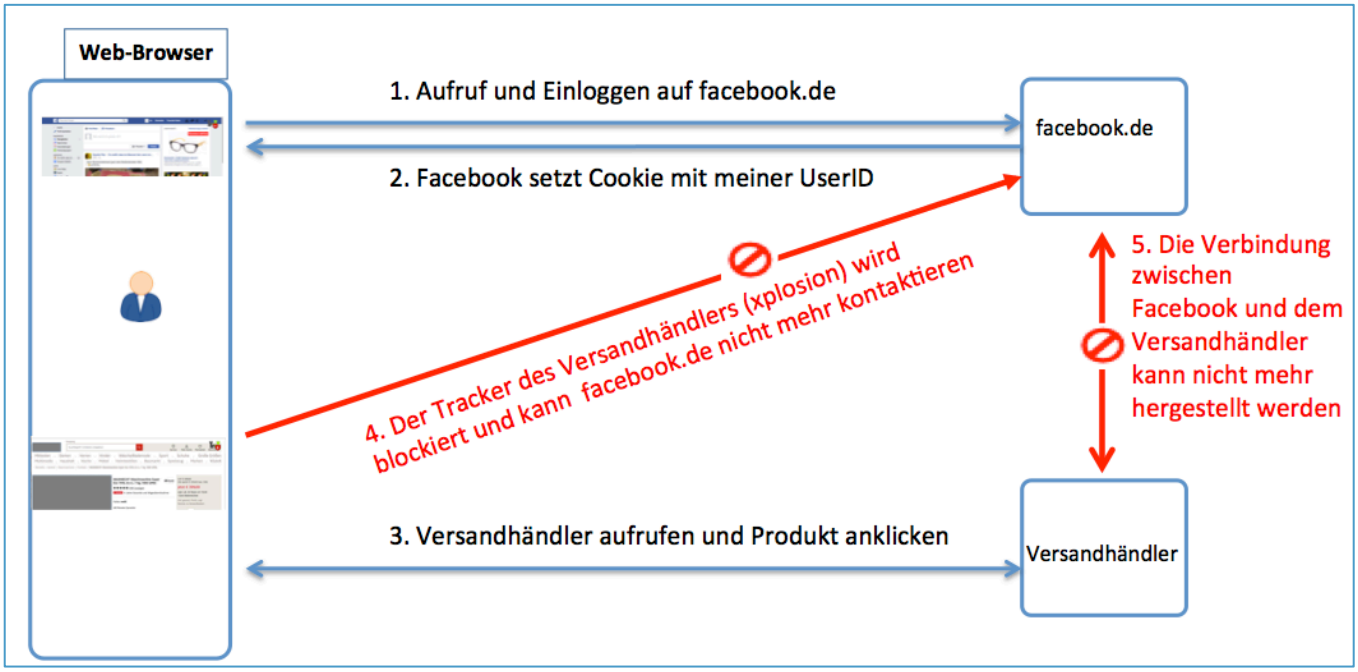
„c_user=100009587506364“

an Facebook übermittelt. Allerdings wird in focus.de diese focus.de <-> facebook Verbindung nicht durch xplosion.de initiiert, sondern durch imrworldwide.com, eine Domain, die von markmonitor registriert wurde.
Weitere Beispiele, wie Tracker browserseitig zusammen gefügt werden, lassen sich auch sehr gut bei HuffingtonPost in Verbindung mit AOL (deren Mutter), Google und Facebook reproduzieren.
Nicht unerwähnt bleiben sollte, dass die TrutzBox diese Art der Zusammenarbeit von Tracking-Firmen verhindert. Das erreicht die TrutzBox dadurch, dass in der Standardeinstellung Tracker-Firmen wie xplosion, Social-Media-Links wie zu Facebook und Third-Party-Cookies verhindert werden (Flag: „Cookies von fremden Seiten blockieren”). Zusätzlich werden in der TrutzBox Standard-Einstellung Tracker wie xplosion komplett geblockt:



(©2016 Comidio GmbH)

Die Webseite des Tracks-Summit verdeutlicht, an welchen Technologien Tracking-Firmen arbeiten, um in Zukunft diesen Datenaustausch weiter zu optimieren. In Zukunft möchte man dazu vor allem auf Cookies verzichten: https://www.tracks-summit.de/news/2016-03-08-mobile-tui-group-testet-cookieloses-tracking/.
Aber auch ohne dass ein Tracker Cookies verwendet, ist die TrutzBox in der Lage, Tracking zu verhindern. Gerade diese Beispiele zeigen, dass es nicht genügt, einfach bekannte Tracker zu blockieren. Es gibt mittlerweile viele weitere technische Möglichkeiten, über Cookies und Canvas das Benutzerverhalten durch Server zu tracken. Auch dies kann die TrutzBox blockieren.



(©2016 Comidio GmbH)

Tracking trotz abgeschalteten JavaScript und Cookies

Dass es auch möglich ist, bei abgeschalteten JavaScript und Cookies einen User wiederzuerkennen, zeigen diese Mechanismen, die in der Praxis auch eingesetzt werden:

- Das http-header Feld „Etag“ nutzen.[136]. Also im Prinzip genau das gleiche wie mit Cookies – mit dem entscheidenden Unterschied, dass diese Etags natürlich auch geschickt werden, wenn der Anwender Cookies durch die Einstellungen oder entsprechende Erweiterungen blockiert. Webseiten können mit solchen Cache-Cookies sogar Anwender wiedererkennen, die JavaScript abschalten und den privaten Modus des Browsers benutzen.

- das Auslesen der Mail-Adresse des Nutzers. Dabei liest die Tracking-Software die E-Mail Adresse (oder auch mehrere E-Mail-Adressen) aus dem „Login-Manager“ des Browsers und nutzt diese dazu, einen Nutzer auf einer anderen Seite oder zu einem anderen Zeitpunkt

[136] http://www.heise.de/security/meldung/User-Tracking-im-Web-Forscher-warnt-vor-heimtueckischer-Tracking-Technik-2048507.html

wieder zu erkennen. Eine Analyse von rund 50.000 Webseiten durch Sicherheitsforscher der Princeton University zu dieser Art von Tracking ist hier[137] nachzulesen.

- Selbst das Abschalten von Java-Script schützt nicht vor Tracking, da es auch mit Hilfe von Cascading Style Sheets (CSS) möglich ist, dem Tracker-Server ein Fingerprint zu liefern[138].

Diese Beispiele zeigen, wie wichtig es für die Anonymisierung ist, dass zum einen der http-header kontrolliert wird und die Blocking-Listen optimal „gefüllt“ sind. Und genau hier zeigt die TrutzBox ihre besondere Stärke.

Mobile Devices

Zusätzlich finden immer mehr Angriffe auf mobile Geräte statt, unabhängig davon ob sie mit MS/Windows, Google Android oder Apple iOS arbeiten. Auf mobilen Geräten ist vor allem das Ausspähen von Nutzerdaten sehr einfach geworden, da die Apps direkt über proprietäre Protokolle mit dem Apps-Server verschlüsselt kommunizieren können, sodass eine Firewall keine Chance hat, die Datenkommunikation zu kontrollieren. Dazu kommt, dass dank Android-ID oder IMEI es den Daten-Spionen besonders leicht gemacht wird, ein mobiles Gerät zu identifizieren und einen Nutzer wiederzuerkennen. Und ein mobiles Devices ist ein besonders interessantes Ziel bei dem ausspionieren von persönlichen Daten, da es auch den Standort seines Nutzers ständig kennt. Das mobile Device kennt auch dann noch seinen Standort, wenn man GPS ausschaltet, da es immer mit einer oder mehreren Mobilfunk Basisstation verbunden ist. Meist hat der Nutzer des Smartphones auch noch Bluetooth oder WLAN eingeschaltet. Beide Kommunikationsprotolle haben die unangenehme Eigenschaft, dass sie ständig nach Kommunikationspartnern suchen und es damit Hot-Spots möglich ist, die Geräte zu erkennen und deren Besitzer zu tracken. Inwieweit es erlaubt ist, auf solche Ortungs-Daten zuzugreifen, ist nicht nur in jedem Land unterschiedlich geregelt. In USA gibt es sogar in jedem Bundesstaat dazu unterschiedliche Regelungen[139].
Eine im März 2018 erstellte Studie, bei der 160.000 der meist benutzen Android-Apps untersucht wurden, hat ergeben, dass 55% dieser Apps versuchen den Standort zu ermitteln und 30% der Apps auf die Kontaktliste des Android-Smartphones zuzugreifen[140][141].

Tests der Zeitschrift „ct“ haben ergeben:

Die Musik-App Shazam sammelt Ortungsdaten und übergibt sie an Werbepartner. Das Spiel "Wer wird Millionär? 2014" spioniert aus, welche Apps der Nutzer sonst noch installiert hat - ohne dass man überhaupt weiß, dass das Spiel auf diese Informationen zugreifen darf. Sonys Fernlöschdienst MyXperia merkt sich Telefonnummern und die letzte Position von Handys, selbst wenn man den Dienst nie aktiviert hat. Fast alle Apps senden systematisch Details wie Kennnummern und Geräte-Infos an Werbepartner

[137] https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/

[138] https://www.heise.de/newsticker/meldung/Crooked-Style-Sheets-Bespitzeln-mit-CSS-3950124.html

[139] https://www.aclu.org/map/cell-phone-location-tracking-laws-state

[140] https://drive.google.com/file/d/1yoeZWznO9H_KZ3YZE2vAQExpzwOV25MQ/view

[141] https://www.buzzfeed.com/nicolenguyen/how-apps-take-your-data-and-sell-it-without-you-even

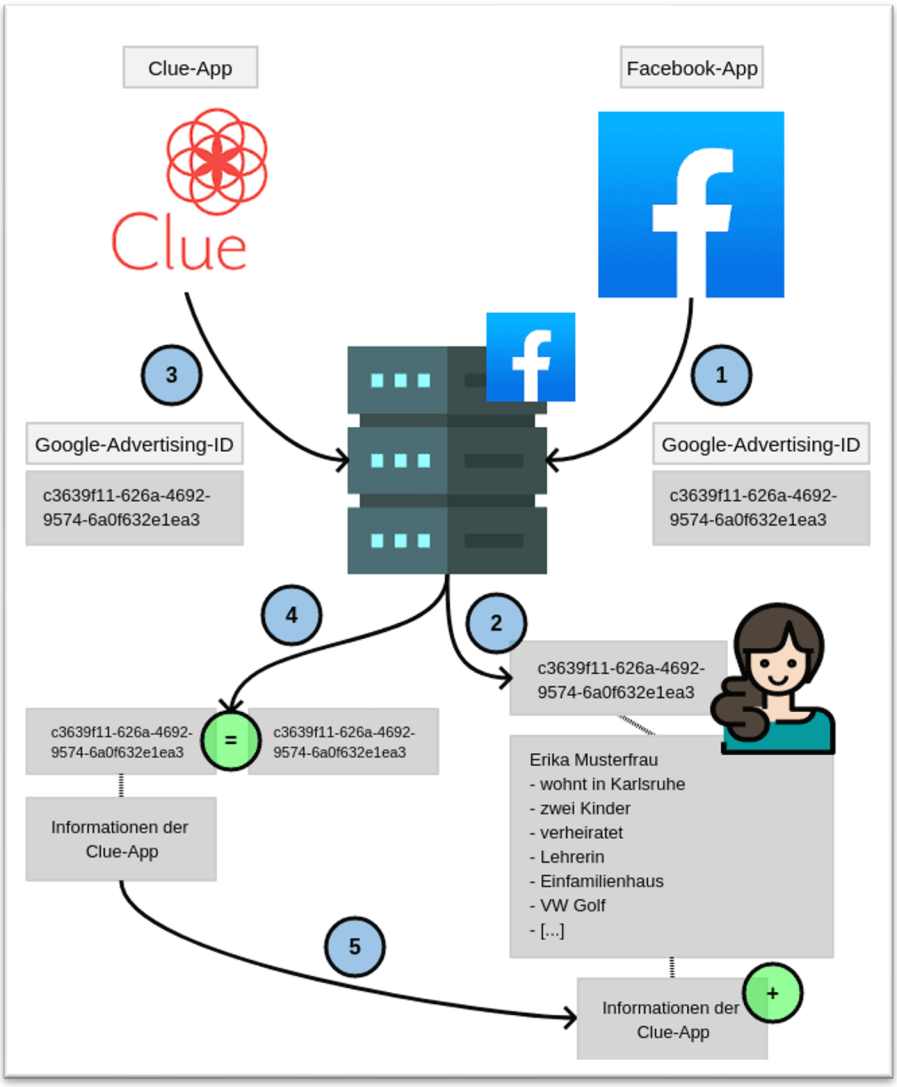
und Statistikunternehmen. Vereinzelt speichern sie auch Adressbücher, Ortsdaten und Netzwerkinformationen.

Die Hersteller von iOS und Android haben eine Werbe-ID eingeführt, die von Werbesystemen genutzt werden sollen, um den Nutzer wiederzuerkennen. Google schreibt Entwicklern seit August 2014 vor, nur noch diese zu Werbezwecken zu verwenden. Viele halten sich aber nicht daran.[142]
Auf der Google I/O 2016 hat Google für das Betriebssystem Android die sogenannte „Awareness-API" vorgestellt. Sie gibt Apps Informationen über den aktuellen Gerätekontext und erweitert damit die Informationen, die sich bisher weitgehend auf die Abfrage des Standorts beschränken. Zu den Kontext-Informationen gehört das aktuelle Wetter, die Nutzeraktivität und Beacons in der Nähe. So kann eine App beispielsweise dann aktiv werden, wenn Nutzer sich einem bestimmten Beacon nähern. Auch die Kombination mit anderen Kontextinformationen beziehungsweise Datum und Uhrzeit sind möglich. So ließen sich Nutzer warnen, wenn sie am Wochenende den geographischen Bereich ihrer Arbeit betreten, oder eine Musik-App reagiert mit einem passenden Soundtrack, wenn der Smartphone Besitzer den Kopfhörer einsteckt und mit Joggen beginnt. [143].
Apps, die diese Erweiterung nutzen, können somit den Anwender noch genauer tracken und das Profil des Nutzers noch weiter verfeinern. Inwieweit das nur der Programmierer der Apps kann oder auch Google in der Lage sein wird, alle diese Daten zu erfassen, muss noch analysiert werden.

Mike Kuketz hat in seinem Blog kuketz-blog.de am Beispiel der Menstruations-App „Clue" sehr anschaulich aufgezeigt, welche Daten diese App an Facebook liefert.

[142]http://www.datenschutzkanzlei.de/2014/10/01/tracking-auf-smartphones-was-die-werbe-id-über-nutzer-verrät/

[143] http://www.heise.de/developer/meldung/Little-App-is-watching-you-Google-veroeffentlicht-Awareness-API-3250311.html



https://www.kuketz-blog.de/wie-tracking-in-apps-die-sicherheit-und-den-datenschutz-unnoetig-gefaehrdet/

Aber nicht nur Facebook bekommt häufig Daten von Apps. Das Infoportal für sichere Handynutzung „MobilSicher“ hat hier eine Liste häufig adressierter Drittanbieter zusammengestellt: https://app-check.mobilsicher.de/drittanbieter

„The Wall Street Journal“ stellt eine gute Übersicht zur Verfügung die zeigt, welche der verbreitetsten Apps welche Daten sammelt[144].

Die Firma NSO Group entwickelt und verkauft Werkzeuge, mit denen sogar die neuesten Generationen von IPhones ausspioniert werden können[145]. Deren Werkzeuge werden vor Allem von staatlichen Institutionen benutzt.

Die „University of Oxford” hat eine Analyse von 1 Mio. kostenloser Android-Apps durchgeführt und ermittelt, ob und welche Tracker diese Apps haben und wie diese Trackerfirmen rechtlich miteinander

[144] http://blogs.wsj.com/wtk-mobile/

[145] http://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html?_r=1

verbunden sind. Wie zu erwarten liegt das Unternehmen Alphabet mit seinen Tochterunternehmen mit 88,44% aller analysierten Apps, die von den Tochterunternehmen von Alphabet getrackt werden, an vorderster Front.

Root parent	*% apps*	*Subsidiary*	*% apps*	*Country*
Alphabet	88.44	Google	87.57	US
		Google APIs	67.51	US
		DoubleClick	60.85	US
		Google Analytics	39.42	US
		Google Tag Manager	33.88	US
		Adsense	30.12	US
		Firebase	19.20	US
		Admob	14.67	US
		YouTube	9.51	US
		Blogger	0.46	US
Facebook	42.55	Facebook	42.54	US
		Liverail	1.03	US
		Lifestreet	<0.01	US
Twitter	33.88	Twitter	30.94	US
		Crashlytics	5.10	US
		Mopub	2.51	US
Verizon	26.27	Yahoo	20.82	US
		Flurry	6.28	US
		Flickr	1.37	US
		Tumblr	1.22	US
		Millennialmedia	0.71	US
		Verizon	0.11	US
		AOL	0.06	US
		Intowow	<0.01	US
		One By AOL	<0.01	US
		Brightroll	<0.01	US
		Gravity Insights	<0.01	US
Microsoft	22.75	Microsoft	22.11	US
		Bing	0.12	US
		LinkedIn	20.62	US
Amazon	17.91	Amazon Web Services	11.57	US
		Amazon	7.72	US
		Amazon Marketing Services	1.73	US
		Alexa	<0.01	US
Unitytechnologies	5.78	Unitytechnologies	5.78	US
Chartboost	5.45	Chartboost	5.45	US
Applovin	3.95	Applovin	3.95	US
Cloudflare	3.85	Cloudflare	3.85	US
Opera	3.20	Adcolony	3.12	US
		Admarvel	0.09	US

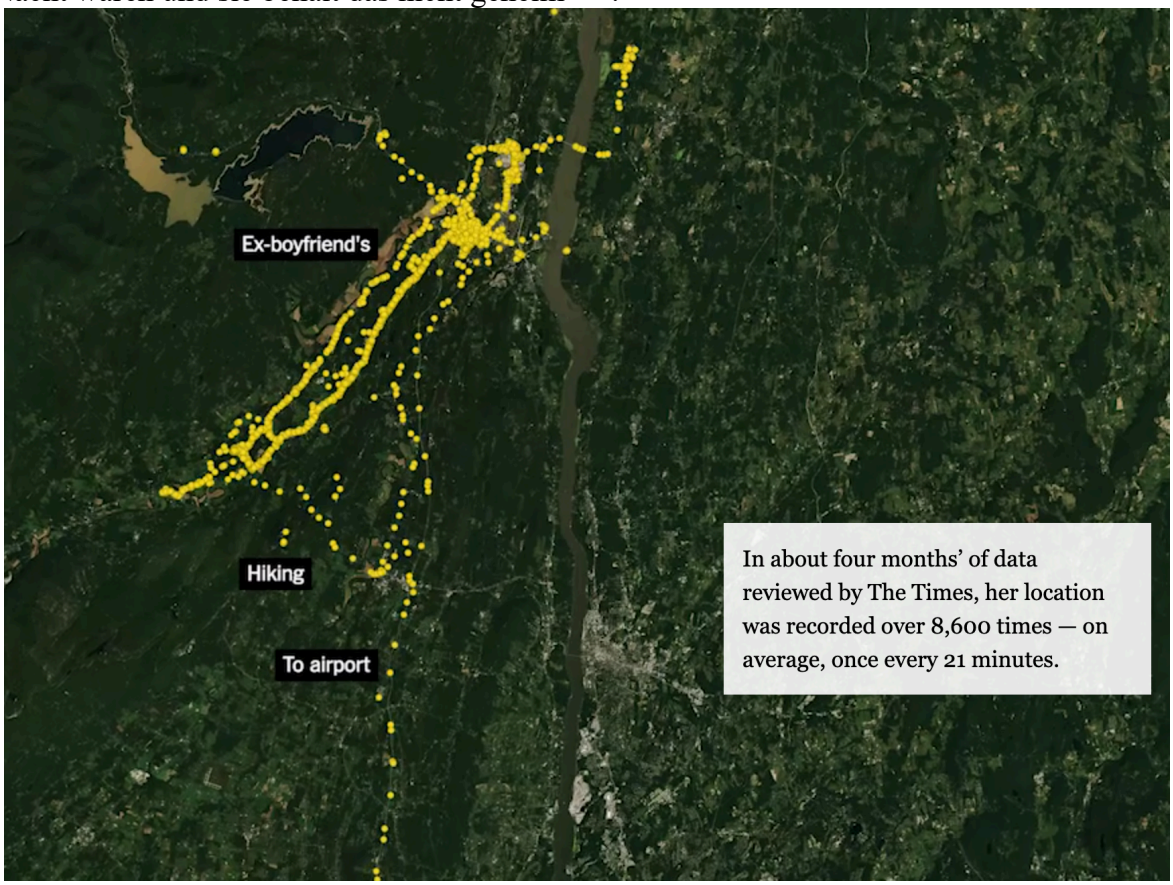
Quelle: https://arxiv.org/pdf/1804.03603.pdf

Diese Apps liefern auch sehr vertrauliche Daten an diese Firmen[146]. Manche Apps liefern sogar komplette Bildschirmkopien ohne den Nutzer darüber zu informieren[147].

[146] https://www.heise.de/newsticker/meldung/Apps-liefern-Facebook-vertrauliche-Daten-Untersuchung-angekuendigt-4316943.html?wt_mc=nl.mac-and-i.2019-02-25

[147] https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots

Ende 2018 erschien in der NYTimes ein sehr anschaulicher Artikel mit dem Titel „Ihre App weiß wo Sie letzte Nacht waren und sie behält das nicht geheim“[148].

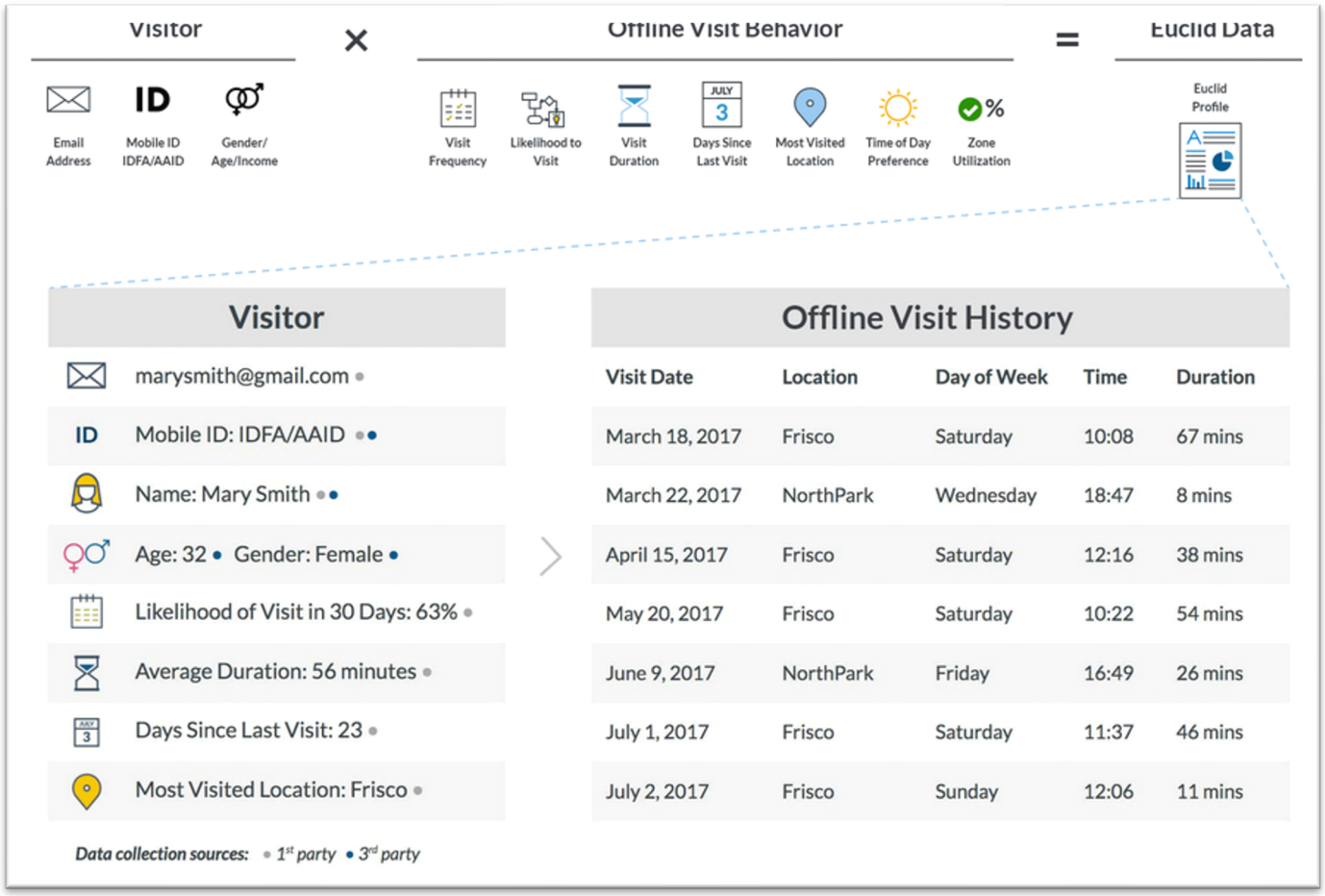


https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

Mobiles Tracking durch WLAN-Hotspots

Die meisten Smartphones sind so konfiguriert, dass sie automatisch nach schon bekannten WLAN-Hotspots suchen. Das ist sehr bequem, da damit sofort wenn man nach Hause, in die Firma oder ins Hotel kommt in dem man sich zuvor am Hotel-WLAN angemeldet hatte, die teure LTE Internet-Verbindung durch einen kostenlosen WLAN-Zugang ersetzt wird. Leider hat diese Funktion zur Folge, daß das Smartphone permanent seine WLAN-Identität per WLAN sendet, in der Hoffnung, ein bekannter WLAN-Hotspot meldet sich darauf hin.
Diese Funktion wird genutzt um Smartphones und dessen Besitzer zu tracken. Als Beispiel dazu dient der Service der Firma Euclid (geteuclid.com). Mit Hilfe deren Service ist z.B. ein Kaufhaus, ein Ladengeschäft oder eine Stadt in der Lage deren Besucher zu analysieren.

[148] https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html



Source: geteuclid.com

Dazu werden die Smartphone Daten des Besuchers abgerufen und mit zuvor ermittelten Daten abgeglichen. Der Euclid-Kunde, also der Ladenbesitzer, bekommt damit eine aufbereitete Liste aller Besucher. Diese Liste beinhaltet neben einer Statistik wie oft der Bsucher das Geschäft betritt, auch die E-Mail-Adresse, den Namen das Geschlecht und das Alter des Besuchers.

Tracking Schutz für mobile Devices

Gerade für mobile Devices würde man sich besonders Werkzeuge zum Schutz vor Überwachung wünschen. Leider gibt es aber kaum solche Erweiterungen. Mozilla hat Ende 2016 eine App mit dem Name „Firefox-Klar“ auf den Markt gebracht, die „Schutz Ihrer Privatsphäre“ verspricht[149]:
„Firefox Klar stellt Ihnen zum Schutz Ihrer Privatsphäre einen Browser mit eingebautem Schutz vor Aktivitätenverfolgung zur Verfügung und ermöglicht auch das Blockieren von Inhalten. Mit Firefox Klar haben Sie die Wahl: Verwenden Sie Firefox Klar als eigenständigen Browser oder nutzen Sie die Funktion zur Blockierung von Inhalten in Safari.“

[149] https://support.mozilla.org/de/kb/was-ist-firefox-klar

Allerdings hat diese App selbst einen Tracker eingebaut, der Daten direkt an die Tracking-Firma adjust übermittelt:

In den Datenschutzbestimmungen bei Mozilla, wird auch darauf hingewiesen „Die Drittanbietersoftware besteht aus einem in Firefox integrierten Software Development Kit (SDK) und einem Internetserver, der vom deutschen Unternehmen adjust GmbH betrieben wird und an den die Daten übermittelt werden.“[150]

Nachtrag vom 14.7.17

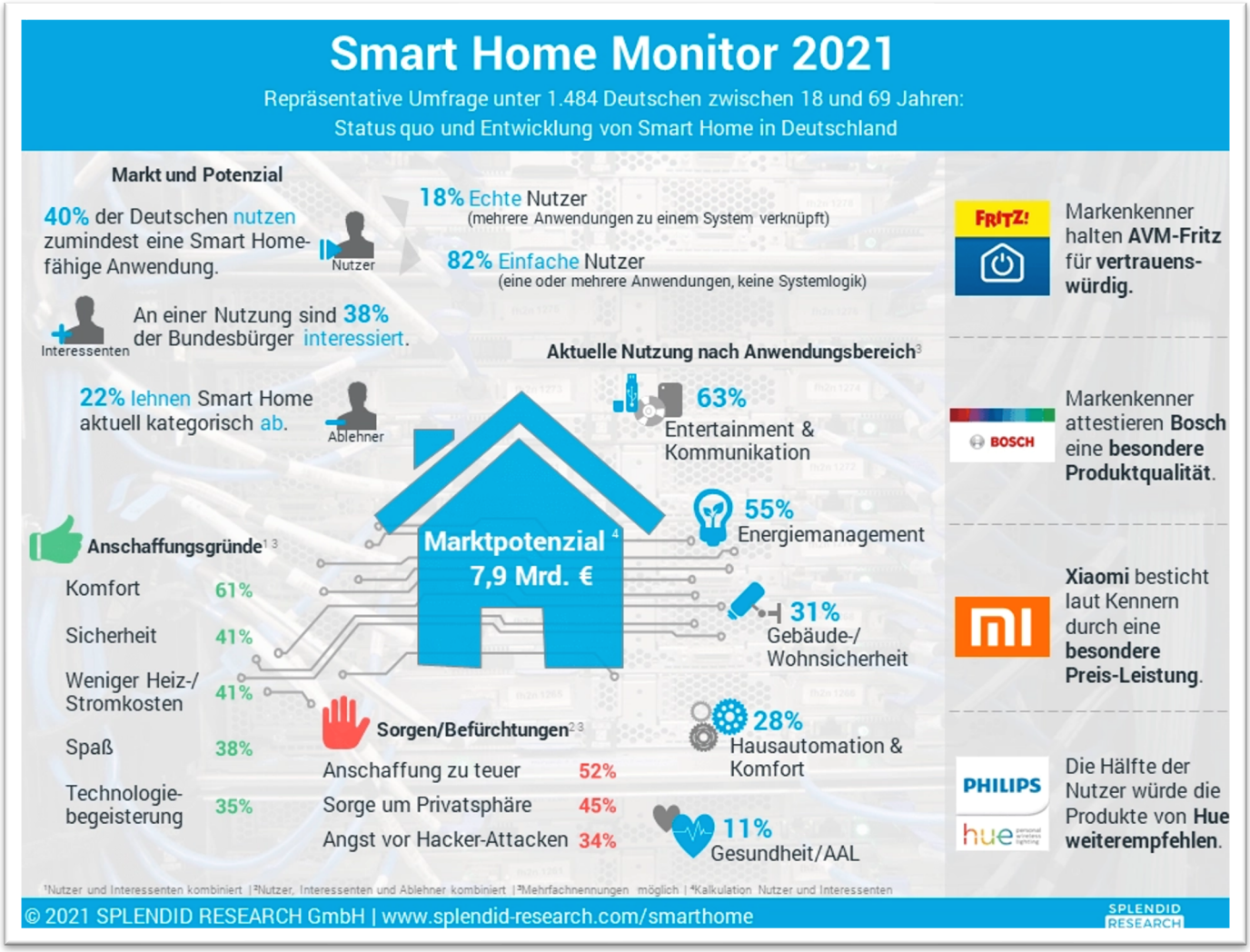
Mozilla hat mittlerweile auch eine Android-Version bereitgestellt. Dabei schreibt Mozilla, dass sie „…auf die Einbindung der Drittanbieter-Lösung Adjust verzichtet haben.“
Weiter schreibt Mozilla: „Zu diesem Schritt haben wir uns aufgrund des Feedbacks entschieden, das wir im Nachgang des Launchs von Klar für iOS insbesondere von unseren deutschsprachigen Nutzern erhalten haben und wir freuen uns, hierauf an dieser Stelle einzugehen. Auch aus der iOS-Version von Firefox-Klar werden wir Adjust entfernen.“[151].
Aktuelle Test von Comidio (stand 3/2020) haben gezeigt, dass Mozilla auch in der iOS-Version Adjust entfernt hat. Allerdings haben diese Tests auch gezeigt, dass Firefox-Klar kaum vor Tracking schützt.

[150] https://support.mozilla.org/de/kb/anonyme-nutzungsdaten-zu-firefox-auf-mobilgeraten-

[151] https://blog.mozilla.org/press-de/2017/06/20/weniger-werbung-mehr-privatsphare-firefox-klar-jetzt-auch-fur-android/

IoT Devices (Internet of Things)

Mittlerweile haben wir nicht nur PCs und Smart-Phones im Einsatz sondern auch zunehmend Alltagsgeräte wie Fernseher, Heizung, Spielekonsole, Fitnestracker u.a. Gadgets, die uns auf der einen Seite das Leben erleichtern, die sich aber auf der anderen Seite bestens dazu eignen, unser tägliches Verhalten auch zu Hause auszuspionieren. Laut der „Smart Home Monitor 2021“ Umfrage, nutzen Anfang 2021 schon 40% Smart Home fähige Anwendungen und weitere 38% sind an deren Nutzung interessiert.



https://www.splendid-research.com/de/smarthome.html

Schon 2015 hat Google ein Patent „Überwachung und Berichterstattung der Haushaltsaktivitäten im Smart Home” angemeldet, welches beschreibt, wie Google unsere häuslichen Aktivitäten mit Hilfe von IoT-Geräten überwachen möchte.[152]

Google Patent (2015): Überwachung und Berichterstattung der Haushaltsaktivitäten im Smart Home

[152] patents.google.com/patent/US20160261932A1/en

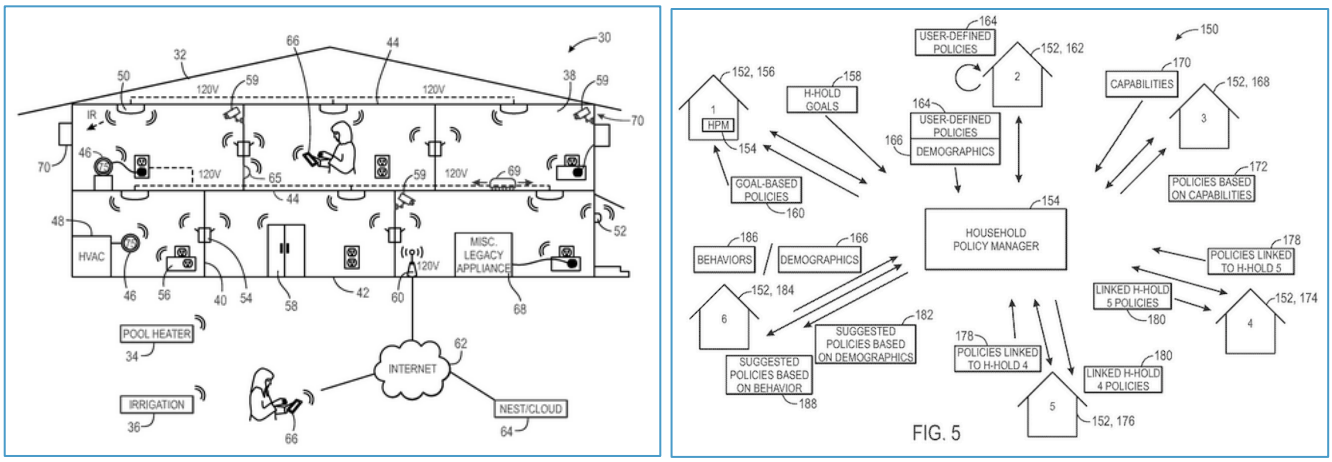


FIG. 5

https://patents.google.com/patent/US20160261932A1/en

2. Gruppe: Geheimdienste und andere staatliche Autoritäten

Geheimdienste haben natürlich viel effektivere Möglichkeiten, Bürger im Internet auszuspähen. Da sie in der Lage sind, Firmen zu nutzen, die direkten Zugang zu Ihren Daten haben, können Geheimdienste den gesamten digitalen Datenverkehr mitlesen. Sie nutzen dazu nicht nur Internetfirmen wie Facebook, Microsoft, Google und Cloud-Anbieter, bei denen der Nutzer seine Daten speichert. Sie können auch über Telekommunikationsunternehmen, die den Internet-Datenfluss steuern (in Deutschland z.B. die Telekom[153],[154]), weltweit und in Echtzeit auf E-Mails, Chat und Browser-Transaktionen des Nutzers zugreifen[155].
An vorderster Front in Bezug auf den Einsatz der genannten Überwachungsmöglichkeiten ist der amerikanische Geheimdienst NSA. Die NSA hat nicht nur automatische Filter im Einsatz, die beim Auftreten bestimmter Schlüsselwörter Kommunikationsteilnehmer auf eine Verdächtigen-Liste setzen. Diese Suchmerkmale werden „Selektoren" genannt[156],[157]. Diese Selektoren sind vergleichbar mit „Suchkriterien" und können individuell konfiguriert werden. Sie können auch gezielt einzelne Telefonnummern, E-Mail Adressen, Chat-, Video-Konferenzen, einzelne Rechner, einzelne Firmen oder ganze Länder im Internet beobachten. Des Weiteren bedienen sich Geheimdienste natürlich auch den gleichen, erprobten Technologien, die auch kommerzielle Daten-Tracker nutzen, z.B. Browser-Fingerprinting, um das Surf-Verhalten eines Einzelnen zu beobachten[158].
Es wird berichtet, dass sich im 3/2015 auf den Computern des Deutschen Nachrichtendienstes (BND) 4,6 Millionen Suchbegriffe befunden haben, die sich auf mehr als eine Million Personen und Unternehmen bezogen haben[159].
Die NSA hat solche Selektoren nicht nur in den USA installiert, sondern arbeitet mit anderen Ländern und deren Geheimdiensten eng zusammen und erhält auch über diese Zusammenarbeit viele Informationen. Darüber hinaus werden die meisten Internet-Vermittlungs-Server (Router) des Internet-Backbones (das ist das Netzwerk-Rückgrat des Internets) von amerikanischen Firmen (z.B. Cisco) hergestellt. Und es kann nicht ausgeschlossen werden, dass diese Vermittlungsserver, die in der ganzen Welt verteilt sind, von der NSA infiltriert worden sind.
Über diese Router kann man zwar alle Daten abgreifen. Doch diese Maschinen sind nicht leistungsfähig genug, um die gewünschten Informationen herauszufiltern. Deswegen gibt es für die Ausspähung speziell entwickelte Geräte z.B. von der Firma Verint (http://de.wikipedia.org/wiki/Verint_Systems). Viele Geheimdienste und polizeiliche Ermittlungsbehörden nutzen diese Lösung, um aus dem riesigen Internet- und auch Telefon-Datenstrom die relevanten Daten zu filtern und zu entschlüsseln. Verint war ursprünglich zwar eine israelische Firma, hatte aber schon immer enge Beziehungen zur NSA. Inzwischen ist Verint eine amerikanische Firma, und die NSA könnte durch Infiltrierung der Geräte auch an in anderen Ländern gesammelte Daten gelangen. Unter www.buggedplanet.info gibt es eine umfangreiche Liste

[153] http://www.heise.de/newsticker/meldung/BND-NSA-Skandal-Deutsche-Telekom-leitete-Transitverkehr-Daten-an-den-BND-2652374.html?wt_mc=sm.feed.tw.ho

[154] http://www.heise.de/security/meldung/Deutsche-Telekom-verteidigt-Kooperation-mit-Geheimdiensten-2526600.html?wt_mc=nl.heisec-summary.2015-01-26

[155] http://electrospaces.blogspot.de/2014/11/incenser-or-how-nsa-and-gchq-are.html

[156] http://www.welt.de/newsticker/dpa_nt/infoline_nt/thema_nt/article140582968/Selektoren-Ablehnungslisten-geheime-Abkommen.html

[157] http://www.spiegel.de/politik/deutschland/bnd-affaere-um-nsa-selektoren-dr-t-als-zeuge-im-bundestag-a-1032939.html

[158] http://www.golem.de/news/bnd-metadatensuche-die-nadel-im-heuhaufen-ist-zerbrochen-1505-114194.html

[159] http://www.welt.de/newsticker/dpa_nt/infoline_nt/thema_nt/article140582968/Selektoren-Ablehnungslisten-geheime-Abkommen.html

von Firmen, die Überwachungslösungen liefern[160]. Wo in Deutschland Geheimdienste stationiert sind zeigt Eagle-Eye auf[161]. Sobald ein Geheimdienst an den gesamten Internet-Datenverkehr heran kommt, kann dieser auch beliebige Informationen herausfiltern.
Für Geheimdienste ist es auch problemlos möglich, drahtlose Verbindungen mitzuhören und evtl. sogar zu manipulieren. Mittlerweile wird davon ausgegangen, dass fast alle SIM-Karten (Handy-Karten) von den US und englischen Geheimdiensten manipuliert sind[162]. Die Zukunft gehört dem mobilen Internet. Gerade die Kommunikation zwischen Maschinen wird zunehmend mit Hilfe von Mobilfunknetzen stattfinden (Machine-to-Machine Kommunikation und Internet der Dinge). In Zukunft werden immer mehr Maschinen einen direkten Kommunikationsanschluss erhalten. Befeuert wird dieser Trend unter anderem durch Entwicklungen wie „Industrie 4.0". Um auch in Zukunft genügend Bandbreite in den Mobilfunknetzten für die Überwachungszwecke sicherzustellen, werden sogar Netzwerkstandards angepasst. Ein Artikel von Erich Möchel entlarvt die Standardisierungspläne auf[163]:
"*Unter den ersten Dokumenten des relativ neuen Technischen Komitees smartM2M im ETSI finden sich ebenfalls klare Hinweise darauf, dass standardisierte Schnittstellen für Polizei aber auch Militärs fix vorgesehen sind. Analog zur Live-Überwachung der Mobilfunknetze soll Strafverfolgern der Zugriff auf den Datenstrom von Sensoren und Maschinen aller Art in Echtzeit ermöglicht werden, etwa um Fahrzeuge punktgenau zu verfolgen, oder Informationen über den gesundheitlichen Zustand von Zielpersonen einzuholen.*"
Der Nutzer kann aber den Geheimdiensten das Leben schwer machen, indem er seine Daten verschlüsselt. Es gilt als ziemlich sicher, dass es noch kein Geheimdienst der Welt geschafft hat, aktuelle Verschlüsselungsverfahren zu durchbrechen. Wichtig ist dabei allerdings, dass die Daten vom Ursprung bis zum Empfänger verschlüsselt sind und verschlüsselt bleiben (Ende-zu-Ende Verschlüsselung).
Das Verschlüsseln hilft allerdings nur dabei, nicht auf die Verdächtigen-Liste zu kommen. Ist der Nutzer einmal im Visier der Geheimdienste, dann gibt es kaum noch Möglichkeiten, sich der anschließenden gezielten Überwachung zu entziehen.
Geheimdienste sind in der Lage, den Kauf des nächsten Monitorkabels so zu manipulieren, so dass der Nutzer bei der Auslieferung ein manipuliertes Kabel bekommt, das es Geheimdiensten erlaubt, per Funk alle Daten auf des Nutzers Bildschirm mitzulesen. Und das ist nur einer von vielen direkten, zielgerichteten Angriffen, zu denen Geheimdienste heute in der Lage sind. Weitere Methoden, die Geheimdienste und andere staatliche Organisationen nutzen, um gezielt einzelne Nutzer auszuspionieren oder sogar zu schädigen, sind sehr ausgefeilte Computerviren oder -trojaner wie z.B. „Regin"[164]. Darüber hinaus hat die NSA gezeigt, dass sie in der Lage ist, sogar Viren zu programmieren die sich im Festplatten-Treiber einnisten und dadurch kaum mehr von Virenscannern auffindbar sind[165].
Wie diese Ausführungen zeigen, ist es also für Internet-Nutzer sinnvoll, ihre Daten im Internet zu verschlüsseln.
Geheimdienste (und auch kommerzielle Daten-Tracker) sind vor allem an den Metadaten interessiert. Metadaten sind im Gegensatz zu den tatsächlich ausgetauschten Daten u.a. die Verbindungsdaten.
Bei einer E-Mail treten die Metadaten zu Tage, wenn Fragen gestellt werden wie:

160 http://buggedplanet.info/index.php?title=DE

http://buggedplanet.info/index.php?title=Main_Page

161 http://www.photocontest-eagle-eye.org/research.html

162 https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

163 http://fm4.orf.at/stories/1754728/

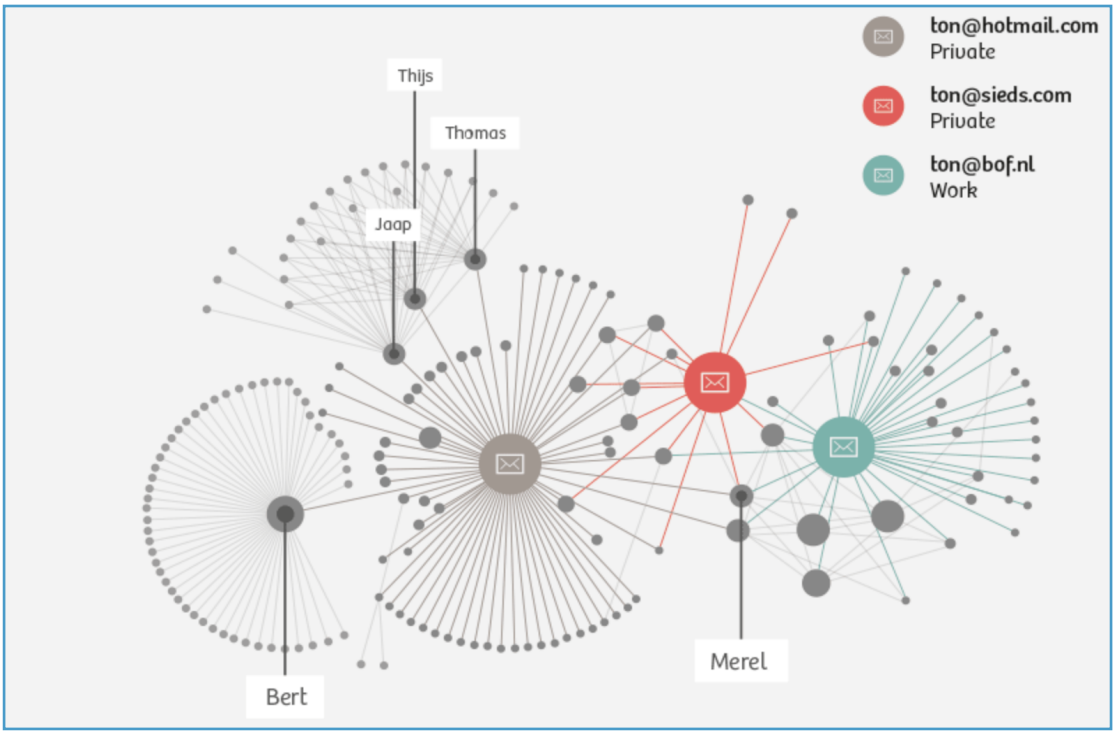
164 http://www.zeit.de/digital/datenschutz/2015-01/regin-trojaner-nsa-spionage-cyberkrieg

165 http://www.wired.com/2015/02/nsa-firmware-hacking/?mbid=social_twitter

- Wer hat die E-Mail geschrieben (Absender)?
- An wen ging die Nachricht und mit wem steht der Absender in Kontakt?
- Wie oft steht der E-Mail Versender mit dem Adressaten in Kontakt?
- Wann hat der Sender die E-Mail geschrieben (wie sind seine Arbeitszeiten und Tagesgewohnheiten)?
- Mit welchem Gerät und welcher E-Mail Software hat er die Nachricht geschrieben (mit diesem Wissen können gezielt weitere Informationen aus dem Device/ E-Mail Software herausgezogen werden)?
- Von welchem Standort hat er die E-Mail geschrieben (Bewegungsprofile)?
- Wie lautet der „Betreff" bzw. Überschrift der E-Mail?
- Sind der Absender und auch der Empfänger technisch in der Lage, die Mail zu verschlüsseln? (technische Fähigkeiten der Kommunikationspartner)?

Vergleichbare Metadaten fallen auch bei allen anderen Kommunikationsarten an (Chat, Audio-, Video-Konferenzen usw.)
Oft sind mit Hilfe von Big Data Algorithmen aus diesen Metadaten mehr Informationen ableitbar, als aus den tatsächlich ausgetauschten Daten. Wenn ein Angreifer in der Lage ist, über längere Zeit den E-Mail Verkehr eines Benutzers zu beobachten, ist er im Stande ein sehr detailliertes Datenprofil über ihn zu erstellen. Dies kann er selbst nutzen oder gewinnbringend verkaufen. In jedem Fall wird es über Jahre speichern.
Metadaten machen die persönlichen Netzwerke und individuellen Zusammenhänge sichtbar und verdeutlichen so die gesellschaftlichen Beziehungen der bespitzelten Person. Der Niederländer Ton Siedsma hat in einem aufschlussreichen Selbstversuch gezeigt, welche Informationen man beim Sammeln der Metadaten über eine Person anhäufen kann[166].
Nach einer Woche waren bereits 15.000 Datensätze angefallen.

166 https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smartphone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt/



Wie man in den Bild gut erkennen kann, gibt der Internet-Nutzer den Daten-Spionen nicht nur Inhalte sondern durch das Aufzeichnen der Metadaten auch seine Kontakte preis.
Es wird zwar immer wieder behauptet, Metadaten seien keine persönlichen Daten, dies wurde allerdings durch eine MIT-Studie widerlegt[167]. Gemäß dieser Studie genügen vier Datenpunkte, um beispielsweise einen Kreditkarteninhaber zu Identifizieren.
Es nützt auch wenig, wenn man seine E-Mail mit PGP verschlüsselt. Die meisten Metadaten sind weiterhin für Datenspione lesbar. Somit sind der E-Mail Provider, die Netzwerk-Administratoren (Internet-Provider des Nutzers und dessen Netzwerk-Backbone-Lieferanten, falls die E-Mail Server ihre Daten immer noch unverschlüsselt austauschen) und die Geheimdienste in der Lage, die vorstehend beschriebenen Profile zu erstellen.
Die Vereinigung „Cause[168]“ hat die Software „DETECT“ entwickelt, die die bei Geheimdiensten (und auch kriminellen Hackern) sehr beliebten Werkzeuge „FinFisher” und “Hacking Team RCS” für alle Internetnutzer erkennbar macht[169].

3. Gruppe: Internet-Kriminelle (Hacker, die es auf das Geld des Internetz-Nutzers abgesehen haben)

Selbstredend sind kriminelle Hacker in der Lage, sich einen Virus zu kaufen (kostet nur wenige Euro) und auf den Rechner des Internetz-Nutzers zu spielen. Falls dieser die Software des Rechners immer auf dem letzten Stand hält, einen guten Virenscanner hat und nicht jeden Anhang oder Link in einer E-Mail unüberlegt anklickt, ist er dagegen recht gut geschützt.

[167] https://www.divsi.de/mit-forscher-widerlegen-anonymitaet-von-metadaten/

168 http://www.globalcause.net

169 https://resistsurveillance.org

Aber Internet-Kriminelle sind in der Lage, fast alle technischen Möglichkeiten der 1. und 2. Gruppe ebenfalls zu nutzen. Da es die ersten beiden Gruppen gibt, die seit Jahren Benutzer-Daten sammeln, liegt es natürlich auch nahe, dass Internet-Kriminelle diese Firmen und staatliche Einrichtungen hacken. Und dies geschieht regelmäßig. Diese Einbrüche sind für einen Hacker natürlich sehr viel lohnenswerter, als nur in den PC eines einzelnen Benutzers einzudringen. Es greifen also nicht nur Geheimdienste die Kundendaten bei großen amerikanischen Internetdienstleister wie Google, Microsoft oder Apple ab. Internet Hacker haben auch schon erfolgreich viele Millionen von Kreditkarten und Login-Passwörter von großen E-Mail Anbietern und Spieleplattformen erbeutet.
Es sollten den ersten beiden Gruppen also möglichst wenige Daten der Internet-Nutzer zugänglich sein. Da die TrutzBox auf Basis von „Eigenhosting“ entwickelt wurde, über die der Nutzer diese Dienste zu Hause selbst betreibt, ist er nicht mehr von solchen zentralen Dienstleistern abhängig, und die Gefahr, dass seine Daten bei einem einzigen Angriff auf solche Massen-Daten von Internet-Kriminellen gestohlen werden, schwindet. Dass es Kriminelle vor allem auf große Massendaten abgesehen haben, zeigt eine Statistik die der amerikanische IT-Security-Anbieter Varonis zusammengestellt hat. Demnach summiert sich die Zahl aller kompromittierten Datensätze von 2013 bis 2018 auf insgesamt fast 10 Milliarden weltweit, die durch Datenverletzungen und Cyberkriminalität verloren gegangen oder gestohlen worden. Mit über sechs Milliarden gestohlenen Datensätzen übersteigt die Gesamtzahl der Datensätze in den USA (in dem die meisten unserer social-media Daten gespeichert sind) die Bevölkerung um das 19-fache.:
http://blog.wiwo.de/look-at-it/2018/11/14/fast-10-milliarden-gestohlene-oder-verlorene-datensaetze-seit-2013/

Kosten eines Cyber-Angriffs

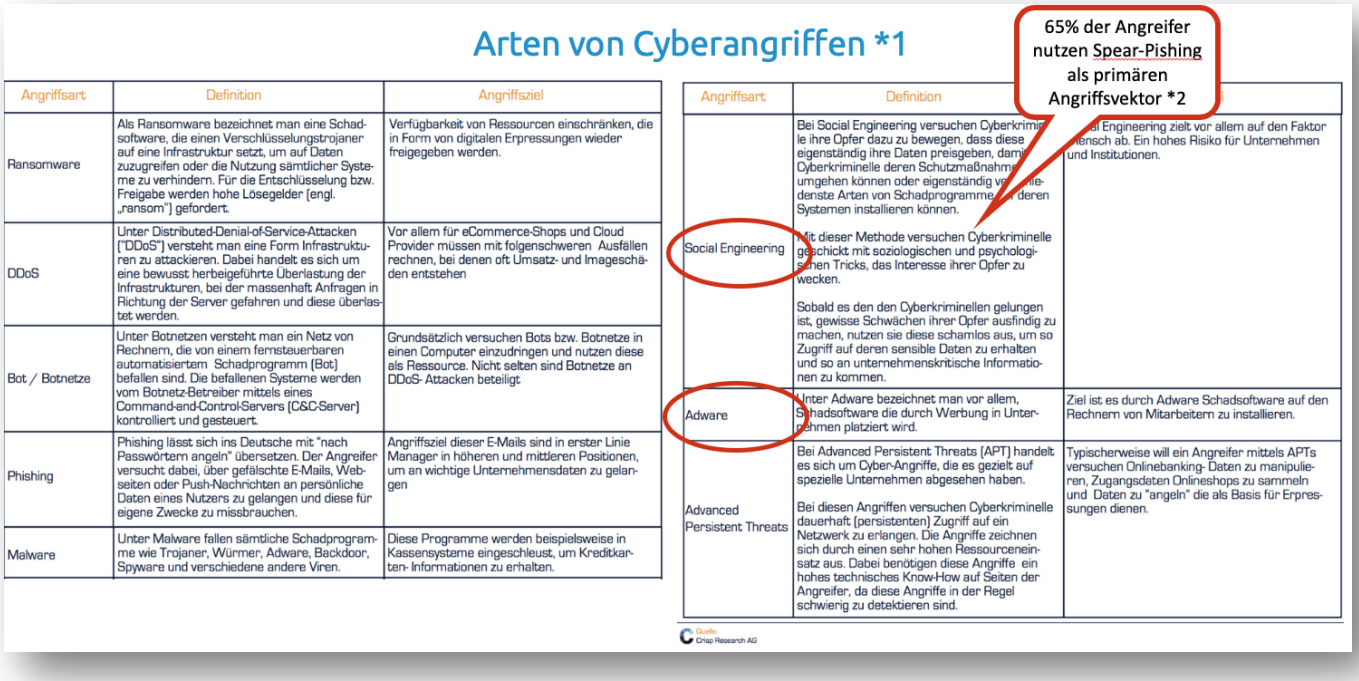
Dass man einen Angriff auf eine Firma recht preiswert im Darknet kaufen kann, zeigt die Deloitte Studie „Black Market Ecosystem: Estimating the cost of ownership“[170] von 12/2018. Hier ein paar Preis-Beispiele:

- Eine komplette Phishing-Kampagne, inklusive Hosting und entsprechendem Toolkit, kostet im Schnitt 500 Dollar pro Monat – der Einstiegspreis liegt bei 30 Dollar pro Monat.
- Eine Keylogging-Kampagne, die darauf ausgelegt ist, Zugangsdaten abzugreifen, kostet inklusive Malware, Verbreitung und Hosting im Schnitt 723 Dollar – wobei der Einstiegspreis mit 183 Dollar auch hier deutlich niedriger liegt.
- Ransomware-Kampagnen oder Trojaner-Angriffe sind im Schnitt ab 1.000 Dollar zu haben.

[170] https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-announces-new-cyber-threat-study-on-criminal-operational-cost.html

- Die Verbreitung eines Banking-Trojaners kostet im günstigsten Fall 1.400 Dollar, kann aber auch mit bis zu 3.500 Dollar zu Buche schlagen.

Crisp-Research hat die Arten von Cyberangriffen auf Firmen in folgende acht Gruppen unterteilt. Zwei dieser Gruppen, „Social Engineering“ und „Adware“ sind besonders effektiv und nutzen den Umstand aus, dass der Geschädigte zunächst sehr genau ausgespäht wird, bevor der eigentliche Angriff stattfindet. Wobei gerade das Angriffs-Scenario „Social Engineering“ besonders häufig (65%) zur Anwendung kommt.



Angriffsart	Definition	Angriffsziel
Ransomware	Als Ransomware bezeichnet man eine Schadsoftware, die einen Verschlüsselungstrojaner auf eine Infrastruktur setzt, um auf Daten zuzugreifen oder die Nutzung sämtlicher Systeme zu verhindern. Für die Entschlüsselung bzw. Freigabe werden hohe Lösegelder (engl. „ransom“) gefordert.	Verfügbarkeit von Ressourcen einschränken, die in Form von digitalen Erpressungen wieder freigegeben werden.
DDoS	Unter Distributed-Denial-of-Service-Attacken ("DDoS") versteht man eine Form Infrastrukturen zu attackieren. Dabei handelt es sich um eine bewusst herbeigeführte Überlastung der Infrastrukturen, bei der massenhaft Anfragen in Richtung der Server gefahren und diese überlastet werden.	Vor allem für eCommerce-Shops und Cloud Provider müssen mit folgenschweren Ausfällen rechnen, bei denen oft Umsatz- und Imageschäden entstehen
Bot / Botnetze	Unter Botnetzen versteht man ein Netz von Rechnern, die von einem fernsteuerbaren automatisiertem Schadprogramm (Bot) befallen sind. Die befallenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert.	Grundsätzlich versuchen Bots bzw. Botnetze in einen Computer einzudringen und nutzen diese als Ressource. Nicht selten sind Botnetze an DDoS- Attacken beteiligt
Phishing	Phishing lässt sich ins Deutsche mit "nach Passwörtern angeln" übersetzen. Der Angreifer versucht dabei, über gefälschte E-Mails, Webseiten oder Push-Nachrichten an persönliche Daten eines Nutzers zu gelangen und diese für eigene Zwecke zu missbrauchen.	Angriffsziel dieser E-Mails sind in erster Linie Manager in höheren und mittleren Positionen, um an wichtige Unternehmensdaten zu gelangen
Malware	Unter Malware fallen sämtliche Schadprogramme wie Trojaner, Würmer, Adware, Backdoor, Spyware und verschiedene andere Viren.	Diese Programme werden beispielsweise in Kassensysteme eingeschleust, um Kreditkarten- Informationen zu erhalten.

Angriffsart	Definition	
Social Engineering	Bei Social Engineering versuchen Cyberkriminelle ihre Opfer dazu zu bewegen, dass diese eigenständig ihre Daten preisgeben, damit Cyberkriminelle deren Schutzmaßnahmen umgehen können oder eigenständig verschiedenste Arten von Schadprogrammen auf deren Systemen installieren können. Mit dieser Methode versuchen Cyberkriminelle geschickt mit soziologischen und psychologischen Tricks, das Interesse ihrer Opfer zu wecken. Sobald es den den Cyberkriminellen gelungen ist, gewisse Schwächen ihrer Opfer ausfindig zu machen, nutzen sie diese schamlos aus, um so Zugriff auf deren sensible Daten zu erhalten und so an unternehmenskritische Informationen zu kommen.	ial Engineering zielt vor allem auf den Faktor Mensch ab. Ein hohes Risiko für Unternehmen und Institutionen.
Adware	Unter Adware bezeichnet man vor allem, Schadsoftware die durch Werbung in Unternehmen platziert wird.	Ziel ist es durch Adware Schadsoftware auf den Rechnern von Mitarbeitern zu installieren.
Advanced Persistent Threats	Bei Advanced Persistent Threats (APT) handelt es sich um Cyber-Angriffe, die es gezielt auf spezielle Unternehmen abgesehen haben. Bei diesen Angriffen versuchen Cyberkriminelle dauerhaft (persistenten) Zugriff auf ein Netzwerk zu erlangen. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz aus. Dabei benötigen diese Angriffe ein hohes technisches Know-How auf Seiten der Angreifer, da diese Angriffe in der Regel schwierig zu detektieren sind.	Typischerweise will ein Angreifer mittels APTs versuchen Onlinebanking- Daten zu manipulieren, Zugangsdaten Onlineshops zu sammeln und Daten zu "angeln" die als Basis für Erpressungen dienen.

Quelle: Crisp Research AG

*1 https://www.crisp-research.com/cyberangriffe-die-attacken-von-heute-die-von-unternehmen-straflich-unterschatzt-werden/
*2 https://blog.wiwo.de/look-at-it/2020/01/08/it-sicherheit-die-wichtigsten-cybersecurity-trends-fuer-das-jahr-2020/

Sechs Gefahrengruppen – Comidio Definition

Da es die Gefahr von Industrie-Spionage und Verlust der Privatsphäre gibt, hat Comidio die Internetgefahren erweitert und in folgende sechs Gefahrengruppen (Threat-Typen) zusammengefasst. Auf Basis dieser Gefahrengruppen wurde die TrutzBox entwickelt:

Threat Level	Threat Type	Explanation	Used Technology	Bypass Solution
1	User Profile Mining	Companies like Facebook get not only the data from their members. No, every page you surf that contains a Facebook LIKE button sends some user data to Facebook. Companies like Amazon, Facebook, Twitter sell data to data dealers like Acxiom, RapLeaf, KaiBlue... Most web pages have some kind of tracking built in. Sometimes 10-30 different tracking solutions in one web page.	Cookies/Flash Cookies, Web bugs, EverCookies, Browser Fingerprinting. eMail tracking through pictures with 1x1 pixel size and eMail tracking services. Document tracking through reload of Word, PDF... documents.	Control or prevent use of Cookies/Flash Cookies, Web bugs, EverCookies and Fingerprinting at your browser. Email client HTML control.
2	Communication Mining	Mining of "Who communicates with whom" information is very likely in the Internet and very valuable for some commercial companies and secret services.	This data could be mined by spying of email traffic and Twitter, Facebook, blog... communication.	Usage of fake and temp/one-time email addresses and remailer services prevent spying of service providers.
3	Governments & Content provider Internet censoring	Governments are limiting public exposure to content that according to their laws does conform to their political correctness. Content providers like Youtube are blocking access to content because of copyright and intellectual property protection laws	At Internet network level all traffic will be checked against white or black labeled source and target IP addresses.	VPN proxies (IP-based) or http proxy server located in another country
4	Access to or manipulation of personal data	Cyber attacks based on viruses, worms or trojans. These techniques are used to spy secret business data or manipulate personal data like banking transactions.	Viruses, worms or trojans will be utilized to access personal data stored on local devices or read data from input devices. Could also be used to manipulate communication data e.g. banking transactions.	Prevention of infections with viruses, worms or trojans by usage of appropriate virus scanners and control of scripting (like java/ flash...) in the browser, email and other Internet client software. Mandatory for encrypted network communication (https)
5	Revoke of network anonymity	Internet Service Providers record which customer Internet contract is assigned to which IP address during a defined timeframe. With judicial assistance there is a possibility to get access to this data and third parties can get name and address of who accessed content somewhere in the Internet.	No special technology needed besides to record which source IP address accessed the content.	Same as threat level 3
6	Unauthorized access to content that violates child protection laws (Youth Protection Act)	Everyone is able to access all content from the internet. But parents wants to protect their children of getting access to content which is unsuitable for their children	Depending of children's age, the parents can select which content filters will be active for every child	Depending on the used technology, the user is able to bypass the filter by addressing IP-addresses instead domain names

(© 2015 Comidio GmbH)

Gefahrengruppe 3 „Governments & Content provider Internet censoring“ hat eine besondere Rolle in dieser Aufstellung. Zunächst möchten freie Bürger selbst entscheiden, auf welche Informationen sie zugreifen möchten. Und niemand möchte sich von irgendjemand zensieren lassen. Aber wir alle leben in einer Zensurgesellschaft, und auch in Deutschland gibt es eine Zensur, die regelt, welche Informationen gut und welche schlecht sind.
Dazu kommt, dass Rechteinhaber, die Rechte an kommerziell gehandelten Daten halten, daran interessiert sind, diese für jedes Land getrennt zu verwalten. Somit haben auch Firmen mit Rechten an digitalen Gütern, wie Filme, Musik, Bilder usw., Interesse, dass Zugriffe im Internet überwacht und gegebenenfalls auch verfolgt werden. Die Studie „Filtering, blocking and take-down of illegal content on the Internet“[171] gibt eine recht gute Übersicht über Internet Zensur Europäischer Länder.

Wie kann sich der Internet-Nutzer gegen Angreifer schützen?

Natürlich ist es ein absolutes Muss, sowohl einen geeigneten Virenscanner zu installieren als auch alle Programme immer auf dem neuesten Stand zu halten. Darüber hinaus ist es wichtig, Betriebssystem-Updates zeitnah einzuspielen und nicht mit einem Betriebssystem zu arbeiten, das vom Hersteller nicht mehr unterstützt wird.
Wenn der Nutzer diese Regeln alle befolgt, ist er zwar vor Viren und Trojanern recht gut geschützt, aber die genannten Maßnahmen können nicht verhindern, dass er Spuren im Internet hinterlässt. Das BSI hat

[171] http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

neun Poster veröffentlicht, die Internetnutzern aufzeigen, was sie bei der Nutzung des Internets beachten sollen[172].
Aber es gibt Tausende von Werkzeugen, die man auf seinem PC oder Smartphone installieren kann, um die Sicherheit bei der Nutzung des Internets zu erhöhen und den Benutzer zu anonymisieren. Viele dieser Werkzeuge sind sogar kostenlos.
Comidio untersucht regelmäßig die gebräuchlichsten Browser, Browser-Plugins und Privacy-Boxen bzgl. Ihrer Schutzwirkung. Hier eine Übersicht der verbreitetsten Sicherheits- und Anonymitäts-Werkzeuge. Die rot eingekreisten Werkzeuge werden von Comidio empfohlen:

(© 2023 Comidio GmbH)

Allgemein kann man feststellen: jedes dieser Werkzeuge hat auch Nachteile:

- Man braucht meist technisches Know-how, um die richtigen Werkzeuge zu finden und auszuwählen.
- Kein einzelnes Werkzeug deckt alle notwendigen Funktionen ab. Man braucht sehr viele dieser Werkzeuge, um im Internet wenigstens einigermaßen sicher und anonym zu sein.
- Manche Werkzeuge sind von Laien kaum bedienbar, man muss technisch versiert sein, um diese Werkzeuge nutzen zu können.
- Die meisten Werkzeuge können nur PCs oder Smartphones absichern. Andere internetfähige Geräte können damit nicht abgesichert werden.

Die meisten **Browser-Plugins** sind entweder für einen Laien kaum zu bedienen, schützen kaum vor Tracking oder liefern sogar selbst Tracking-Daten an ihren Hersteller. Lediglich uBlock und uMatrix sind sehr hilfreich, aber für einen Laien nicht zu bedienen.

[172] https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Broschueren/broschueren_node.html

Fast alle **Browser**-Hersteller überschlagen sich mit Ankündigungen jetzt endlich unerwünschte Tracker und Werbung zu blockieren. Aber Tests von Comidio zeigen, dass sie kaum schützen. Fast alle Browser liefern sogar regelmäßig Daten an ihren Hersteller. Lediglich den Browser von JonDoNym und den Tor-Browser können wir empfehlen. Allerdings sind diese Browser auch so restriktiv, dass viele Web-Seiten Probleme bereiten.
Bei den **Privacy Boxen** sieht es nicht viel besser aus. Aufgrund Ihrer technischen Architektur, dass diese im Netzwerk in der Lage sind, den gesamten Netzwerkverkehr zu kontrollieren, ist das eigentlich die einzige Lösung um wirklich einen Rundum-Schutz zu bieten. Allerdings bieten die meisten Security- und Privacy-Boxen meist nur Teillösungen an. Viele sind lediglich Firewalls, die sicherstellen, dass nichts Böses ins eigene Netz kommt, schützen aber gar nicht davor, dass private oder persönliche Daten ins Netz raus gehen. Lediglich die Freedom-Box kann hier recht umfänglich schützen. Aber die ist recht komplex aufzusetzen und zu bedienen.
Comidio hat diese Erfahrung genutzt, um eine möglichst einfach zu bedienende Security- und Privacy-Box zu bauen, die einen Rundum-Schutz bietet.
Am besten wäre es natürlich, man würde sämtliche Kommunikation im Internet verschlüsseln. Leider hat man darauf nur dann einen Einfluss, wenn auch der Kommunikationspartner in der Lage ist, die Kommunikation zu end- und verschlüsseln. Das mag bei E-Mail und Chat noch möglich zu sein, aber in anderen Fällen, wie z.B. Browsen auf Webseiten, genügt das Verschlüsseln der Kommunikation nicht, da man ggf. dem Kommunikationspartner nicht alle persönlichen Daten geben möchte. Aber dass wir ungewollt persönliche Daten weitergeben, geschieht jeden Tag, wenn wir im Internet surfen. Denn selbst bei einer verschlüsselten Verbindung, bekommt der angesteuerte Web-Server persönliche Daten, die man ihm i.d.R. gar nicht geben möchte. Das geschieht über HTTP-Header-Tags. Und noch viel schlimmer, oft hat die aufgerufene Webseite zusätzliche andere Webseiten eingebaut (Daten-Tracker), die auch noch persönliche Daten erhalten.
Um alle oben genannten Bedrohungen mit einem einfachen Lösungsansatz zu eliminieren, kann man mit diesen beiden Maßnahmen fast alle Probleme lösen:

- Für E-Mail, Chat-, Audio-, Video-Kommunikation und soziale Netzwerke: weg von zentralistischen Lösungen und hin zum „Eigenhosting“, die den Kommunikationspartner authentisiert und die gesamte Kommunikation mit dem Partner end-to-end verschlüsselt.
- Beim Surfen im Internet keine Daten-Tracker bedienen und dem aufgerufenen Web-Server auch nur die Daten geben, die ich ihm geben möchte und die er wirklich benötigt.

Und genau diese beiden Lösungsansätze verfolgt die TrutzBox.

Erster Ansatz: weg von zentralistischen Lösungen

Immer mehr persönlich Daten landen auf den Servern großer (in der Regel amerikanischer) Internet-Unternehmen, die meist kostenlose Social Media Dienste anbieten (Google+, Facebook, Twitter, Skype, WhatsApp, Mail-Server usw.). Vor allem Jugendliche, aber auch schon Kinder, werden durch Gruppendruck mehr oder weniger genötigt, ihre Daten diesen Unternehmen anzuvertrauen. Mangels deutlicher Warnungen oder leicht verständlicher Anleitungen zu ihrem Schutz hinterlassen sie dort freiwillig sehr persönliche Daten, selbst wenn sie wissen, dass diese nie mehr gelöscht werden und in Zukunft gegen sie verwendet werden können.
Und die wenigen, die diese Social Media Dienste nicht nutzen, können nicht verhindern, dass ihre Daten trotzdem erfasst werden, sobald sie eine E-Mail an einen Freund schreiben, der seinen Mail-Account bei

Google hat. Oder sie sind auf einem Bild bei Facebook zu sehen, das von einem „Freund“ hochgeladen worden ist. Durch diese zentralisierten Services wird das Internet immer angreifbarer. Für einen Hacker ist es natürlich lohnender, den Server eines großen Internet Social Media Anbieters anzugreifen, als einen einzelnen PC, da er bei Erfolg gleich Millionen von User-IDs, Passwörtern oder Kreditkartennummern erbeuten kann. Diese kann er dann massenweise auf dem Internet-Schwarzmarkt verkaufen. Auch Geheimdiensten ist es in manchen Ländern gestattet, auf diese Daten zuzugreifen.
Obwohl das Internet ursprünglich als vollständig dezentrales System geplant war, haben sich mittlerweile auch einige zentralistische Technologien etabliert, die das Internet operativ zusammenhalten. Das ist zum einen der DNS (Domain Name Service) , der über eine hierarchisch aufgebaute Server-Struktur die Internet Domain-Namen (wie z.B. comidio.de) in die dazugehörige interne IP-Adresse umsetzt.
Eine weitere wichtige und mittlerweile zu sehr zentralistische Funktion haben die Internet-Zertifizierungsstellen. Wenn der Nutzer die Seite eines Servers aufruft, der behauptet seine Bank zu sein, dann möchte der Nutzer sicher sein, dass dieser Server (dieser Domain-Name) auch wirklich der Server seiner Bank ist. Dazu hat seine Bank bei einer Zertifizierungsstelle ein Zertifikat für seinen Web-Server beantragt, das beim Aufruf des Bank-Servers an seinen Browser übermittelt wird, und mit dessen Hilfe sein Browser feststellen kann, ob dieses Zertifikat wirklich von einer dem Browser bekannten Zertifizierungsstelle kommt. Leider gibt es mittlerweile auch schwarze Schafe unter den Firmen, die diese Zertifikate vergeben, sodass Kriminelle auch an Zertifikate gelangen können, die anderen Unternehmen zustehen würden.
Seit Anfang 2015 ist auch die chinesische Regierung berechtigt, solche Server-Zertifikate auszustellen. Dabei wird gerade die chinesische Regierung beschuldigt, durch gefälschte Zertifikate auf verschlüsselte Daten bei Apple und Microsoft zugegriffen zu haben.[173]. Erste Zertifizierungs-Missbräuche sind in diesem Zusammenhang schon aufgedeckt worden[174].
Welche Probleme und Risiken, allein durch die Zentralisierung der Zertifizierungstellen mittlerweile entstanden sind, beschreibt http://www.secupedia.info/wiki/SSL sehr ausführlich.
Um den Gefahren derartiger zentralisierter Ansätze zu entgehen, ist im Internet eine Tendenz zu beobachten, die unter dem Namen „Eigenhosting“ oder auch Edge-Computing bekannt ist. Das bedeutet, dass der Internetnutzer selbst einen kleinen Server betreibt, auf dem E-Mail-, Cloud- und alternative Social Media Dienste laufen (z.B. *diaspora*[175]*, Mastodon*[176] oder *ello*[177]) und seine Daten nur noch auf dem eigenen, häuslichen oder Firmeneigenen Server gespeichert sind. Damit hat der Nutzer selbst die Kontrolle darüber, was mit seinen Daten geschieht. Die großen Daten-Sammel-Unternehmen gehen leer aus. Und einem Hacker ist es nicht mehr möglich, durch einen einzigen Angriff gleichzeitig an Millionen von Datensätzen zu gelangen.
Durch dieses Eigenhosting lässt sich auch der Anteil der meist identischen Passwörter, die Dienstleister wie Facebook, E-Mail Provider, Twitter und Google von ihren Kunden speichern, reduzieren.
Für diese privaten Server gibt es verteilte Trust-Strukturen als Ersatz für die gebräuchlichen hierarchischen (und damit auch zentralistischen) Zertifizierungsmechanismen (z.B. monkeysphere[178]).

[173] http://www.spiegel.de/netzwelt/netzpolitik/china-internetsicherheit-nur-mit-dem-segen-der-zensoren-a-1016649.html

[174] http://googleonlinesecurity.blogspot.de/2015/03/maintaining-digital-certificate-security.html

[175] https://diasporafoundation.org/

[176] joinmastodon.org

178 http://web.monkeysphere.info

Leider wird auch DNS[179] immer mehr dazu missbraucht, Daten Zugriffe im Internet zu sperren, oder sogar zu falschen Servern umzuleiten. DNS wurde zwar von Anfang an auf Basis einer verteilten Architektur entworfen, aber nur um die Ausfallsicherheit zu erhöhen. Da jedes an das Internet angeschlossene Gerät einen voreingestellten DNS benutzt, ist es leicht möglich, darin Einträge darin zu fälschen. Comidio wird zu gegebener Zeit Alternativen zum heutigen DNS bewerten (z.B. WOT) und gegebenenfalls eine bessere Lösung anbieten.

Etablierte Lösungen sich der Massen-Spionage zu entziehen

Neben den Aktivitäten von Comidio, wurden gerade in letzter Zeit weitere Projekte entwickelt, mit dem Ziel, sich gegen Massenüberwachung zu wehren. Hier nur eine kleine Auswahl:

FreedomBox

Ein erwähnenswertes Open-Source Projekt, das sowohl Eigenhosting als auch Anonymisierung zum Ziel hat, ist „FreedomBox“[180]. Comidio hatte unter anderem auch die FreedomBox als Basis für die TrutzBox in Erwägung gezogen. Leider ist derzeit nicht abzusehen, wann die Entwickler der FreedomBox ein erstes Stable-Release freigeben werden. Und so, wie die FreedomBox geplant wurde, ist sie auch leider nicht für einen Technik-Laien bedienbar. Gerade aufgrund des letzten Punktes, beschloss Comidio, die FreedomBox nicht als Grundlage für die TrutzBox zu verwenden.

RetroShare

Eine weitere sehr interessante Lösung, um eine Entkopplung von zentralistischen und unsicheren Dienstleistern herbeizuführen, ist „RetroShare“ (retroshare.cc)[181].

„RetroShare ist eine betriebssystemunabhängige Open-Source Plattform, die eine private und sichere, dezentralisierte Kommunikation ermöglicht.

Diese erlaubt dem Nutzer, sicher mit Freunden oder der Familie zu chatten oder Daten auszutauschen, indem ein vertrauenswürdiger Bereich des Netzes erzeugt wird, durch die Authentifizierung von Partnern und der OpenSSL Verschlüsselung jeglicher Kommunikation.

RetroShare unterstützt die gemeinsame Datennutzung, Chats, Nachrichten, Foren oder andere Nachrichtenkanäle.“

RetroShare hat besonders den Datenaustausch mit anderen Benutzern gut gelöst. Er basiert, wie auch bei der TrutzBox TrutzMail-Lösung auf einer Peer-to-Peer Lösung (P2P). Die Daten werden also direkt (ohne zentralen Server) mit dem Kommunikationspartner ausgetauscht. Leider ist die Benutzeroberfläche von RetroShare sehr unübersichtlich, und der Nutzer muss sich, wie auch bei PGP, selbst um die Verwaltung der Schlüssel kümmern. Das erschwert die Bedienung für Laien. Derzeit entwickelt die Open-Source-Gemeinde eine Version 0.6, die die die Handhabung erleichtern soll.

179 DNS: Domain Name Service, der einen Domain Namen in eine IP-Adresse übersetzt

180 http://freedomboxfoundation.org

181 http://retroshare.sourceforge.net/index_de.html

Volksverschlüsselung

Die Deutsche Telekom und das Fraunhofer Institut wollen mit der „Volksverschlüsselung“ das Verschlüsseln von E-Mails massentauglich machen. Netzpoliktik.org hat in der Volksverschlüsselung allerdings einige Hürden und sogar Nachteile gefunden[182]:

- Die Software ist nicht Quelloffen und somit ist es nicht nachvollziehbar, ob dort nicht irgendwelche unerwünschte Hintertüren eingebaut wurden
- Die Volksverschlüsselung darf nur für private Zwecke genutzt werden. Man darf damit also keine E-Mail an seinen Steuerberater schicken?
- In der Lizenz räumt sich Fraunhofer und die Telekom das Recht ein, personenbezogene Daten des LIZENZNEHMERS zum Zwecke der Verarbeitung zu erheben. Welche das genau sind und was sie damit machen, lassen sie erst einmal offen.
- Mit der Volksverschlüsselung wird Anonymität verhindert, dass Absender und Empfänger sich vor der Nutzung zuerst registrieren müssen und dabei ihre Identität nachweisen müssen.

I2P

Das Invisible Internet Project (I2P,[183]) wurde mit freier Software realisiert und setzt auf das bestehende Internet-Netzwerk ein anonymes bzw. pseudonymes Netzwerk. In diesem können Nutzer und Anbieter von Dienstleistungen ohne Preisgabe ihrer Identität zueinander finden und Daten austauschen. Ein Teil der Dienste ist in Form von Webanwendungen integriert und über den Browser erreichbar. Viele im normalen Internet verfügbare Dienste wurden auf dieses I2P Netz portiert, sodass auch dort die üblichen Funktionen verfügbar sind (Web-Server, Browser, Chat, Mail, Such-Funktionen, p2p-Datenaustausch…). Da die Anwendungen völlig unabhängig vom normalen Internet interagieren, funktioniert das I2P parallel neben dem normalen Internet, und zwischen diesen zwei Weltenkönnen kaum Daten ausgetauscht werden. Der Internet-Nutzer bewegt sich entweder in dem einen oder dem anderen Netzwerk. Somit bietet das I2P keine Sicherheit, wenn das normale Internet genutzt wird.
Im Laufe der Jahre hat sich das I2P als die Standardplattform für alle, die etwas zu verbergen haben, etabliert. Es wird auch Teil des Darknet genannt. Im I2P wird alles, was man sich unter „illegal“ vorstellen kann angeboten und gehandelt. Aber nicht nur Internet-Kriminelle bedienen sich hier, auch Behörden und Geheimdienste kaufen dort gerne Ausspähsoftware, Passwörter oder „Zero-Day-Exploits[184]“ ein. Schad-Software nutzt in der Regel Software-Fehler aus, um sich auf dem Zielrechner einzunisten. Software-Fehler, die noch nicht der Allgemeinheit bekannt sind, werden Zero-Day-Exploits genannt. Falls ein Hacker eine solche Lücke findet, kann er dieses Wissen für viel Geld an andere verkaufen, die dann diese Lücke so lange ausnutzen können, bis dieser Software-Fehler behoben ist.
Mittlerweile ist I2P aber auch nicht mehr vor Ermittlungsbehörden sicher[185].

---

182 https://netzpolitik.org/2016/volksverschluesselung-fuer-unfreie-buerger/

183 https://geti2p.net/de/

184 http://de.wikipedia.org/w/index.php?title=Exploit&redirect=no#Zero-Day-Exploit

185 http://www.faz.net/aktuell/feuilleton/medien/anonymes-netzwerk-tor-das-dunkle-netz-wird-ausgeleuchtet-13258804.html

Browser-Plugins zum Schutz der Privatsphäre

Auf dem Browser-Plugin Markt gibt es eine unüberschaubare Menge an kostenloser Browser-Erweiterungen, um die Privatsphäre des Internet-Nutzers zu schützen.
Die fünf meistverwendeten Anti-Tracker-Plugins sind:

- Adblock Plus
- Privacy Badger
- Disconnect
- Ghostery
- uMatrix

Ein weiteres sehr gutes Plugin, das gegen Browser-Fingerprinting schützt, ist Random Agent Spoofer[186].
Aufgrund seiner komplexen Einstellmöglichkeiten, ist es allerdings mehr für technische Profis geeignet.
Die Webseite www.alternativeTo.net zeigt eine Übersicht der meist verbreiteten Browser-Plugins zum Schutz der Privatsphäre[187]. Sobald man allerdings tiefer in die Technik dieser Tracker-Filter einsteigt, werden einige Unterschiede in der Art und Weise wie diese Tools arbeiten, sichtbar[188].
Browser-Erweiterungen stellen jedoch auch keinen umfänglichen Schutz dar. Gründe hierfür sind:

- Sie sind nicht auf allen Internet-Devices, Betriebssystemen oder Browsern verfügbar. Internet-Devices, wie Fernseher oder Set-Top-Box, Smart Home oder Fitness Devices, ermöglichen erst gar nicht, Plugins zu installieren.
- Es ist heute üblich, zu Hause sehr viele internetfähige Geräte zu haben. Wie soll der Nutzer den Überblick behalten, ob alle Familienmitglieder wirklich alle wichtigen Plugins installiert haben, und diese Plugins richtig benutzt oder überhaupt bedient werden können?
- Andere Plugins, wie z.B. Add Blocker Plus (ABP), erlauben es Werbetreibenden sich “frei zu kaufen”, und Ghostery gehört einer Software Firma, die Daten für Werbefirmen ermittelt[189]. Wie soll ein Laie abschätzen können, ob er einem Plugin trauen kann?
- Frei verfügbare Anonymisierungs-Web-Proxys, wie der von Startpage/Ixquick[190], sind Proxies, die lediglich die Google-Suche vor Google anonymisieren. Sie verhindern aber keine Daten-Tracker, die bei weiteren Aufrufen von Folgeseiten den Nutzer ausspionieren. Proxies wie z.B. Immunityzone[191], können lediglich die Seite "in Vertretung“ aufrufen und dann ein Bild der Seite an den eigenen Browser zurück senden. Dadurch können JavaScript-Code, der eine Benutzer-Eingabe erfordert und Cookies nicht richtig verarbeitet werden. Das hat zur Folge, dass viele Webseiten nicht richtig funktionieren. Alle diese zentral gehosteten Anonymisierungs-Web-Proxys haben außerdem den Nachteil, dass der

[186] https://addons.mozilla.org/de/firefox/addon/random-agent-spoofer/

[187] http://alternativeto.net/software/ghostery/

[188] https://gigaom.com/2014/05/11/not-all-ad-blockers-are-the-same-heres-why-the-effs-privacy-badger-is-different/

[189] http://venturebeat.com/2012/07/31/ghostery-a-web-tracking-blocker-that-actually-helps-the-ad-industry/

[190] https://startpage.com/ (nachdem das Suchergebnis angezeigt wurde, auf „Anonym öffnen“ drücken)

[191] https://www.immunityzone.com

Betreiber alle Web-Aufrufe des Anwenders mit protokollieren könnte, man muss ihm somit vertrauen. Des Weiteren ist die Reaktionszeit beim Surfen sehr langsam, da zunächst einmal die gesamte Seite auf dem Proxy geladen wird, diese analysiert wird und dann erst dem Client-Web-Browser per Internet übergeben wird.
Diese Einschränkungen und Nachteile treten bei einem Proxy wie dem Proxy der TrutzBox nicht auf. Dieser Proxy wird selbst gehostet (ohne Zugriff eines Dritten) und dieser Proxy sendet alle zur Funktionalität der Webseite notwendigen Elemente an den Browser

- Die meisten Plugins sind für Laien zu kompliziert zu bedienen. Z.B. Plugins, zur Verwaltung von Cookies oder Vermeidung von Java-Script, sind nur von Experten zu bedienen. Und wenn die Webseite vom Nutzer ein Cookie verlangt, schaltet er Cookies dann doch wieder ein, da er keine Alternative kennt oder hat.

- Sehr gute aber nicht einfach zu bedienende Plugins, die das Tracking verhindern können sind:
- CanvasBlocker
- Don't FingerPrint Me
- uMatrix
- Decentraleyes
- Manche Plugins sind sehr restriktiv und blockieren alles, was evtl. schädlich sein könnte, sodass ein störungsfreies Surfen im Internet nicht mehr möglich ist. Das ist z.B. mit allen Java-Script-Blocking-Plugins der Fall, aber auch mit spezialisierten sicheren Browsern wie der Tor-Browser und dem JonDoFox.

Das Plugin „Privacy Badger“[192] fällt hier allerdings aus dem Rahmen. Es ist eines der wenigen Plugins, das nicht von einer kommerziellen Firma entwickelt wird. Des Weiteren ist es auch das einzige Tool, das keine vorgefertigte Backlist mit bekannten Tracker-Firmen nutzt, um die Tracker zu filtern, sondern während des Betriebs beim Anwender feststellt, ob der HTTP-Header Tracking-Daten an den Server liefert. Ist das der Fall, wird diese Seite mit „gelb“ gekennzeichnet, und es werden keine Tracking-Daten zurückgeliefert. Wenn Privacy Badger im späteren Verlauf des Surfens erkennt, dass die gleiche Tracking-Seite zum dritten Mal in andere aufgerufene Seiten eingebunden wurde, dann markiert sie diese Tracking Seite rot und blockiert sie für weitere Aufrufe.
Allerdings haben Browser-Plugins auch grundsätzliche Nachteile bzw. Einschränkungen. So leitet der Browser nicht alle Zugriffe durch das Plugin. Somit kann der Browser auch Tracking-Zugriffe durchführen, ohne dass ein Plugin das erkennen kann. Alle Browser greifen z.B. auf ihre eigenen Server zu, um die Nutzung des Browsers zu protokollieren und zu prüfen, ob Updates vorliegen.
Des Weiteren gibt es auch unzählige Browser-Plugins die selbst den Nutzer tracken. Dazu gibt es eine umfangreiche recht aktuelle Studie „Extended Tracking Powers: Measuring the Privacy Diffusion Enabled by Browser Extensions„[193].

[192] https://www.eff.org/de/node/73969

[193] https://www.securitee.org/files/extendedtracking_www2017.pdf

Es gibt einige Untersuchungen, die feststellen sollen, welches Browser-Plugin sich am besten zum Schutz vor Trackern eignet. Allerdings ist das nicht einfach zu beantworten, da das Plugin, das die meisten Server-Kontakte blockiert, nicht unbedingt das Beste ist[194]. Denn zu viele Seiten einfach zu sperren kann auch zu unerwünschten Fehlfunktionen der angezeigten Webseite führen. Wichtig ist auch, wie ein Tool verdächtige HTTP-Header-Daten erkennt und geeignet abändert.
Comidio hat diese unterschiedlichen Technologien analysiert und sich entschlossen, auch eine Tracker-Domain-Liste zum Erkennen von Tracker-Links einzusetzen. Aber zusätzlich erkennt die TrutzBox auch verdächtige http-Header-Daten, die der Browser an den Web-Server liefern möchte und verändert diese bei Bedarf.
Durch ihre einmalige TrutzBox Technology ist die TrutzBox in der Lage, die grundsätzlichen Nachteile von Browser-Plugins zu umgehen. Da die gesamten Filter-Funktionalitäten auf einer dedizierten Hardware automatisch für alle internetfähigen Geräte zu Hause zur Verfügung stehen, sind keine Anpassungen auf den Endgeräten nötig. Der Anwender kann sein E-Mail- und Browser-Programm weiterhin wie gewohnt benutzen. Der leicht zu bedienende „Security-Slider“ erlaubt es jedem Laien, bei auftretenden Darstellungsproblemen, die Sicherheit allmählich zurückzunehmen.

Warum es nicht ausreicht einfach nur einen Tracker-Blocker zu installieren

Auf dem Markt existieren einfache Tracker-Blocker in Form von Browser-Plugins (Ghostery, disconnect ...) oder Tracker-Blocker mit eigener Hardware wie eBlocker. Diese Werkzeuge überwachen alle Internet-Zugriffe und gleichen die aufgerufenen URLs mit eigenen Black-/White-Lists ab. Falls ein Zugriff auf eine URL stattfinden soll, die sich in der mitgelieferten Blacklist befindet, wird der Zugriff daraufhin unterbunden. Somit können keine Tracking-Daten an einen Daten-Tracker übermittelt werden. So weit so gut.
Es gibt jedoch in Web-Seiten Server-Kontakte zu fremden Servern, die man nicht ohne weiteres blockieren sollte, obwohl diese nicht immer für die Funktionalität einer Webseite benötigt werden. Diese Server-Kontakte finden oft sofort statt, wenn die Seite geladen wird. Allerdings wird dieser Server erst benötigt, wenn man eine bestimmte Funktion auf der Web-Seite anklickt.
Hierzu ein Beispiel (Stand 3.3.2020):
Beim Aufruf der Seite welt.de wird automatisch sofort auch podigee.com kontaktiert. Über podigee.com wird ein Podcast Player in die Webseite von welt.de geladen. Bei dem Kontakt mit podigee.com wird auch eine eindeutige ID übergeben und podigee.com speichert auch gleich noch einen Cookie, mit dessen Hilfe man spätere Kontakte wieder diesem Nutzer zuordnen kann. Es ist eigentlich nicht notwendig dass welt.de sofort diesen Server-Kontakt herstellt und evtl. persönliche Daten an podigee.com übergibt. Es würde genügen, wenn welt.de die Podcast-Funktion auf der Web-Seite erst dann aktiviert, wenn der Benutzer diese Funktion auf der Web-Seite aufruft.
In diesem Fall muss ein Tracker-Blocker diese Verbindung zu podigee.com mit all seinen Nebenwirkungen zulassen, da ansonsten die Podcast-Funktion nicht funktionieren würde. Auch die TrutzBox lässt diesen Kontakt zu podigee.com zu, aber sie übergibt bei aktivierten TrutzBrowse nicht alle angeforderten Daten an podigee.com und verhindert auch, dass podigee.com einen Cookie setzen darf.

[194] http://www.areweprivateyet.com

Verschleierung von IP-Adressen

Bei jedem Internet-Datentransfer erhält der Server die IP-Adresse des Clients (bzw. des Internet-Routers des Clients). Das ist im IP-Routing Protokoll fest definiert. Über diese IP-Adresse lässt sich sehr einfach der Internet-Service-Provider (über den der Nutzer seinen Internetanschluss geliefert bekommt) ermitteln. Kommerzielle Daten-Tracker, die über einen längeren Zeitraum das Nutzerverhalten über mehrere Webseiten tracken möchten, interessieren sich meist nicht für die IP-Adresse, da diese sich bei Privatanwendern normalerweise täglich ändert. Allerdings kann ein Tracker die ungefähre Lokation des anfragenden Geräts ermitteln.
Falls aber ein juristisch begründetes Interesse besteht, kann bei dem Internet-Service-Provider die Identität des Internetanschlusses (also Benutzername und -adresse) in Erfahrung gebracht werden. Somit kann ein Web-Service Anbieter über die IP-Adresse mit hoher Wahrscheinlichkeit herausfinden, aus welchem Land der Aufruf seiner Webseite kam und, abhängig vom Land, Daten sperren (z.B. Youtube Videos nur für bestimmte Länder frei geben). Ermittlungsbehörden, Abmahnanwälte und Geheimdienste können über diesen Weg auch den Aufrufer einer Webseite herausfinden und gegen ihn ermitteln. Es kann also viele Gründe geben, die IP-Adresse zu verschleiern.
Zwei technische Möglichkeiten gibt es, die IP-Adresse so zu verschleiern, dass der Server, von dem Daten abgerufen werden, die IP-Adresse des Clients auf den ersten Blick nicht erkennen kann:

- VPN Gateways und Internet-Proxys
- Tor

Bei beiden lösungen werden ein oder mehrere (kaskadierte) Netzwerk-Proxys im Internet genutzt. Diese unterbrechen das Netzwerk zwischen dem Benutzer und dem Server und bauen anschließend eine neue Netzwerkverbindung zum Ziel auf. Allerdings sind auch diese drei Verfahren nicht 100% sicher, da immer die Möglichkeit besteht, durch „Website Fingerprinting“ die durch den Proxy erreichte Anonymisierung aufzuheben. Beim „Website Fingerprinting“ vergleicht ein globaler Angreifer den Anfang und das Ende der Proxy-Kette und kann durch eine „Korrelationsanalyse“ dem anonymisierten Benutzer den ursprünglichen Auftraggeber wieder zuordnen[195].
Des Weiteren kann es auch sein, dass die Webanwendung selbst die IP-Adresse an den Server weiterleitet (z.B. der Flash-Player den die Webseite nutzt).

Vergleich der beiden Verschleierungstechniken

Technisch gibt es zwei verschiedene Möglichkeiten, die IP-Adresse des Clients zu verschleiern.

VPN Gateways und Internet-Proxys

VPN Gateway Provider und Internet-Proxys sind keine gute Lösung, wenn es um Anonymisierung geht. Viele nutzen VPN Provider, um Restriktionen von Medienanbietern wie YouTube oder Netflix zu umgehen. Das funktioniert sogar in manchen Fällen (abhängig davon, wie der Anbieter das Herkunftsland des Clients prüft, und wie genau das VPN aufgesetzt wurde). Allerdings kann der VPN Provider in der Regel nicht nur den gesamten Datenverkehr mitlesen, sondern sogar manipulieren (da er technisch eine Art

195 http://www.heise.de/security/meldung/I-f-Tor-Deanonymisierung-zu-81-erfolgreich-2458992.html?wt_mc=nl.heisec-summary.2014-11-20

„Man in the Middle“ darstellt). Oftmals bieten auch Kriminelle solche VPN Dienste an, um Daten mitzulesen (evtl. sogar Passwörter) oder Daten zu Ihrem Schaden zu manipulieren.
Diese Meinung vertritt auch die englische Ausgabe der Zeitschrift Wired und warnt vor allem vor kostenlosen VPN Angeboten.[196]
Die Seite vpnpro.com gibt eine Übersicht über VPN-Anbieter und stellt fest, dass 101 VPN-Anbieter lediglich von 23 Firmen betrieben werden[197],[198].

Bei dem kostenlosen VPN-Dienst „Hotspot Shield Free“ wurde nachgewiesen, dass er „...personalisierten Werbeanzeigen in die Gratis-Version seines VPN-Clients zu injiziert und außerdem den Standort des Nutzers trackt“[199].

Aber wie alle zentralen Services sind auch VPN-Gateway-Betreiber nicht davor gefeit, gehackt zu werden. Jüngstes Beispiel ist das Eindringen von Hackern in die VPN-Server der Firma „NordVPN“[200]. Solche Hacks sind besonders folgenreich, da Hacker mit gestohlenen privaten VPN-Schlüsseln VPN-Verbindungen abfangen können und damit Zugriff auf die verbundenen Geräte bekommen. Zumindest sind solche zentrale Gateway-Betreiber in vielen Ländern gezwungen, Verbindungsprotokolle aufzuzeichnen und an Behörden auszuliefern. Besonders ärgerlich ist, wenn ein Hersteller von VPN-Hardware es nicht schafft, Sicherheitslücken schnell zu schließen und dann gehackte Firmenzugänge im Internet veröffentlicht werden. Genau das ist den Nutzern des VPN-Servers „Pulse Connect Secure“ passiert, als im August 2020 1800 IP-Adressen mit Benutzernamen und Passwörtern veröffentlicht wurden, mit denen man sich in 900 Firmennetze einloggen konnte. Und das, obwohl die Sicherheitslücke seit April 2019 bekannt war [201].
Besonders bedenklich wird es, wenn der VPN-Anbieter auch noch bewusst Daten sammelt. So sammelt z.B. die Firma „Sensor Tower“ Daten für seine eine Analyse-Plattform und bietet gleichzeitig einen VPN-Dienst an[202].

Es gibt Anbieter, die eine eigene Hardware-Box anbieten, die das Konfigurieren des VPN Zugangs auf Client-Seite übernehmen („Project Sierra network encryption device” oder „Wemagin »). Da aber deren Techniken lediglich die Eigenschaften von VPN Netzwerken nutzen, ist wirkliche Anonymisierung und Ende-zu-Ende Verschlüsselung nicht gegeben. Wemagin behaupten zwar, alle anderen Probleme auch gelöst zu haben, verschweigt aber leider, wie sie das angestellt haben wollen.

Tor

Wenn Webseiten über das Tor-Netzwerk[203] aufgerufen werden, kann Tor die IP-Adresse verschleiern. Technisch ist dies Tor gut gelungen, aber mittlerweile sind sich Experten ziemlich sicher, dass viele Tor-Exit-Server, die bei unverschlüsseltem Datenverkehr alle Daten mitlesen können, durch die NSA (und

[196] https://www.wired.co.uk/article/free-vpn-android-ios-privacy

[197] https://vpnpro.com/wp-content/uploads/Infographic-VPNpro-97-VPN-products-run-by-just-23-companies.pdf

[198] https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/

[199] https://www.heise.de/newsticker/meldung/VPN-Anbieter-Aktivisten-beklagen-Datenmissbrauch-3795523.html

[200] https://www.heise.de/security/meldung/NordVPN-Co-Hacker-stiegen-in-Server-von-verschiedenen-VPN-Anbietern-ein-4563846.html

[201] https://www.heise.de/news/Liste-mit-900-VPN-Firmenzugaengen-in-Erpresserforum-veroeffentlicht-4863761.html

[202] https://www.buzzfeednews.com/article/craigsilverman/vpn-and-ad-blocking-apps-sensor-tower

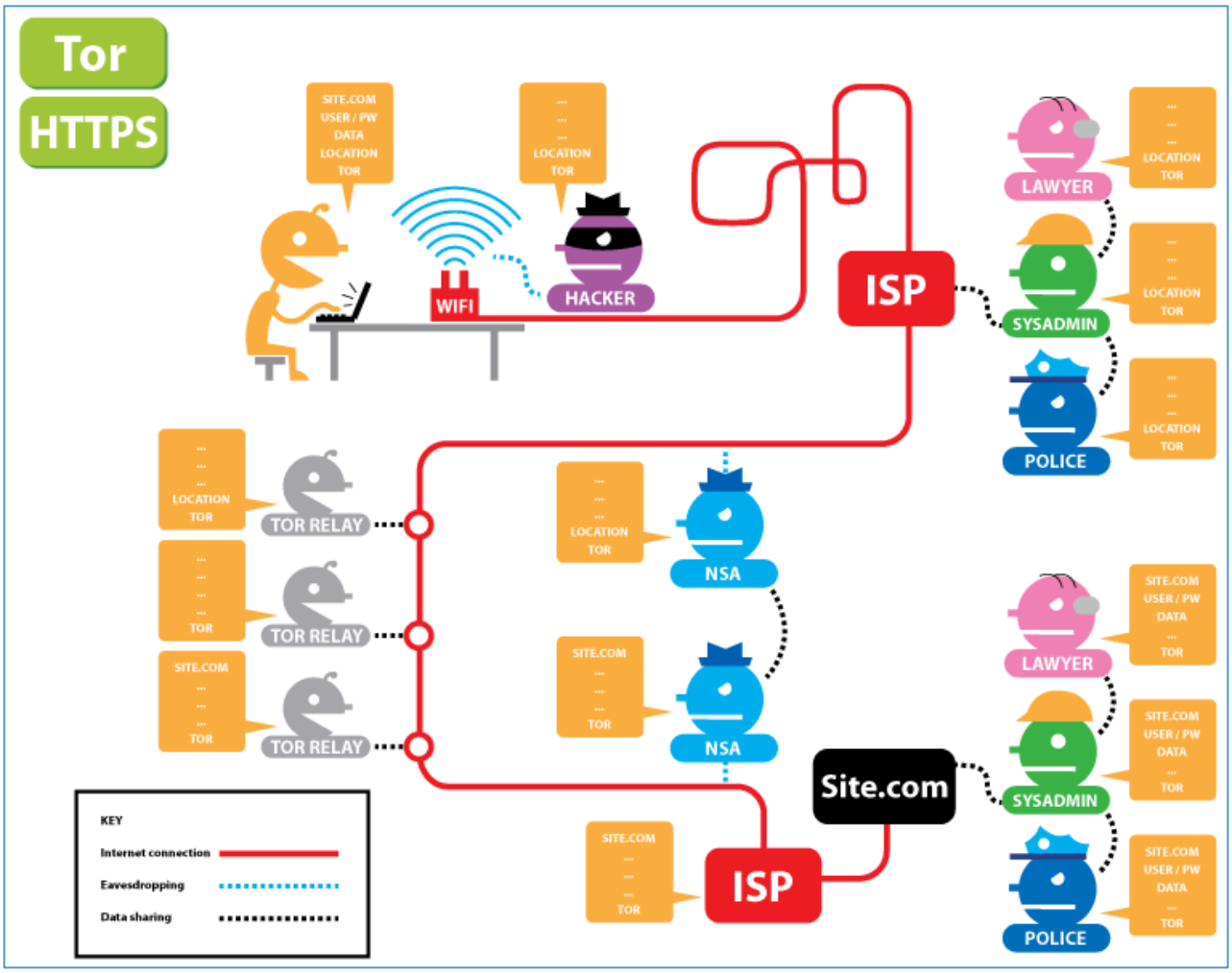
[203] https://de.wikipedia.org/wiki/Tor_(Netzwerk)

anderen staatlichen Institutionen) infiltriert worden sind. Die NSA betreibt wahrscheinlich viele dieser Exit-Server bzw. hat einige dieser Exit-Server gehackt und mit eigenem Code präpariert[204]. Nicht nur Geheimdienste sind gerade an dem Tor-Datentransfer sehr interessiert. Auch kriminelle Hacker haben sich solcher Exit-Servern bedient, um Schadcodes zu verteilen[205].
Selbst die Tor Entwickler warnen mittlerweile davor, sich zu sehr auf Tor zu verlassen[206]. Es wurde schon dokumentiert, dass speziell der Datenverkehr von Tor-Exit-Servern von staatlichen Einrichtungen auf verdächtige Schlüsselwörter hin gescannt wird. Diese Art von Angriffen auf das Tor-Netzwerk ist für TrutzMail keine Gefahr, da TrutzMail die Daten End-to-End verschlüsselt überträgt.
Es gibt auf dem Markt einige Anbieter, die den Einstieg in Tor durch eine eigene Hardware-Box erleichtern (z.B. Invizbox, Cloak, TorFi, PORTAL oder Anonabox). Diese wird zu Hause hinter den Internet-Router platziert, sodass sämtlicher Internet-Datenverkehr von dieser Tor-Box durch das Tor-Netzwerk geleitet wird.
Viele unbedarfte Nutzer glauben, dass sie durch Tor anonym im Internet unterwegs sind und niemand ihre Daten mitlesen kann. Sie sind sich nicht bewusst, dass dies nicht stimmt und dass die Gefahr groß ist, dass sie gerade so in das Visier der Geheimdienste geraten. Sie wissen auch nicht, dass Tracking durch Browser-Fingerprinting durch Tor nicht verhindert werden kann. Erst wenn Tor richtig installiert wurde und die Verbindung zum Web-Server obendrein noch verschlüsselt ist, dann kann zumindest der Datenverkehr zwischen dem Device und dem Server nicht mehr mitgelesen werden.
Aber der Client hat keinen Einfluss darauf, ob der Server eine verschlüsselte Verbindung anbietet (HTTPS - TLS). Selbst wenn beide Voraussetzungen gegeben sind, kann der Betreiber des Servers und alle anderen Daten-Tracker, die in seiner Webseite mit eingebunden sind, das Browser-Profil und Surf-Verhalten des Internet-Nutzers tracken. Das wird allerdings von TrutzBrowse verhindert.
Unabhängig davon, dass Daten-Tracker weder durch Tor noch durch verschlüsselte HTTPS-Verbindungen verhindert werden, ist selbst der Weg der Daten vom Browser zum Web-Server nicht wirklich abhörsicher. Folgende Animation zeigt sehr schön, wie sich verschlüsselte HTTPS-Verbindungen und Tor auf die Datensicherheit auswirken und wer trotzdem bei welcher Konstellation noch welche Daten abgreifen kann: https://www.eff.org/pages/tor-and-https.

204 http://www.heise.de/newsticker/meldung/Neues-von-der-NSA-Tor-stinkt-1972983.html

205 http://www.heise.de/newsticker/meldung/Russischer-Tor-Server-schleuste-Malware-in-Programme-2432114.html
http://www.heise.de/security/meldung/OnionDuke-Downloads-von-Tor-Nutzern-mit-Schadcode-verseucht-2457271.html?wt_mc=nl.heisec-summary.2014-11-17

206 http://www.spiegel.de/netzwelt/netzpolitik/wie-sicher-sind-hidden-services-im-tor-netzwerk-a-1001969.html



Dabei werden folgende Interessensgruppen und Daten-Gruppen unterschieden:
Interessensgruppen die Zugriff auf Daten haben:

- User: Anwender
- Hacker: der beim Anwender das WLAN/Router abhört
- Lawyer: Anwender-ISP-Lawyer: (z.B. Abmahn-) Anwalt
- SYSADMIN1: Anwender-ISP SysAdmin – Systemtechniker des Internet Service Providers
- POLICE: Anwender-ISP Police: Polizei, Ermittlungsbehörden
- TorRelay1: Betreiber eines Tor-Eintritts-Servers
- TorRelay2: Betreiber eines Tor-Vermittlungs-Servers
- TorRelay3: Betreiber eines Tor-Austritts-Servers
- NSA1: Geheimdienste die den Internet-Backbone vor TOR abhören
- NSA2: Geheimdienste die den Internet-Backbone nach TOR abhören
- ISP: Internet-Service-Provider des Server Betreibers
- Lawyer: Server Betreiber-ISP-Lawyer: (Abmahn-) Anwalt
- SYSADMIN2: Systemtechniker des Server Betreibers
- POLICE: Server Betreiber-ISP Police: Polizei, Ermittlungsbehörden

Haben Zugriff auf welche Daten:

- SITE.COM: die Seite die aufgerufen wird
- USER/PW: eingegebenes Benutzer-ID und Passwort
- DATA: die übertragenen Daten
- LOCATION: die IP-Adresse des Benutzers und damit den Standort und Identität des Benutzers
- TOR: ob der Benutzer Tor benutzt oder nicht

Wer kann bei Nutzung von TOR und/oder HTTPS welche Daten sehen?

Wer kann meine Daten sehen	User: Anwender	Hacker: der beim Anwender das WLAN/Router abhört	Lawyer : Anwender-ISP-Lawyer: (Abmahn-) Anwalt	SYSADMIN: Anwender-ISP SysAdmin – Systemtechniker	POLICE: Anwender-ISP Police: Polizei, Ermittlungsbehörden	TorRelay1: Betreiber eines Tor-Eintritts-Servers	TorRelay2: Betreiber eines Tor-Vermittlungs-Servers	TorRelay3: Betreiber eines Tor-Austritts-Servers	NSA1: Geheimdienste die den Internet-Backbone vor TOR abhören	NSA2: Geheimdienste die den Internet-Backbone nach TOR abhören	ISP: Internet-Service-Provider des Server Betreibers	Lawyer : Server Betreiber-ISP-Lawyer: (Abmahn-) Anwalt	SYSADMIN2: Systemtechniker des Server Betreibers	POLICE: Server Betreiber-ISP Police: Polizei, Ermittlungsbehörden
Ohne HTTPS und ohne TOR	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort
nur mit TOR	Ziel-Seite, Uid+PW, Daten, Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	....., ..., ..., Standort, TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR
nur mit HTTPS	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, ..., ... Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort	Ziel-Seite, Uid+PW, Daten, Standort
HTTPS und TOR	Ziel-Seite, Uid+PW, Daten, Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., Standort, TOR	....., ..., ..., TOR	Ziel-Seite, ..., ... Standort	....., ..., ..., Standort, TOR	Ziel-Seite, ..., ..., ..., TOR	Ziel-Seite, ..., ..., ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR	Ziel-Seite, Uid+PW, Daten, ..., TOR

(© 2015 Comidio GmbH)

Somit kann Tor lediglich die IP-Adresse des Nutzers verschleiern. Comidio hat in TrutzBrowse diese Möglichkeit als zuschaltbare Option eingebaut.

Keine IP-Verschleierungstechnik ist perfekt

Vergleicht man die beiden vorgestellten Anonymisierungsdienste, so bieten die VPN Betreiber den geringsten und Tor den größten Schutz gegen die Aufhebung der Anonymisierung (also Rückverfolgung) der IP-Adresse.
Hacker und kommerzielle Tracker interessieren sich kaum für die IP-Adresse des Nutzers. Das liegt zu einem daran, dass sich bei privaten Internet-Nutzern die IP-Adresse meist täglich ändert und somit für Fingerprinting kaum geeignet ist. Zum anderen ist es auch nicht möglich aus der IP-Adresse die wahre Identität des Anwenders zu ermitteln, ohne die Identität des Angreifers aufzudecken. Besonderes Interesse an der IP-Adresse haben somit Ermittlungsbehörden und Abmahnanwälte, die den IP-Provider zur Herausgabe der Adressdaten eines Kunden zwingen können.

Beide beschriebenen Methoden zur IP-Verschleierungstechnik verschleiern die IP-Adresse lediglich auf Netzwerkebene. Aber eine Applikation auf Client-Seite ist meist trotzdem in der Lage, die externe IP-Adresse zu ermitteln und nach Anforderung an einen neugierigen Server zu übermitteln. Diese Applikation kann ein Browser sein, aber auch jede beliebige andere Anwendung auf dem Client. Um möglichst sicher zu sein, dass die eigene IP-Adresse trotz Nutzung von Tor nicht übermittelt wird, sollte man wissen, ob eine gerade genutzte Anwendung dazu in der Lage ist. Jeder Standard-Browser ist dazu in der Lage, da dazu der Server lediglich ein paar Zeilen JavaScript auf seine Webseite programmieren muss. Aber selbst wenn man JavaScript ausschaltet, gibt es mindestens drei weitere Browser-Funktionen mit deren Hilfe der Server die IP-Adresse ermitteln könnte:

- WebRTC: ist eine Browser-Funktion, die fast jeder aktuelle Standard-Browser beherrscht und über einen speziellen Aufruf die IP-Adresse übermittelt. Mit https://www.privacy-tools.io/webrtc.html lässt sich leicht herausfinden, ob die IP-Adresse trotz IP-Anonymisierung über WebRTC ermittelt werden kann.

- Das Flash-Modul des Browsers: mit dieser Funktion wurde die Tor-Hacking-Software Torsploit entwickelt, mit dessen Hilfe das FBI einige illegale Shops und deren Kunden im DarkNet aufspüren konnte[207]. Mit http://ip-check.info lässt sich herausfinden, ob die IP-Adresse trotz IP-Anonymisierung über das Flash-Modul des Browsers ermittelt werden kann.

- FTP: jeder moderne Browser beherrscht auch das FTP-Protokoll, und zumindest der Standard-Browser unter IOS lässt es zu, dass ein Server über FTP trotz Proxy-Einstellung die IP-Adresse ermitteln kann. Auch das lässt sich mit https://whatismyipaddress.com/ feststellen.

Um ganz sicher zu gehen, dass zumindest der Browser die IP-Adresse nicht trotzdem übermittelt, ist es empfehlenswert, einen angepassten Browser wie den Tor-Browser[208] zu verwenden. Leider ist der Tor-Browser derart restriktiv, dass das Surfen auf normalen Webseiten im Internet (also nicht auf Webseiten im Tor-Netzwerk) sehr schnell zu Funktionsproblemen führt.

Sichere E-Mails

Besonders schwierig ist es auch, E-Mails sicher zu übertragen. Es gibt zwar schon seit Jahren für fast alle E-Mail Programme PGP bzw. S/Mime Erweiterungen, mit dessen Hilfe E-Mails verschlüsselt werden, aber diese werden kaum genutzt. Auch wenn es relativ einfach ist, diese Erweiterungen zu installieren, so muss man zunächst einmal verstehen, wie man die notwendigen Schlüssel bezieht, verwendet und verwaltet. Und da das sowohl Absender als auch Empfänger machen müssen, hat sich das Verschlüsseln von E-Mails bis heute im täglichen Gebrauch nicht durchsetzen können. Selbst Unternehmen tauschen in der Regel E-Mails unverschlüsselt aus.
Aber selbst wenn E-Mails verschlüsselt werden, verschlüsseln diese E-Mail Erweiterungen lediglich den E-Mail Inhalt. Die E-Mail Metadaten sind weiterhin auf dem Weg zwischen Absender und Empfänger

[207] http://www.heise.de/ix/meldung/Ehemaliger-Tor-Entwickler-steckt-hinter-der-FBI-Malware-Torsploit-3194740.html

[208] https://www.torproject.org/download/download-easy.html.en

lesbar. E-Mail Metadaten sind z.B. wer, hat wann, von welchem Standort, an wen, mit welchem Betreff eine Mail ausgetauscht. Und gerade Metadaten sind für bestimmte neugierige Gruppen im Internet sehr interessant.
Mittlerweile ist die Kommunikation zwischen dem Mail-Programm auf meinem Endgerät mit dem Mail-Server zwar verschlüsselt, aber der Mail-Provider kann unverschlüsselte Mails lesen. Und die Kommunikation zwischen den Mail-Servern ist gelegentlich auch unverschlüsselt, sodass jeder, der Zugriff auf das Internet-Netzwerk hat, alle Mails lesen kann. Und das sind weit mehr als man denkt.
Es gibt auf dem Markt wohl neben der TrutzBox keine weitere Mail-Lösung, die

- die komplette Mail (also inklusiver Metadaten) verschlüsseln kann,
- das Standard-Mail-Format mit allen seinen Features beibehält,
- ohne Änderung von jedem gewohnten Mail-Programm nutzbar ist und
- die gesamte Verwaltung der Mail-Schlüssel so automatisiert hat, dass der Anwender nie mit Mail-Schlüsseln in Berührung kommt.

Dass E-Mails inklusive der Metadaten verschlüsselt werden und das gewohnte Mail-Programm ohne Änderung weiter verwendet werden kann, ist vor allem für Firmen eine wichtige Voraussetzung. Firmen brauchen die Verschlüsselung der Metadaten, da sie nicht Preis geben möchten, mit wem sie regelmäßig E-Mails austauschen. Und für Firmen wäre es ein unzumutbarer Aufwand, ein zweites E-Mail-Programm auf allen Firmen-PCs für alle Mitarbeiter zu unterstützen.

Sichere Chat- und Audio-/Video-Kommunikation (RTC – Real-Time-Communication)

In den letzten Jahren haben sich viele Lösungen für Chat- und Audio-/Video-Kommunikation im Markt etabliert. Firmen nutzen Video-Konferenz-System Services wie z.B. von Apple, Microsoft, Zoom, Adobe oder Cisco, um intern oder mit externen Teilnehmen zu konferieren. Im Privatmarkt haben sich neben Apple, Threema, Telegram, Signal vor allem WhatsApp als Messenger und Konferenzwerkzeug durchgesetzt.
Zunehmend haben die Hersteller dieser Software auch Funktionen zum End-to-End Verschlüsseln der Kommunikationsinhalte eingebaut[209].
Aber bisher gibt es keine einzige massenmarkttaugliche Lösung auf dem Markt, mit deren Hilfe es nicht möglich wäre, das Kommunikationsverhalten von Nutzern zu analysieren. Das liegt daran, dass alle Lösungen von zentralen Dienstleistern betrieben werden. Da diese zumindest die Vermittlung der Kommunikationsteilnehmer übernehmen, sind sie durch die Analyse der Metadaten technisch in der Lage, sehr aussagekräftige Kommunikationsprofile zu erstellen. Diese Sicherheitslücke kann nur durch ein Eigenhosting gelöst werden. Also den Video/Chat -Konferenzserver selbst betreiben.

[209] http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/so-verschluesseln-whatsapp-facebook-google-skype-co-14403760.html?printPagedArticle=true#pageIndex_2

Was ist eine „Security & Privacy-Box“?

Was versteht man unter einer "**Security & Privacy-Box**" bzw. was kann man von ihr erwarten? Definition von Comidio:

*Eine **Security & Privacy-Box** ist ein elektronisches Gerät in Form einer Hardware-Software-Kombination, welches maximale Sicherheit und Privatheit bei der Nutzung des Internets bietet.*

Was kann man aufgrund dieser Definition von einer **Security & Privacy-Box** erwarten? Hierzu hat Comidio folgende Anforderungen zusammengestellt, die auch Grundlage beim Design der TrutzBox maßgebend war.

- Schutz für alle Internetaktivitäten: eine Security & Privacy-Box sollte Privatheit bei möglichst allen Tätigkeiten im Internet ermöglichen. Also egal was man im Internet macht, beim E-Mailen, Surfen/Browsen, Chatten, bei Video-Audio-Konferenzen usw. sollte eine Privacy-Box für Sicherheit und Privatheit sorgen. Denn was nützt es, wenn man zwar beim Surfen geschützt ist, aber beim Chatten oder E-Mailen seine privaten Daten irgendwelchen, unbekannten Datenhändlern oder kriminellen Hackern ungefragt und ohne Zustimmung preisgibt.

- Internet-Sicherheit und Privatheit sind untrennbar miteinander verbunden. Sobald Angreifer die Internet-Sicherheit überwinden können, ist die Privatheit automatisch gefährdet. Wenn ein Angreifer Schadsoftware auf einem PC oder ein IoT-Gerät platzieren kann, ist er in der Lage, auch private Daten zu lesen und diese zu missbrauchen. Je mehr ein Angreifer über uns weiß, um so einfacher kann dieser uns angreifen und unsere Sicherheit kompromittieren. Deswegen wird von einer solchen Lösung neben Schutz der Privatsphäre zusätzlich auch Internet-Sicherheit erwartet.

- Schutz aller Geräte: eine Security & Privacy-Box sollte alle am Internet angeschlossenen Geräte schützen. Wir nutzen heute schon verschiedene Betriebssysteme, PC-Hardware, Fernseher Fitness-Armbänder und sonstige IoT-Geräte. Auf allen diesen Geräten sind persönliche Daten gespeichert, die vor unberechtigtem Zugriff geschützt werden müssen. Gerate Iot Geräte sind für Angreifer besonders interessant, da diese schlecht zu schützen sind und kompromittierte Geräte Jahrelang unentdeckt von Angreifern für kriminelle Handlungen genutzt werden können.

- Gesamter Internet-Datenverkehr sollte kontrolliert werden: es gibt unzählige Browser-Plugins, die Daten-Tracker stoppen und vor Werbung schützen. Da aber ein Internet-Browser immer auch Plugins umgehen kann und an den Plugins vorbei Daten mit dem Internet austauscht, kann selbst das beste Plugin nicht alle Daten kontrollieren. Und da Browser-Plugins Apps auf PCs oder Smartphones nicht schützen, und es für die meisten IoT-Geräte keine Möglichkeit gibt, deren Datenaustausch zu kontrollieren, ist es unabdingbar, den Datenaustausch auf Netzwerk-Ebene an zentraler Stelle, also außerhalb des zu kontrollierenden Gerätes, zu überwachen. Nur so ist gewährleistet, dass kein Gerät unbeobachtet Daten mit dem Internet austauscht.

- Es wird auch oft diskutiert, ob eine Security & Privacy-Box auch verschlüsselten Datenverkehr kontrollieren soll. Ja, soll sie. Denn gerade Apps kommunizieren verschlüsselt mit Daten-Trackern, die die Privatsphäre kompromittieren. Einer Security & Privacy-Box muss man immer vertrauen, deshalb ist das potenzielle Aufbrechen der Verschlüsselung ein kleineres Sicherheitsrisiko, als den verschlüsselten Datenverkehr unkontrolliert durchzulassen.

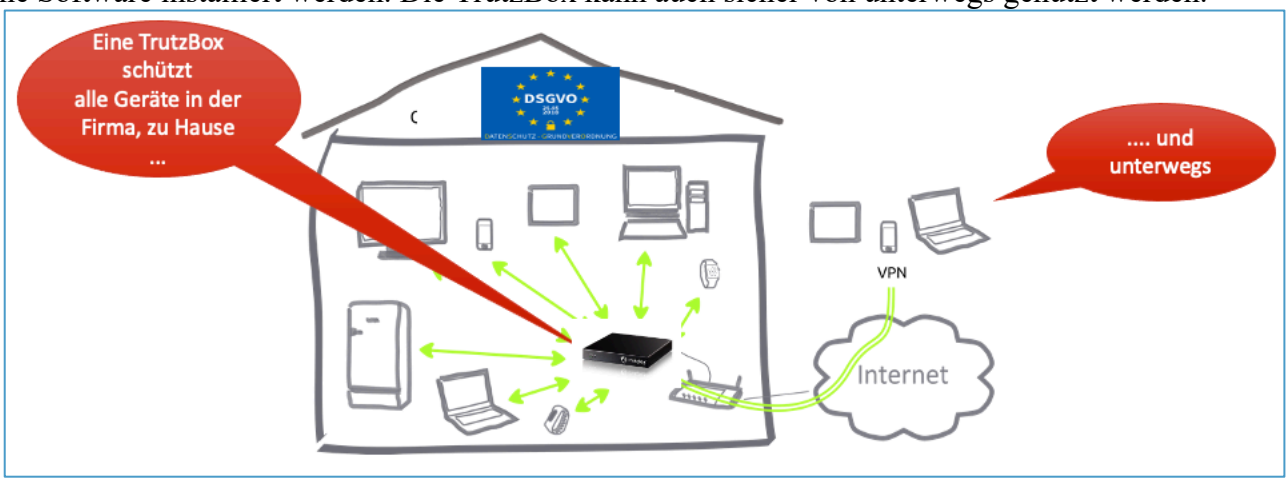
- Einfache Installation und Nutzung: nur wenn eine Security & Privacy-Box einfach zu installieren und zu betreiben ist, wird sie auch genutzt. Kompliziert zu bedienende Browser-Plugins wie z.B. NoScript oder die E-Mail-Schlüsselverwaltung führen dazu, dass NoScript kaum genutzt wird und auch E-Mails selten verschlüsselt werden. Das sollte mit einer Security & Privacy-Box möglichst ohne Änderung der Benutzer-Gewohnheiten automatisch funktionieren. Somit sollte der Nutzer alle seine Programme auf allen Devices wie gewohnt weiter nutzen können und von der zusätzlichen gewonnen Privat- und Sicherheit gar nichts merken. Auch sollte die Performance durch die Nutzung einer Security & Privacy-Box den Nutzer nicht einschränken und in seinem Tun behindern.
- Man muss der Security & Privacy-Box vertrauen können: da eine Security & Privacy-Box als eines der besten Überwachungsinstrumente missbraucht werden könnte, ist es unabdingbar, dass man der Security & Privacy-Box vertrauen kann. Dazu gehört, dass sämtliche Software der Lösung quelloffen ist, so dass Fachleute diese verifizieren können. Außerdem muss sie durch Nutzung aktueller Sicherheits-Technologien vor Angreifern bestmöglich geschützt sein. Das Unternehmen, das die Privacy-Box herstellt und betreibt, muss unabhängig von externer Einflussnahme sein und frei von finanzieller oder sonstiger vertraglicher Verflechtung mit anderen Unternehmen, die den Schutz der Privacy-Box einschränken oder sogar missbrauchen könnten.
- **Bezahlbar um massentauglich zu sein:** das betrifft nicht nur den Kaufpreis, sondern auch die laufenden Kosten für Service und Stromverbrauch.

Die Comidio GmbH hat bei der Entwicklung der TrutzBox diese Anforderungen alle berücksichtigt und konnte diese Anforderungen auch ziemlich umfänglich abdecken.
Natürlich hat eine Security & Privacy-Box auch Nachteile die hier nicht verschwiegen werden sollten. Neben den zusätzlichen Kosten macht jede zusätzliche Erweiterung des eigenen Netzwerks die technische Infrastruktur komplexer. Auch kann ein solches zusätzliches Gerät ausfallen oder Fragen bei der Bedienung aufwerfen. Das bedeutet zusätzlicher Zeitaufwand um sich mit diesem zusätzlichen Device zu beschäftigen.
Aber die Vorteile einer Security & Privacy-Box liegen auf der Hand: nur eine Lösung, die sämtlichen Datenverkehr mit dem Internet kontrollieren kann, ist in der Lage, das gesetzlich zugesicherte Recht auf Privatheit und Kontrolle der eigenen Daten sicherzustellen.

Comidio TrutzBox Funktionen und Architektur

Eric Schmidt, Google, 2013*: „Ihr müsst für eure Privatsphäre kämpfen, oder ihr werdet sie verlieren“*[210]

Die TrutzBox ist ein Werkzeug zur „Digitalen Selbstverteidigung“. Mit Hilfe der TrutzBox kann vermieden werden, dass unnötig Daten heraus gegeben werden. Die TrutzBox ist eine Hardware/Software-Kombination, die in das interne Netzwerk eines Haushalts oder einer Firma installiert wird und die alle Geräte schützt, die Zugriff auf das Internet haben. Auf diese zu schützenden Geräten muss keine zusätzliche Software installiert werden. Die TrutzBox kann auch sicher von unterwegs genutzt werden.



(© 2015 Comidio GmbH)

Dadurch gibt die TrutzBox die Kontrolle über die Daten an den Benutzer zurück.
Sie bietet folgende Sicherheits- und Anonymisierungsvorteile:

- Im **Internet surfen, ohne dass Datenspuren** des Nutzers von anderen mitgelesen werden können (TrutzBrowse)
- Vermeidung von Spuren aller Geräte (Browser, IoT-Geräte, Apps…)
- **Kinder- bzw. Jugendschutz**, durch Einstellmöglichkeiten festlegen; wer welche Webseiten aufrufen darf (TrutzContent)
- Die TrutzBox bietet dem Nutzer die Möglichkeit des **Eigenhostings**; d.h. er ist nicht mehr so oft auf Dienstleister im Internet angewiesen, die ihm nicht die erforderliche Sicherheit und Anonymität bieten,
- **Sichere, verschlüsselte E-Mails** die bei der Übertragung nicht mit-gelesen oder sogar manipuliert werden können. Außerdem wird sichergestellt, dass die E-Mail-Adresse des Absenders wirklich von diesem E-Mail-Account kommt.
- **Video-Konferenzen (TrutzMeeting) und Chat (TrutzChat)** TrutzRTC. Dadurch ist der Nutzer nicht mehr auf Dienstleister wie Zoom oder Whatsapp angewiesen, bei denen er die Services mit seinen Daten bezahlt.

[210] http://www.telegraph.co.uk/technology/eric-schmidt/10076175/Eric-Schmidt-interview-You-have-to-fight-for-your-privacy-or-you-will-lose-it.html (abgerufen am 4.12.2015)

- Zusätzlich schützt die TrutzBox auch vor „Einbrechern“ in das **sichere lokale Netzwerk** des Nutzers - TrutzBase (Firewall und Network Intrusion Detection System (N-IDS)).

Somit kann der Internet-Nutzer mit Hilfe der TrutzBox kontrollieren, welche Daten er wem geben möchte. Das Einzigartige an der TrutzBox ist, dass der Benutzer TrutzBox-Funktionen mit allen seinen internetfähigen Geräten zu Hause oder in seinem Unternehmen nutzen kann. Also können nicht nur PC, MAC oder mobile Geräte sondern auch Fernseher, mobile Geräte wie iPhone, iPad, Android-Geräte usw. als auch schon vorhandene oder zukünftige „Smart Home“ Geräte wie Heizung, Zahnbürste oder Fitness-Armband kontrolliert und geschützt werden.
Bei der Architektur der TrutzBox wurden viele der bisher hier erwähnten Bedrohungen und Abwehrmöglichkeiten berücksichtigt. Es wird jedoch nie möglich sein, sich gegen alle dieser Bedrohungen vollständig zu schützen. Hundertprozentige Sicherheit gibt es nicht, auch nicht mit der TrutzBox. In der Praxis muss immer ein Kompromiss zwischen diesen vier Anforderungen gefunden werden:

- Marktreife - man kann endlos den Bedrohungen hinterher laufen und Zug um Zug Lösungen in das Produkt einbauen. Aber die Lösung kommt nie auf den Markt,
- dem Grad des Schutzes,
- den Kosten für Entwicklung und Betrieb (somit auch der Preis den der Kunde zu zahlen hat) und
- der Bedienbarkeit für den Anwender.

Comidio ist in Bezug auf diese Anforderungen ein guter Kompromiss gelungen.
Die folgenden Kapitel beschreiben die TrutzBox Funktionen und ihre technische Umsetzung.

Comidio BSS (Business Support System) und OSS (Operational Support System)

Comidio unterhält zum Verwalten seiner Kunden und der TrutzBoxen ein BSS (Business Support System) und ein OSS (Operational Support System). Das BSS beinhaltet die trutzbox.de Webseite inkl. Content-Management-System, den Shop, CRM und Payment System. BSS und OSS dienen Comidio dazu, dem Kunden nach dem Kauf die Comidio TrutzServices liefern zu können.

TrutzServices

Ein Kunde kann eine, oder falls eine Firma gleich mehrere Remote-Mitarbeiter damit ausstatten möchte, auch mehrere TrutzBoxen kaufen. Er kauft gleichzeitig ein Servicepaket dazu (TrutzServices). Der Services-Vertrag stellt den Comidio-Support und die TrutzBox Updates sicher. Der Services-Vertrag steuert auch die Laufzeit der TrutzMail Zertifikate und damit die Nutzbarkeit von TrutzMail und TrutzChat (für TrutzMeeting muss nur der Einladende eine TrutzMail-Adresse besitzen, die anderen Teilnehmer nicht). Das Servicepaket beinhaltet:

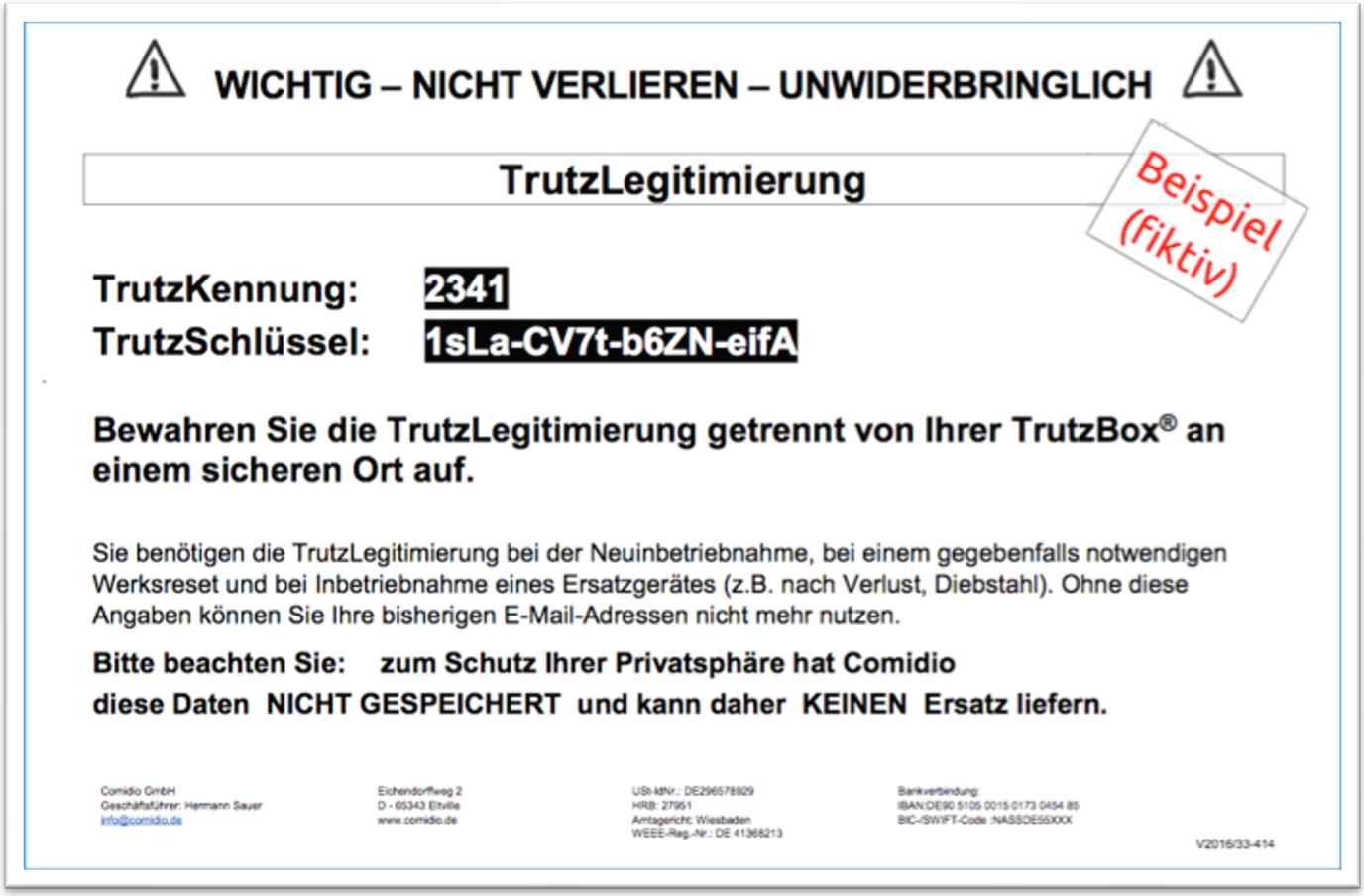
- je nach Servicepaket (TrutzBox-Home oder TrutzBox-Business) ein Kontingent von TrutzMail Accounts pro TrutzBox, für eine Laufzeit von 12 Monaten.
- Online-Support per TrutzBox-Forum oder per E-Mail für TrutzBox-Home- und zusätzlichen Installations-Support per Telefon für TrutzBox-Business-Kunden.
- Regelmäßige Updates für
- Updates der Empfänger-Zertifikate – damit werden abgelaufene oder kompromittierte Zertifikate anderer TrutzMail Accounts Ihrer TrutzBox bekannt gemacht.
- TrutzBox Software-Fehlerbeseitigungen,
- Sicherheits-Updates und
- kleinere funktionelle Erweiterungen
- TrutzContent: Updates für Filterlisten
- TrutzBrowse: Updates für Header-Ergänzungen, Standard-Slider-Einstellungen und TrutzBrowse-Blacklists

Der Kunde kann dieses Servicepaket nach Ablauf von 12 Monaten um jeweils 12 Monate verlängern. Jeweils 30 Tage und 10 Tage vor Ablauf des Service-Vertrags erhält der Kunde eine Erinnerungs-E-Mail an die im trutzbox.de Account hinterlegte Adresse, mit der Bitte, seinen Vertrag um weitere 12 Monate zu verlängern. Falls der Service Vertrag ausgelaufen ist, wird im TrutzBox UserInterface eine Meldung aktiv, die darauf hinweist, dass die TrutzBox sich in einem nicht aktualisierten Status (ohne Sicherheits- und Funktionsupdates) befindet.
Das Servicepaket ist an den Kauf einer TrutzBox gebunden. Der Kunde kann somit für jede gekaufte TrutzBox individuell entscheiden, ob er weitere TrutzMail Accounts erwerben und ob er diese Services um weitere 12 Monate verlängern möchte. Ansonsten lässt er den Service einfach auslaufen.

Die TrutzBox-Hardware geht mit dem Kauf der TrutzBox an den Kunden über. Der Kunde kann auch ohne Vertragsverlängerung die TrutzBox mit einigen Funktionen weiter nutzen, jedoch ohne die sichere E-Mail Funktion und Services, wie TrutzRTC, die an die E-Mail-Adresse gebunden sind.

Die TrutzLegitimierung aus Anwendungssicht

Beim Kauf einer TrutzBox registriert sich der Kunde im Comidio Shop mit seiner schon vorhandenen, normalen (nicht sicheren) E-Mail Adresse. Nach Bezahlung erhält er die TrutzBox, inkl. einer TrutzBox Kennung (TrutzKennung) und eines Passworts (TrutzSchlüssel). Die Kombination aus TrutzKennung und TrutzSchlüssel bildet die TrutzLegitimierung. Der TrutzSchlüssel wird bei Comidio nicht gespeichert und kann nach Verlust auch nicht wieder hergestellt werden.



(© 2016 Comidio GmbH)

Nur mit dieser TrutzLegitimierung kann der Kunde seine TrutzBox in Betrieb nehmen. Danach werden alle TrutzMail Zertifikate indirekt mit dieser TrutzLegitimierung signiert; d.h. TrutzMail Adressen sind an eine TrutzLegitimierung gebunden. Die TrutzLegitimierung muss gut verwahrt werden, da nur so bei Austausch der Hardware oder nach Zurücksetzen der TrutzBox auf Auslieferungszustand, die bereits registrierten TrutzMail Accounts reaktiviert werden können. Wenn ein TrutzBox-Besitzer seine TrutzBox-Hardware verkauft, darf die TrutzLegitimierung nicht weitergeben werden, da der neue Eigentümer mit dieser TrutzLegitimierung die E-Mail Identität des Verkäufers annehmen könnte.

Durch Bindung der TrutzMail Identitäten an die TrutzLegitimierung (und nicht an die TrutzBox Hardware) kann Comidio alle zukünftigen Anwendungsfälle (Use-Cases) mit der erforderlichen Sicherheit abdecken:

- TrutzBox verkaufen,
- TrutzBox verlieren,
- Austausch defekter TrutzBoxen; und das mit oder ohne des TrutzBox Speichermediums (z.B. SD-Karte oder SSD-Platte),
- mehrere TrutzBoxen kaufen und Dritten zur Verfügung stellen,
- Wiedereinrichtung bereits vergebener TrutzMail Accounts auf der gleichen TrutzBox,
- TrutzBox auf Auslieferungszustand zurücksetzen,
- TrutzBox Nutzerdaten sichern und wieder zurück speichen.

Die TrutzLegitimierung ist vergleichbar mit einem Fahrzeugbrief, der den Eigentümer eines Fahrzeugs ausweist. Diese TrutzLegitimierung wird nicht bei Comidio gespeichert und kann bei Verlust auch nicht wiederhergestellt werden. Bei Verlust kann von Comidio nur eine neue TrutzLegitimierung für den gekauften Service generiert werden. Das hat für den Eigentümer allerdings zur Folge, dass er mit dieser neuen TrutzLegitimierung seine TrutzBox zwar wieder betreiben, aber aus Sicherheitsgründen seine alten TrutzMail Adressen nicht mehr nutzen kann. Deshalb ist es unbedingt erforderlich, dass der Kunde die TrutzLegitimierung sicher verwahrt.
Wer die TrutzLegitimierung hat, kann bei Diebstahl die damit bereits registrierten TrutzMail Accounts aufsetzen und die TrutzMail Identität z.B. des Bestohlenen übernehmen. Verlust des TrutzZertifikats, sollte Comidio sofort gemeldet werden, damit Comidio alle damit ausgestellten TrutzMail Accounts für „ungültig“ erklären kann. Durch den TrutzMail Blacklist-Update werden dann allen TrutzBoxen, die dieses Zertifikat haben, die Kompromittierung mitgeteilt.
Somit hat Comidio dafür gesorgt, dass die TrutzBox die komplette Zertifikats- und Key-Verwaltung für den Anwender übernimmt. Weitere Details dazu sind im Kapitel TrutzMail beschrieben.
Loggt sich ein Kunde in seinem Account bei trutzbox.de ein, wird ihm eine Übersicht seines Comidio Accounts angezeigt. Er kann sehen, in wieweit sein TrutzMail Kontingent ausgeschöpft ist, kann weitere TrutzMail Account-Kontingente kaufen, oder die Laufzeit seiner Kontingente und seines Servicepakets um weitere 12 Monate verlängern.

Die TrutzLegitimierung aus System-Sicht

Die TrutzLegitimierung bekommt jeder Kunde pro TrutzBox einmal ausgedruckt und in dem TrutzBox Paket mitgeliefert. Sie wird zentral von Comidio kurz vor Auslieferung einer bestellten und bezahlten TrutzBox generiert. Sie beinhaltet die TrutzKennung und den zugehörigen TrutzSchlüssel. Beides muss der Kunde sowohl bei der erstmaligen Inbetriebnahme der TrutzBox als auch nach einem Reset auf Werkseinstellung eingeben. Mittels TrutzLegitimierung identifiziert er sich als „Besitzer“ eines TrutzBox Service-Abos, und sie gibt ihm das Anrecht auf die TrutzServices (Mail und Updates). Bei der Auslieferung der TrutzBox Hardware ist die TrutzLegitimierung der TrutzBox Hardware noch nicht zugeordnet.

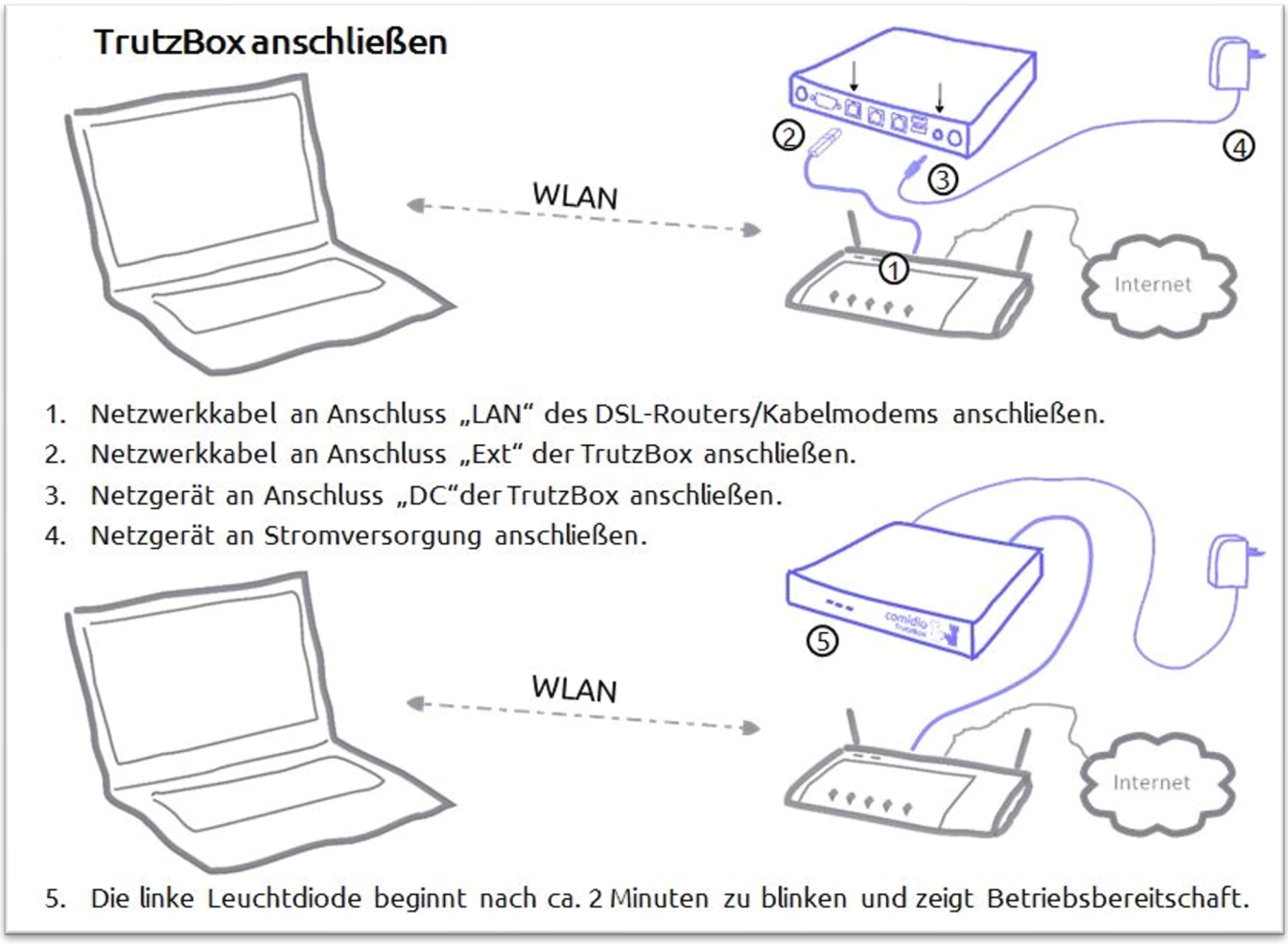
Erst bei der Inbetriebnahme der TrutzBox durch den Kunden wird die TrutzLegitimierung mit der TrutzBox Hardware verknüpft (genauer gesagt mit der SSD-Platte, auf der alle Daten gespeichert sind). Während des Betriebs der TrutzBox wird dann überprüft, welche TrutzServices der Kunde nach aktueller Abo-Situation bekommt. Da ein Abo anfangs immer 12 Monate läuft und danach jeweils um 12 Monate verlängert werden kann, wird damit auch das Ablaufdatum (Expire-Date) der TrutzMails und Updates gesteuert. Die TrutzServices (Mail und Updates) sind somit immer mit der TrutzLegitimierung verknüpft.
TrutzMail Adressen sind somit an die TrutzLegitimierung und an die TrutzBox Hardware (SSD-Karte) gebunden, die mit dieser TrutzLegitimierung in Betrieb genommen wurde. Alle TrutzMails, die mit einer bestimmten TrutzLegitimierung erstmalig registriert wurden, können mit der gleichen TrutzLegitimierung jederzeit auf einer beliebigen TrutzBox Hardware nachträglich wieder angelegt werden. Wenn die TrutzLegitimierung einem Dritten in die Hände fällt, kann dieser die E-Mail Identität seines rechtmäßigen Besitzers übernehmen. Somit ist die TrutzLegitimierung unbedingt sicher und vor unberechtigtem Zugriff zu verwahren!
Mit seiner TrutzLegitimierung kann der Kunde jederzeit eine beliebige TrutzBox Hardware in Betrieb nehmen. Somit kann Comidio eine defekte TrutzBox Hardware (genauer gesagt seine SSD-Platte) austauschen, da der Kunde mit Hilfe dieser TrutzLegitimierung die neue TrutzBox Hardware, mit seinen registrierten TrutzMail Adressen, wieder in Betrieb nehmen kann.
Damit kann sicher gestellt werden, dass alle privaten Schlüssel und Passwörter nur auf der TrutzBox gespeichert sind und bei Verlust wieder neu generiert bzw. wieder hergestellt werden können.
Der Kunde kann auch seine TrutzBox-Hardware nach Rücksetzung auf Auslieferungsstand ohne Risiko verkaufen, und der Käufer kann diese gebrauchte TrutzBox Hardware nutzen, indem er diese mit seiner eigenen TrutzLegitimierung in Betrieb nimmt.
Comidio speichert die TrutzLegitimierung aus Sicherheitsgründen nicht. Falls der Kunde seine TrutzLegitimierung verliert, kann diese nicht wieder hergestellt werden. Er kann somit seine TrutzBox mit seinen registrierten TrutzMails nicht mehr neu einrichten. Er verliert das Recht auf seine schon registrierten TrutzMailAdressen und Services. Der Kunde sollte bei Verlust der TrutzLegitimierung Comidio kontaktieren, um ein neues TrutzService Abo erwerben zu können (ist nur nach Rücksprache mit Comidio im Shop erhältlich).

TrutzBox Setup

Die TrutzBox kann von jedem, ohne spezielle technische Kenntnisse, in Betrieb genommen werden. Aus diesem Grund wurde bei der Architektur der TrutzBox sehr viel Wert auf eine einfache Setup-Funktion gelegt. Da die TrutzBox speziellen Sicherheitskriterien genügen muss, ist es leider nicht möglich, die TrutzBox nur durch einfaches Verkabeln in Betrieb zu nehmen. Die Inbetriebnahme besteht aus drei Schritten:

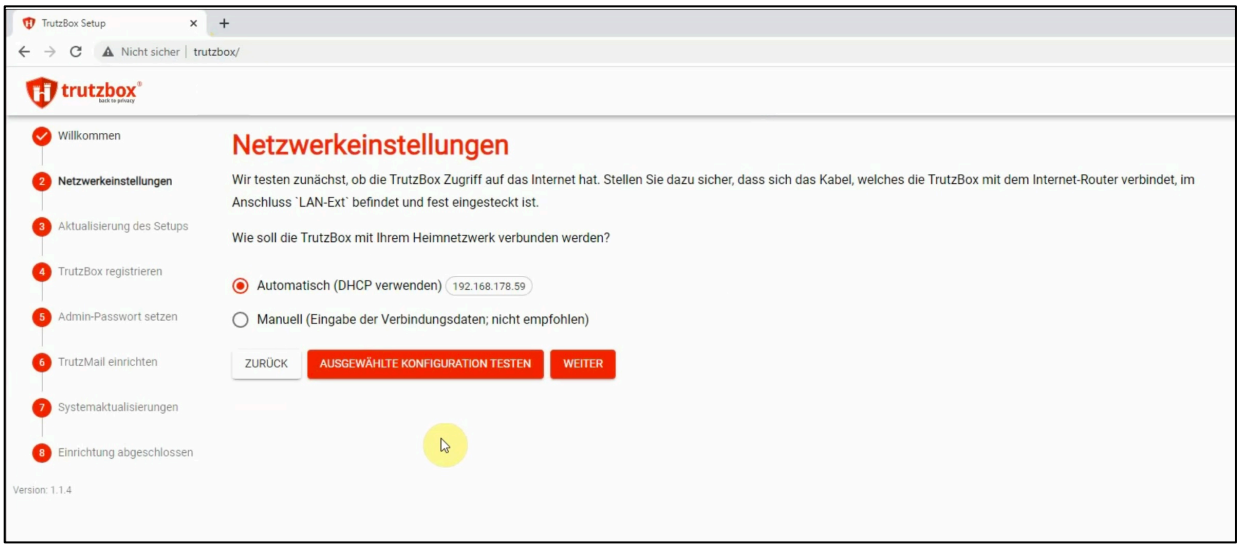
Schritt 1: Verkabelung

Die Verkabelung ist recht einfach, da die TrutzBox lediglich mit einem mitgelieferten LAN-Kabel an den Internet-Router angeschlossen werden muss.



Schritt 2: TrutzBox Setup

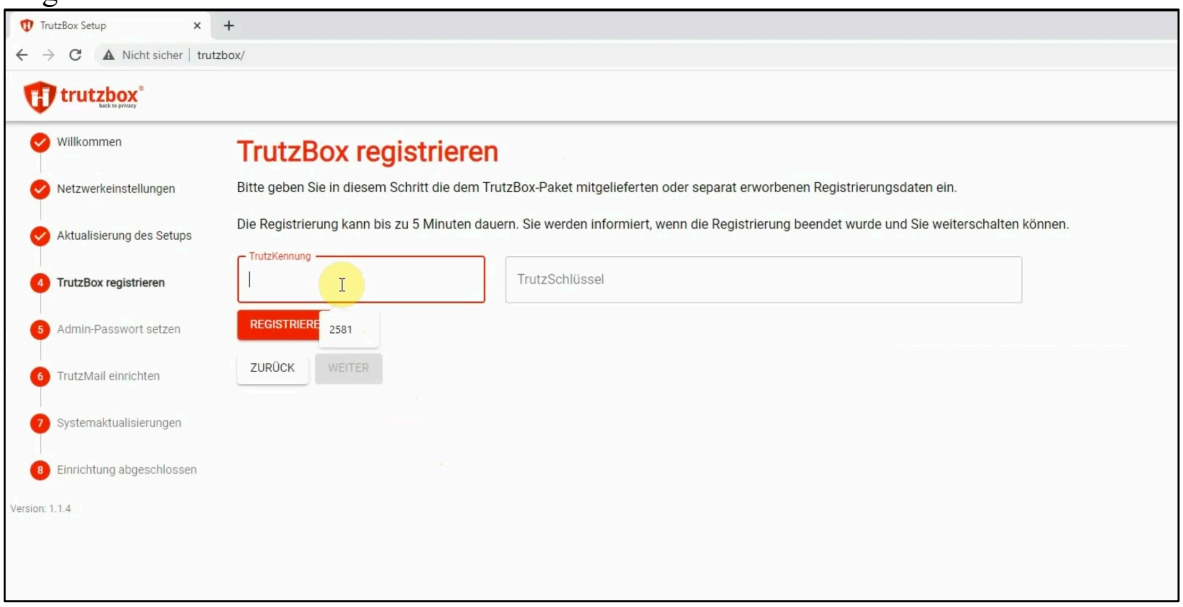
Die Einrichtung der TrutzBox (Setup) kann nun über einen PC ausgeführt werden, der am Internet-Router angeschlossenen sein muss. Dazu wird am PC ein Browser gestartet. Durch die Eingabe des Links http://trutzbox/ gelangt man in das Setup-Menü der TrutzBox.
Nach kurzem Begrüßungstext und Bestätigung der Lizenzbedingungen, prüft die TrutzBox, ob es mittlerweile ein neues Setup-Programm gibt. Wenn ja, wird das neue Setup-Programm automatisch geladen. Danach prüft die TrutzBox ob sie Zugriff auf das Internet hat. Hier kann auch eingestellt werden, ob die TrutzBox die IP-Adresse automatisch bezieht (DHCP) oder man eine eigene feste IP-Adresse einstellen möchte (eine feste IP-Adresse wird nicht empfohlen).



(© 2023 Comidio GmbH)

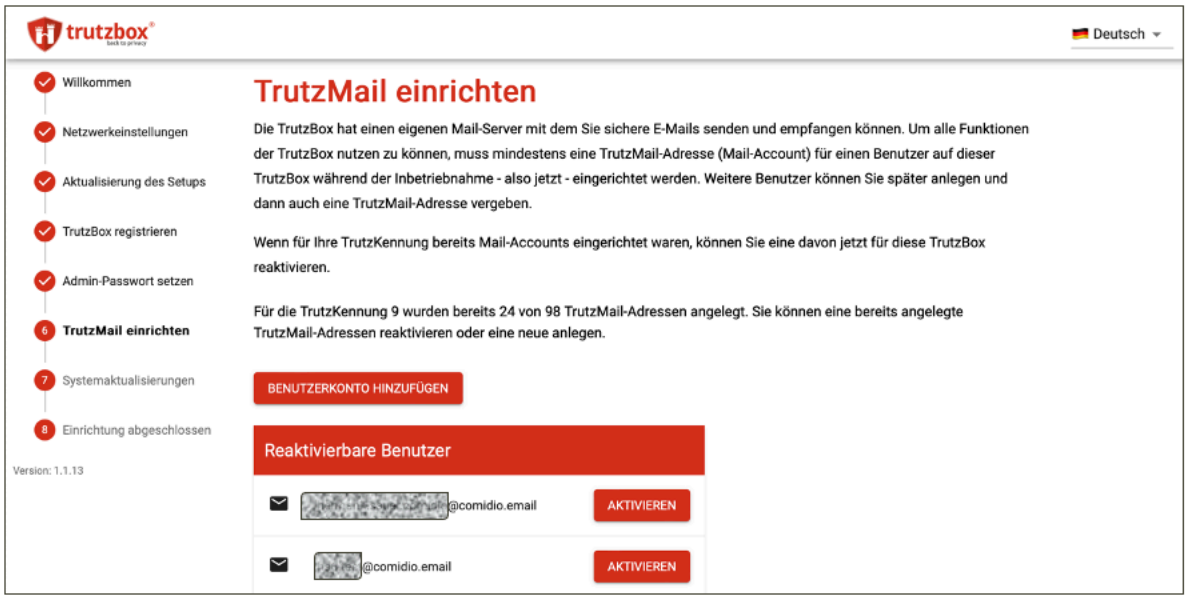
Falls der Internet-Zugriff misslingt, sollte die Verkabelung oder Netzwerk-Einstellung des Internet-Routers überprüft werden.

Als nächstes muss die TrutzBox registriert werden. Dazu muss die mitgelieferte TrutzBox-Legitmation eingeben werden.



(© 2023 Comidio GmbH)

Nach dem Setzen eines Admin-Passworts, wird mindestens ein TrutzMail-Account auf der TrutzBox eingerichtet. Dazu kann man einen zuvor registrierten TrutzMail-Account reaktivieren, oder einen neuen TrutzMail-Account anlegen.



(© 2023 Comidio GmbH)

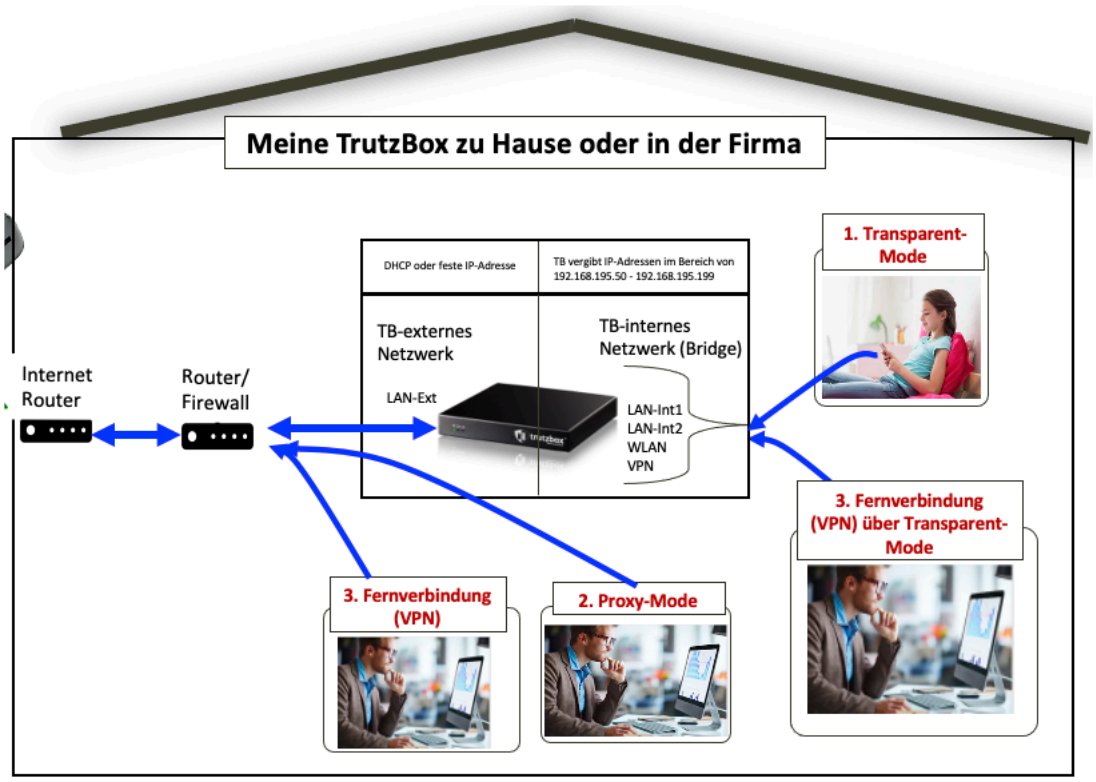
Nachdem das Setup noch updates der TrutzBox einspielt ist das Setup abgeschlossen.

Mit erneutem Aufruf von http://trutzbox/ kann nun die Administrator-Oberfläche der TrutzBox aufgerufen werden. In seltenen Fällen ist es notwendig, den Browser-Cache zuvor zu löschen.

Schritt 3: Benutzer Devices an der TrutzBox anschließen

Es gibt drei Möglichkeiten, ein Gerät (z.B. PC, mobiles Gerät, Fernseher ...) an die TrutzBox anzuschließen:

1. im Transparent-Mode . Dabei wird das Gerät direkt an das interne Netzwerk der TrutzBox angeschlossen. Das kann per Lan-Anschluss (RJ45) oder mit dem optional erhältlichen WLAN-Modul geschehen
2. über einen Proxy-Eintrag im Browser des Geräts oder in den Netzwerk-Einstellungen des Geräts
3. Oder über eine VPN-Verbindung zur TrutzBox. Diese Möglichkeit empfehlen wir vor allem für mobile Geräte (Smartphone oder Laptop), da dann die TrutzBox auch unterwegs genutzt werden kann..



(© 2020 Comidio GmbH)

Für jedes Gerät kann individuell entschieden werden, über welche Anschlussmöglichkeiten das Gerät die TrutzBrowse und TrutzContent Funktionen der TrutzBox nutzen soll. Um erste Erfahrungen mit der TrutzBox zu sammeln empfiehlt Comidio zunächst nur ein Gerät an die TrutzBox anzuschließen.

Möglichkeit 1: Internet Device wird an TrutzBox Netzwerk angeschlossen (Transparent-Mode)

Bei Nutzung des Jugendschutzes sollte man für diese Geräte unbedingt diesen Transparentmode nutzen, da es in den anderen Anschluss-Alternativen mit etwas technischem Know How möglich ist, die Konfiguration im Endgerät wieder zu ändern und somit den Jugendschutz der TrutzBox zu umgehen.
Um Geräte im Transparent-Mode an die TrutzBox anzuschliessen, werden die Geräte netzwerkmäßig direkt per WLAN (optional bestellbar) oder LAN-Kabel an der TrutzBox angeschlossen. In diesem Fall sollte kein Proxy in dem Endgerät konfiguriert sein. Es brauchen in diesem Fall keine Einstellungen auf dem Endgerät vorgenommen werden. Da in diesem Betriebs-Modus die gesamte Datenkommunikation über die TrutzBox geleitet wird, ist weder der Benutzer noch eine Applikation in der Lage, sich der Kontrolle der TrutzBox zu entziehen.
Beim Anschluss per LAN-Kabel wird eines der beiden freien LAN-Int-Anschlüsse (LAN-Intern) an der TrutzBox genutzt. Sollen mehr als zwei Geräte per LAN-Kabel angeschlossen werden, können die Anschlüsse durch einen zusätzlichen Hub, Switch oder Router erweitert werden (nicht im Lieferumfang enthalten).
Geräte, die direkt per Netzwerk an die TrutzBox angeschlossen sind, werden im TrutzBox Administrator-Menü mit der Endung .sec aufgeführt.
Sollen alle ihre Geräte die TrutzBox nutzen, könnte das WLAN des Internet-Routers sogar abgeschaltet werden.

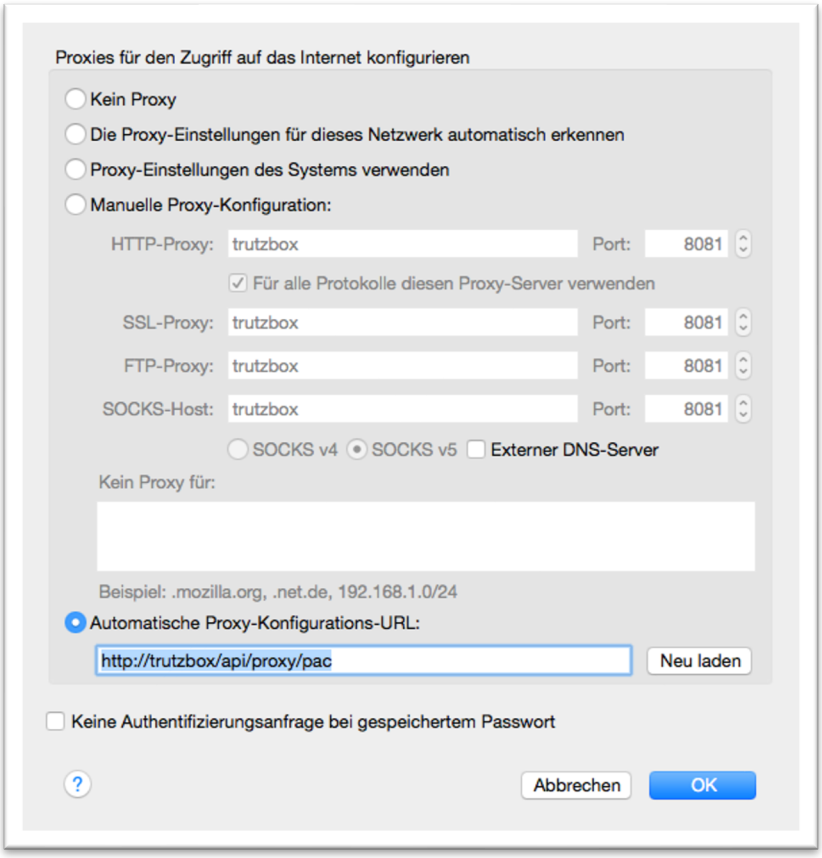
Details zu diesen Einstellungen sind dem TrutzBox Handbuch zu entnehmen.

Möglichkeit 2: Internet Device bleibt am angeschlossenen Internet-Router angeschlossen (Proxy-Mode)

Wir empfehlen zunächst nichts am vorhandenen internen Netzwerk zu ändern und erste Erfahrungen mit dieser Konfiguration zu sammeln. Damit der Netzwerk-Verkehr per Proxy-Eintrag über die TrutzBox geleitet wird, gibt es zwei Wege zu unterscheiden:

- **in Firefox die TrutzBox als Proxy eintragen.** Dann geht nur der Firefox-Browser über die TrutzBox, andere Programme gehen weiter ungehindert ins Internet. Diese Möglichkeit bietet nur der Firefox-Browser
- **in den Netzwerk-Einstellung des Endgeräts die TrutzBox als Proxy eintragen**. Dann geht der gesamte Netzwerk-Verkehr, der über dieses Netzwerk läuft durch die TrutzBox. Das entspricht so ziemlich dem Transparent-Mode. Das geht bei allen Betriebssystemen, inkl. iOS, macOS, Linux, Windows, Android und auch bei vielen, aber nicht allen IoT-Geräten (Fernseher, Video-Überwachungskamera, Heizungsregler..).

Um einen Proxy in Firefox oder im Netzwerk einzutragen, wird im Browser unter Netzwerkeinstellungen, Proxy-Einstellung entweder für alle Netzwerke der Proxy „trutzbox“ mit der Portnummer 8081 eingetragen oder dort unter automatische-Proxy-Konfiguration das PAC-Script http://trutzbox/api/proxy/pac eingetragen.
Hier die Einstellung für Firefox:



Möglichkeit 3: Internet Device per VPN (Fernverbindung) mit der TrutzBox verbinden

Für mobile Geräte empfehlen wir diese Alternative. Sie hat den Vorteil, dass die TrutzBox sowohl aus dem eigenen Netzwerk heraus, als auch unterwegs genutzt werden kann.
Dazu muss zunächst auf der TrutzBox im Menü „Netzwerk“ -> „Fernzugriff“ der VPN-Server aktiviert werden. Danach muss man ca 15min warten bis sich der VPN-Server initialisiert und dann kann in der Benutzereinstellung der TrutzBox ein Benutzer für den VPN-Zugriff aktiviert werden. Dadurch wird eine Konfigurationsdatei erzeugt, die im VPN-Client auf dem Endgerät in die VPN-App importiert werden muss. Für den Fernzugriff ist zudem notwendig, dass der Port 1194 (UDP) von Ihrem Router zur TrutzBox weitergeleitet wird.

Für alle drei Fälle gibt es eine ausführliche Beschreibung in unserem Online-Handbuch: https://wiki.trutzbox.de/view/TrutzBox_Handbuch
Der Vorteil von Alternative 2und 3 ist, dass man im Gegensatz zu Alternative 1, einfach auch mal mit einem Schalter die TrutzBox umgehen kann. Das könnte gelegentlich hilfreich sein, falls die TrutzBox in ihrer Standard-Einstellung zu viel filtert und es dadurch Probleme mit einer Anwendung gibt. Natürlich kann man solche Probleme einer Anwendung auch durch Anpassung der Filter in der TrutzBox lösen.

TrutzBox Zertifikate

Um den Betrieb der TrutzBox und den Austausch von TrutzMails abzusichern, generiert die TrutzBox mehrere digitale Zertifikate. Dies geschieht ohne Eingriff des Benutzers.
Hier die wichtigsten Zertifikate:

- 1. Ein **TrutzMail Zertifikat** pro TrutzMail Adresse. Es bestätigt die Echtheit der TrutzMail Adressen und dient dazu, die Absender zu authentifizieren. Es wird von Comidio zertifiziert. Falls beim Senden einer TrutzMail, das TrutzMail Zertifikat des Empfängers noch nicht bekannt ist, wird es vom zentralen Comidio Zertifikat-Server geholt (PGP-Keyring: /var/lib/comidio/trutzmail/openpgp/). Das TrutzMail Zertifikat enthält
- den öffentlichen 2048 RSA Schlüssel (Public Key) des Empfängers, mit dem der Sender die E-Mail automatisch verschlüsselt.
- die Tor-Hidden-Service Adresse (onion-Adresse), um Mails an die Empfänger-TrutzBox ausliefern zu können.
- Dieses TrutzMail Zertifikat wird auch für die TrutzBox zur TrutzBox Kommunikation zwischen XMPP-Servern verwendet.

- 2. **Ein TrutzBox Zertifikat** pro TrutzBox, das zur Authentifizierung gegenüber Comidio z.B. bei der Registrierung von neuen Mail-Accounts auf der TrutzBox dient. Es wird beim Setup der TrutzBox einmalig auf der TrutzBox generiert. Die Laufzeit dieses Zertifikats beträgt ca. 10 Jahre und wird nach Ablauf dieser Zeit automatisch neu erstellt.
- /etc/comidio/boxCert.pem): TrutzBox Zertifikat (X509: Signature Algorithm: sha256WithRSAEncryption, = SHA2), PublicKey: RSA 4096Bit
- /etc/comidio/box.Key.pem: TrutzBox Private Key (4096 Bit RSA-Key)

- 3. Ein **Mail-/Web-Server-TLS-Zertifikat** pro TrutzBox (für https://trutzbox/, und SMTPs IMPAs). Dieses Zertifikat wird mit 4. (Proxy-CA-Zertifikat) signiert. Es dient dazu, die TrutzBox gegenüber eines Nutzers (Web-Browser, Mail-Client, XMPP-Client, ...) zu authentisieren. Es liegt unter /etc/comidio/webCert.pem bzw. unter /usr/share/ca-certificates/comidio/comidio_email.crt.

- 4. Ein **Proxy-CA-Zertifikat** pro TrutzBox. Dieses Zertifikat dient dazu, die bei TrutzBrowse dynamisch generierten SSL Zertifikaten, die TrutzBrowse pro aufgerufener SSL Verbindung generiert, zu signieren. Dieses Zertifikat sollte im Web-Browser und Betriebssystem importiert werden, damit diese die Authentizität des Web-, XMPP-Chat- und Mail-Servers auf der TrutzBox überprüfen können. Es liegt unter /etc/comidio/proxyCA.crt.

- 5. Ein Zertifikat für die **Authentisierung des Jitsi-Servers** (TrutzRTC Video-Konferenz-Servers). Dies muss ein eigenes, von den anderen vier Zertifikaten unabhängiges Zertifikat sein, da es nicht auf den Hostnamen „trutzbox“ ausgestellt werden darf. Wenn es auf den Hostnamen „trutzbox“ ausgestellt wäre, dann könnten sich andere TrutzBox Besitzer, die schon ein Stamm-Zertifikat ihrer eigenen TrutzBox in ihren Browser geladen haben, nicht

mit einer fremden TrutzBox verbinden. Der Browser würde das Zertifikat ohne nachzufragen ablehnen, da der Browser erfolglos versuchen würde, die Gültigkeit mit diesem eigenen TrutzBox Stamm-Zertifikat zu bestätigen.

- 6. Ein Zertifikat für den Fernzugriff (VPN-Server auf der TrutzBox). Dies wird erst dann generiert, wenn auf der TrutzBox der Fernzugriff aktiviert wird.
- 7. Ein Zertifikat pro TrutzBox-Account bzw. TrutzMail-Adresse, für die der Fernzugriff aktiviert wurde. Dieses Zertifikat beinhaltet einen Schlüssel dessen cipher auf "AES-256-CBC“ basiert. Das Zertifikat befindet sich in der .ovpn Datei (Open-VPN-Konfigurations-Datei) die dem Nutzer per TrutzMail zugeschickt wird.
- 8. Ein im Internet bekanntes, offizelles LetsEncrypt-Zertifikat. Dieses kann im Menü „Fernzugriff“ oder auch im Menü „Videokonferenz“ für den vom Internet aus erreichbaren Domän-Namen (TrutzDynDNS) der TrutzBox generiert werden. Dieses Zertifikat ist notwendig, falls die TrutzBox vom Internet aus erreichbar sein soll. Z.B. bei der Nutzung des Videokonferenz-Servers auf der TrutzBox.

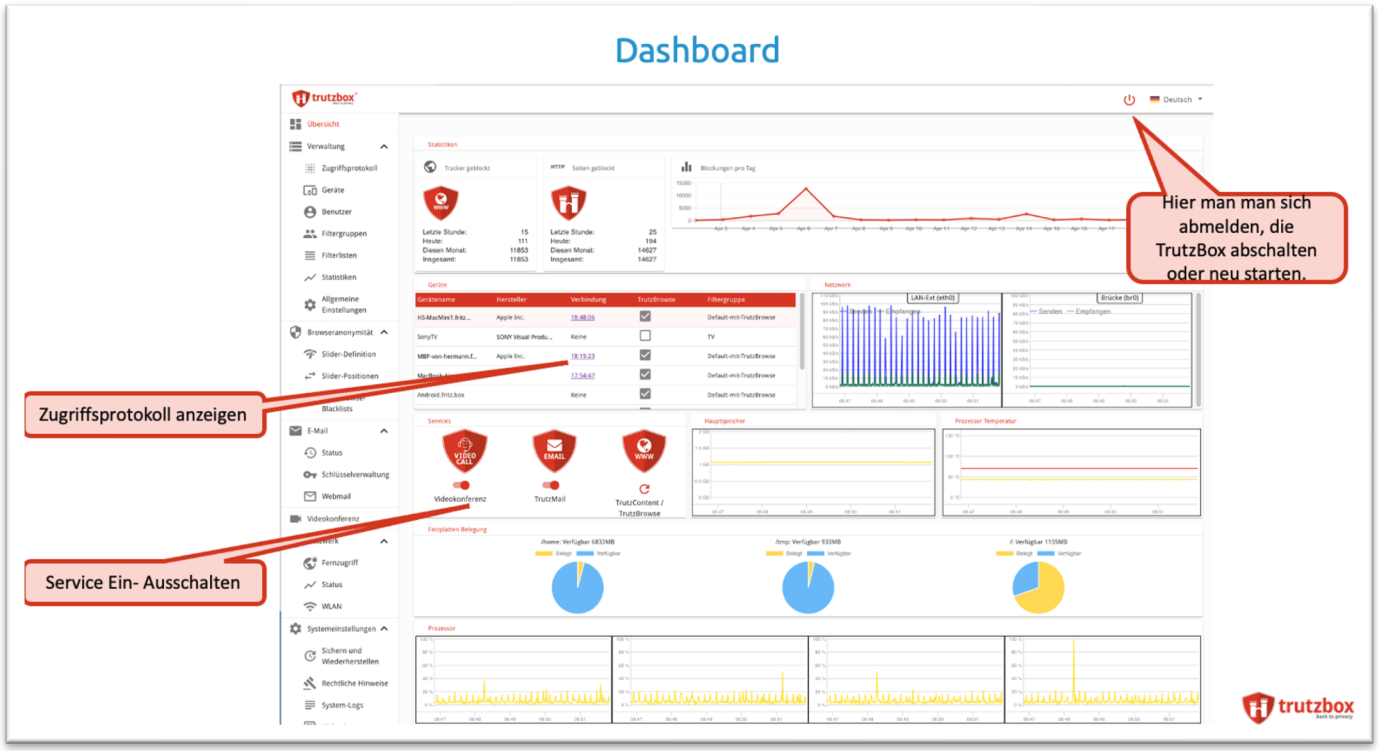
Falls die TrutzBox von Comidio ausgetauscht oder vom Anwender auf Werksauslieferungsstand zurückgesetzt wird, werden alle Daten auf der TrutzBox gelöscht. Somit werden auch alle Zertifikate auf der TrutzBox gelöscht und beim erneuten Setup der TrutzBox neu generiert. Die Schlüssel in den Zertifikaten werden dadurch ebenfalls erneuert.

TrutzBox Administrator Oberfläche

Die TrutzBox Administrator Oberfläche wird im Browser mit http://trutzbox/ aufgerufen. Hier werden alle administrativen Einstellungen der TrutzBox durchgeführt. In diesem Kapitel werden wir lediglich auf die wichtigsten Funktionen eingehen. Eine genaue Beschreibung kann man online im TrutzBox-Handbuch finden.

Übersicht

Nachdem die TrutzBox-Oberfläche aufgerufen wurde, wird die TrutzBox Übersicht bzw Dashboard angezeigt.



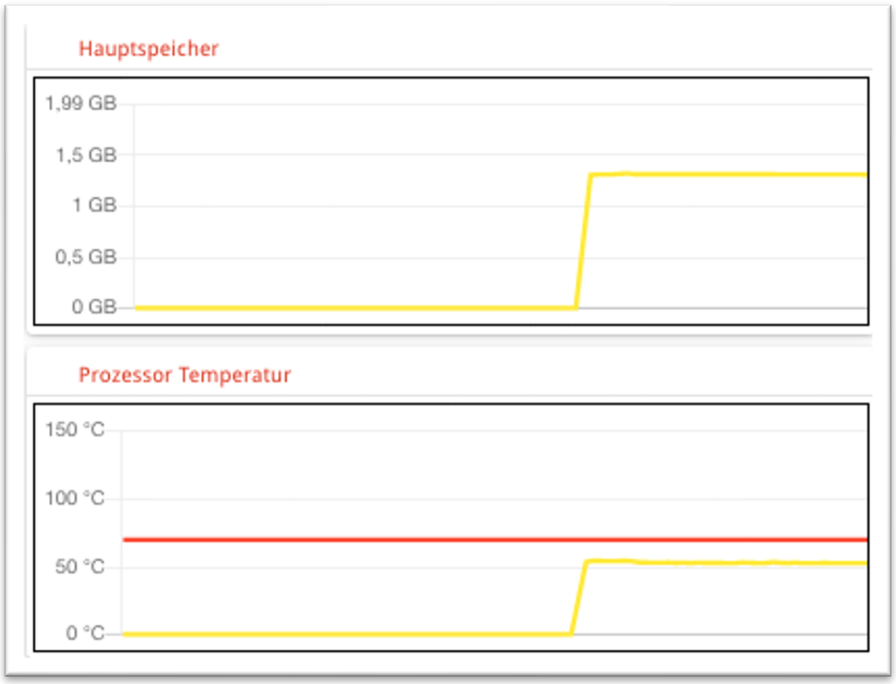
(© 2020 Comidio GmbH)

Dort werden folgende Daten angezeigt:

- eine Zusammenfassung der statistisch erhobenen Blocking-Daten von TrutzBrowse (Tracker geblockt) und TrutzContent (Seiten geblockt), sowie die geblockten Tracker pro Tag.
- Eine Übersicht aller Geräte, die mit der TrutzBox verbunden sind oder waren. Falls noch Verbindungsdaten verfügbar sind, wird unter „Verbindung“ die Zeit der neuesten Verbindungsdaten angezeigt. Mit Klick auf diese Zeit wird das vorhandene Zugriffsprotokoll des Geräts angezeigt.
- Eine Übersicht des aktuellen Netzwerk-Verkehrs. „LAN-Ext“ ist der unsichere externe LAN-Anschluss, in der „Brücke“ sind alle Daten der internen Netzwerkanschlüsse zusammengefasst (LAN-Int1, LAN-Int2 und falls vorhanden das eingebaute WLAN).

- Status der TrutzBox-Services (rotes Symbol bedeutet: Service ist aktiv, graues Symbol bedeutet: Service ist nicht aktiv):
  - Videokonferenz (TrutzMeeting),
  - Mail (TrutzMail),
  - Proxy (TrutzContent/TrutzBrowse)
- Auslastung der TrutzBox CPUs und Hauptspeicher,
- Hardware-Daten, wie Auslastung des Speichermediums und Temperatur

Dabei bedeuten die Hardware-Daten folgendes:



(© 2024 Comidio GmbH)

Hauptspeicher

- gelbe Linie, aktuell belegter Hauptspeicher
- auf der y-Achse wird der maximal verfügbare Hauptspeicher aufgeführt

Prozessor Temperatur (CPU):

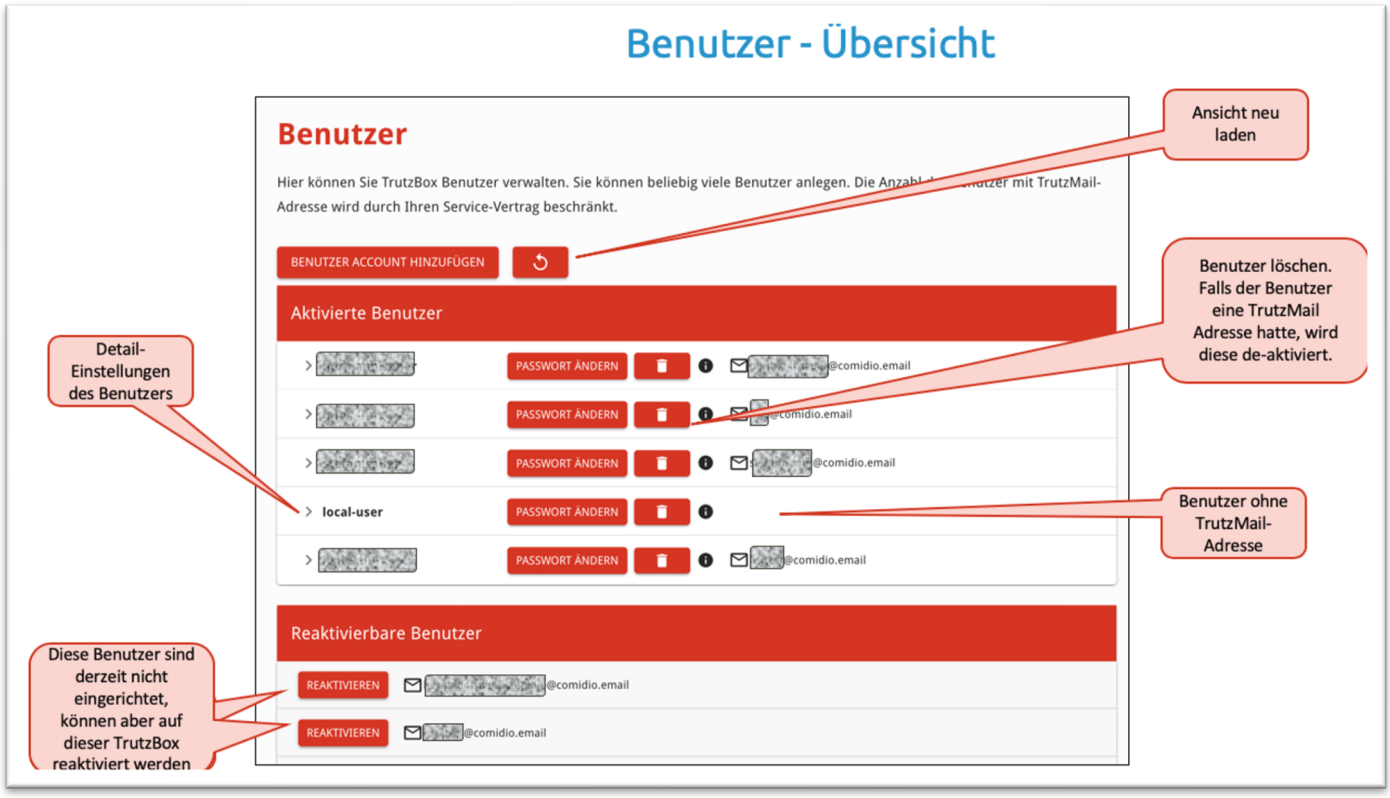
- gelbe Linie, aktuelle Temperatur, hier bei ca. 55 Grad.
- rote Linie, die bisher höchste gemessene Temperatur, hier ca. 70 Grad.
- TrutzBox schaltet sich automatisch bei ca. 105 Grad ab.

Benutzer verwalten

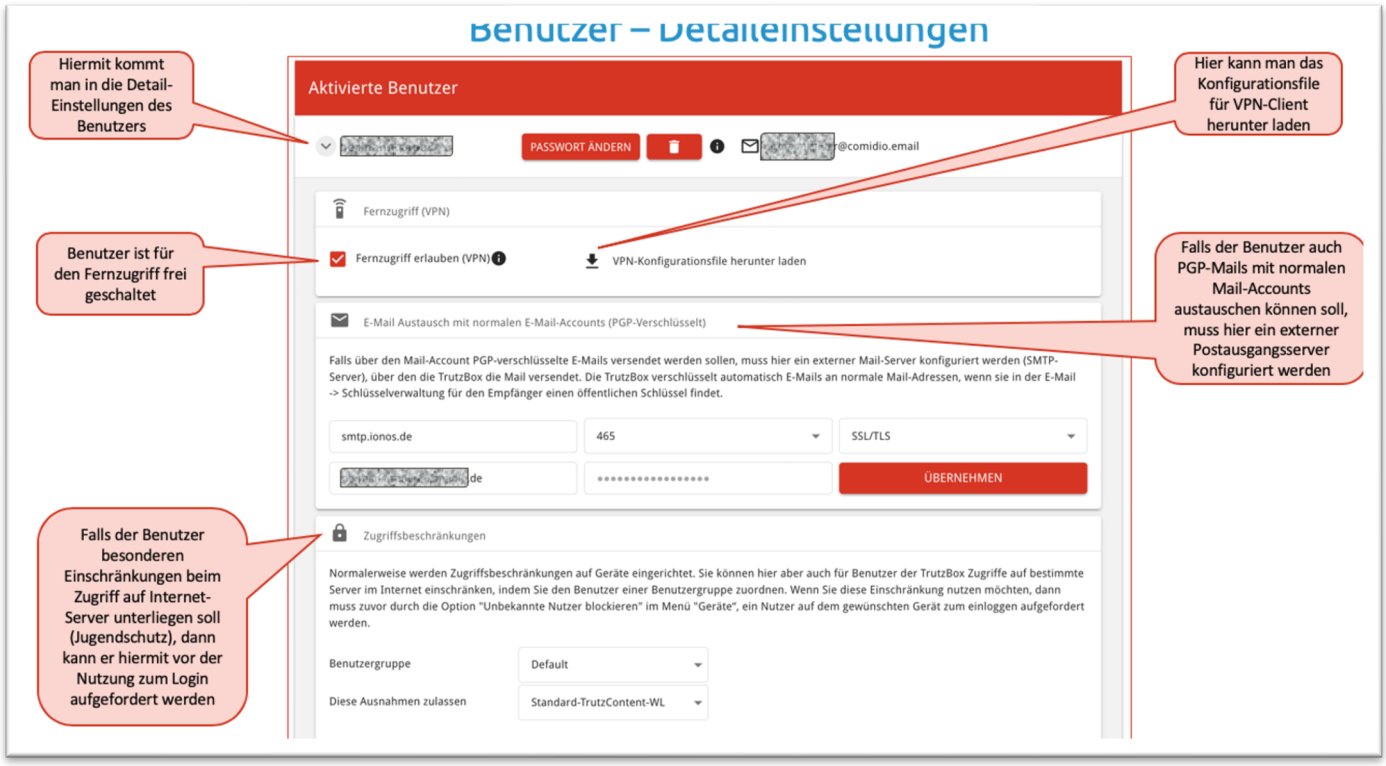
Die TrutzBox hat eine eigene Verwaltung ihrer Benutzer. Es gibt drei Arten von Nutzer-Accounts:

1. den Benutzer „admin“ gibt es nur einmal und wird beim Einrichten (Setup) der TrutzBox angelegt. Dabei vergibt der Einrichter der TrutzBox auch ein sicheres Password für den Benutzer „admin“. Der Benutzer „admin“ hat Administrator-Rechte auf Betriebssystem Ebene und ist für die meisten TrutzBox Services nicht bekannt. Er wird lediglich zum Einloggen auf der TrutzBox-Admin-Oberfläche und in Webmin benötigt. Mit diesem Benutzernamen ist es möglich, sich auch über ein Terminal-Programm auf Betriebssystem Ebene einzuloggen.
2. Ein normaler TrutzBox Benutzer – der keine TrutzMail Adresse hat. Dieser Benutzer kann für TrutzContent-Filter verwendet werden.
3. Ein TrutzBox Benutzer, der auch eine TrutzMail Adresse hat. Diese TrutzMail Adresse kann aktiviert oder deaktiviert sein. Aktive TrutzMail Adressen werden benötigt für
   I. TrutzMails (zwischen TrutzBoxen),
   II. PGP-Mails an nicht-TrutzBox Besitzer,
   III. für Chat und um einen Video-Konferenzraum zu öffnen. Teilnehmer einer Video-Konferenz und TrutzBrowse Nutzer benötigen keine Benutzer-Id auf der TrutzBox.
   IV. Für den Fernzugriff auf die TrutzBox. Der Fernzugriff muss für jeden Benutzer frei geschaltet werden, der sich über das Internet mit der TrutzBox verbinden können soll.

Die Anzahl der TrutzMail Adressen ist durch den Service-Vertrag begrenzt. Da es keine Begrenzung der Anzahl Benutzer **ohne** TrutzMail-Adresse gibt, können beliebig viele lokale Benutzer ohne TrutzMail-Adresse angelegt werden.
TrutzMail Adressen müssen über alle TrutzBoxen hinweg eindeutig sein, was beim Einrichten automatisch geprüft wird. Lokale Nutzernamen müssen lediglich auf der eigenen TrutzBox eindeutig sein.
Benutzer mit einer TrutzMail Adresse können aktiv oder deaktiviert sein. TrutzMail Adressen werden beim Löschen des Benutzers auf der TrutzBox deaktiviert. TrutzMail-Adressen werden automatisch deaktiviert, wenn die TrutzBox nach einem Reset auf Werkseinstellung neu aufgesetzt wird.
Wenn der Service-Vertrag ausläuft und nicht verlängert wird, läuft der Gültigkeitszeitraum des TrutzMail-Zertifikats ab. Dann akzeptiert die Empfänger-TrutzBox die Mail nicht mehr.
Falls der Service-Vertrag es erlaubt, können deaktivierte TrutzMail Adressen in der Benutzerverwaltung der TrutzBox re-aktiviert werden.
Im Menüpunkt „Benutzer“ können weitere Benutzer hinzugefügt, reaktiviert, geändert oder gelöscht werden.



Des Weiteren kann für jede TrutzMail Adresse hier auch ein „Standard Mail Ausgang“ Account konfiguriert werden. Dieser wird benötigt, falls man PGP-Verschlüsselte E-Mails an nicht-TrutzBox Besitzer **verschicken** möchte. Zum **Empfangen** von E-Mails über normale Mail-Server wird dieser Eintrag nicht benötigt.
Mit dem Pfeil links kommt man in die Detail-Einstellung des Benutzers.

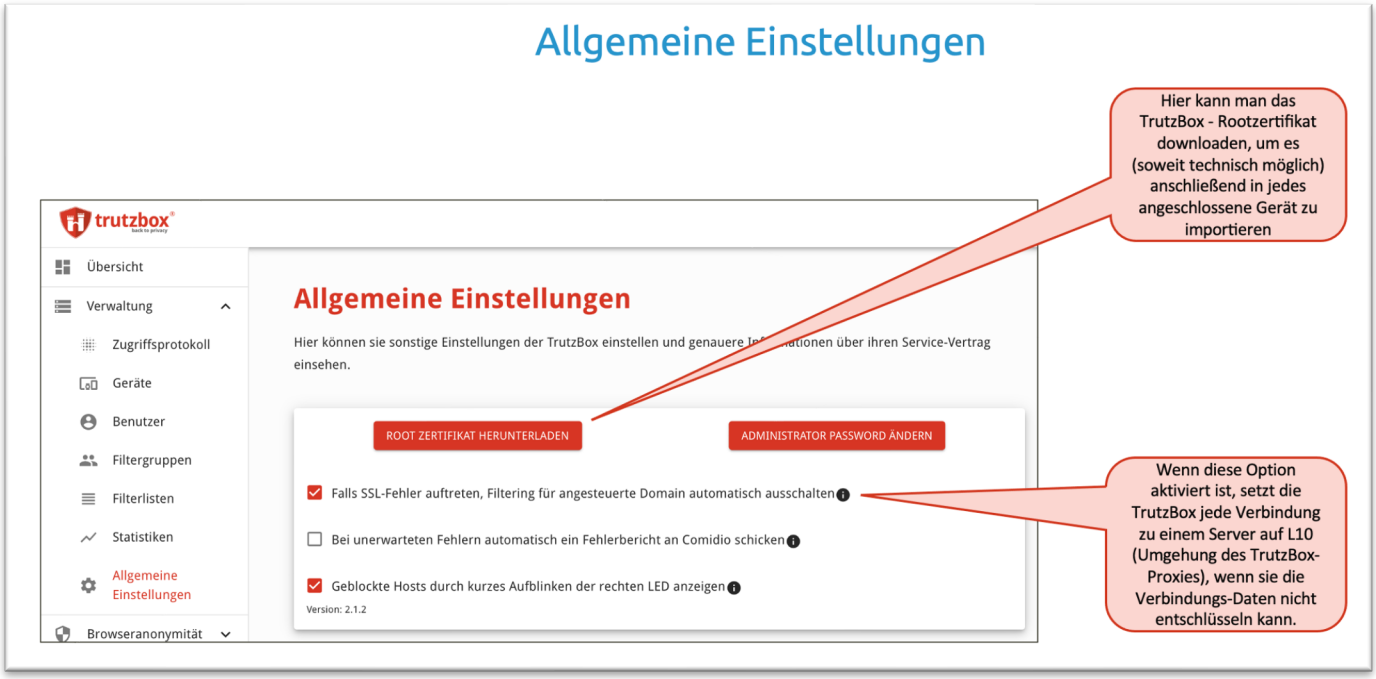


(© 2020 Comidio GmbH)

Allgemeine Einstellungen

Über den Menüpunkt „Allgemeine Einstellungen“ sind allgemeingültige Einstellungen und das Downloaden des TrutzBox-Rootzertifikats möglich. Das TrutzBox-Root-Zertifikat muss auf jedem Endgerät installiert sein, wenn entweder

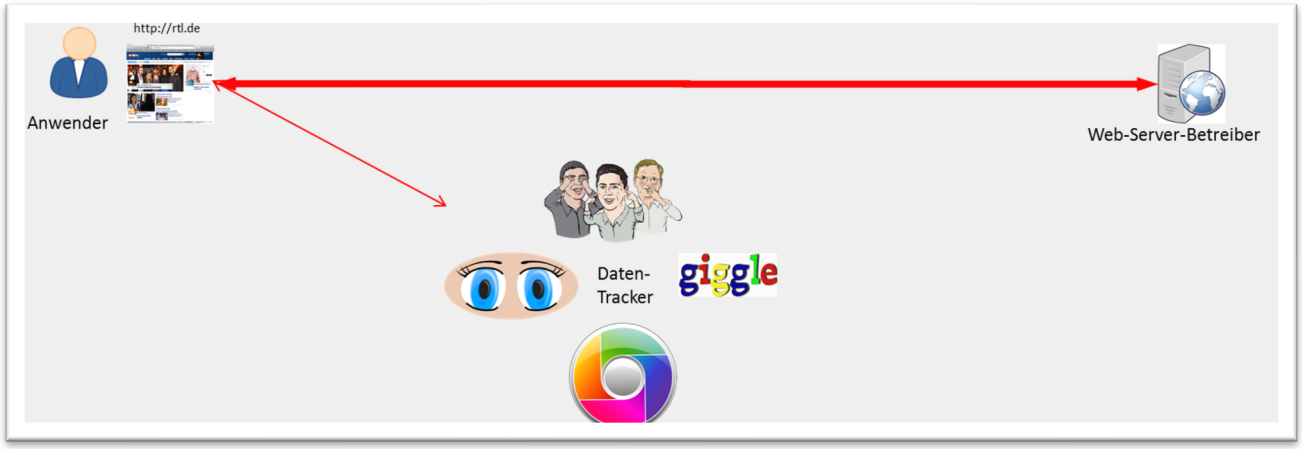
- für dieses Gerät TrutzBrowse aktiviert ist, oder
- über dieses Gerät sicher und verschlüsselt mit einem Mail-Programm auf den Mail-Server der TrutzBox zugegriffen werden soll (TrutzMail)



(© 2020 Comidio GmbH)

TrutzContent/TrutzBrowse – Spurenarmes Nutzen des Internets

Die TrutzBox schützt den Internet-Anwender, indem sie verhindert, dass Angreifer oder Daten-Sammler beim Surfen im Internet an dessen Profildaten kommen. Die TrutzBox, mit ihrer TrutzContent und TrutzBrowse Funktion, ist kein „Werbeblocker“. Allerdings erschwert die TrutzBox, dass Werbefirmen Nutzungsdaten sammeln können. In den Standard-Einstellungen verhindert die TrutzBox nicht, dass im Browser Werbung angezeigt wird. Das blockieren von Werbung kann der TrutzBox Administrator allerdings bei Bedarf einschalten.
TrutzContent/TrutzBrowse ist ein „Privatisierungs-Werkzeug“, das die heimliche Analyse des Nutzerverhaltens beim Surfen im Internet verhindert. Somit können Informationen über das Verhalten der Internet-Nutzer kaum mehr ohne ihr Wissen über Jahre gespeichert und gewinnbringend vermarktet werden. Informationen, die zwischen Ihren Geräten und einem Server im Internet ausgetauscht werden, können kontrolliert, ggf. blockiert oder zumindest „anonymisiert“ werden.
Wie bereits festgestellt, kann man bei der Nutzung von Apps auf einem Smartphone und beim Surfen im Internet von Web-Server Betreibern oder Dritten ausgespäht werden. Und das sogar Webseiten übergreifend. Dies geschieht, indem der „Ausspäher“ Sie durch Ihre einmalige Browser- und Betriebssystem-Einstellungen (Browser-Fingerprint) oder einem Cookie (eine Datei, die die Webseite auf Ihrem Gerät erstellt, und die die Webseite beim nächsten Aufruf wieder lesen kann) wiedererkennt.



(© 2015 Comidio GmbH)

Die meisten Ansätze für mehr Anonymisierung im Internet versuchen das Problem im Browser zu lösen. Dazu gibt es Plugins für die Verwaltung von Cookies, um JavaScript abzuschalten, ferner Blocker-plugins im Browser, die Domains von bekannten Trackern blockieren oder sogar speziell angepasste Browser (z.B. Chromium oder Tor-Browser). Comidio kam nach der Analyse vieler dieser angebotenen Lösungen und nach Umfragen bei Nutzern zur Erkenntnis, dass

- viele Laien nicht in der Lage sind, einen neuen Browser oder ein Browser-Plugin zu installieren und danach zu bedienen.
- JavaScript abschalten zur Folge hat, dass die meisten Webseiten nicht mehr funktionieren.
- DNT-Flag (Do-not-Track) von Tracking-Domains nicht beachtet wird.

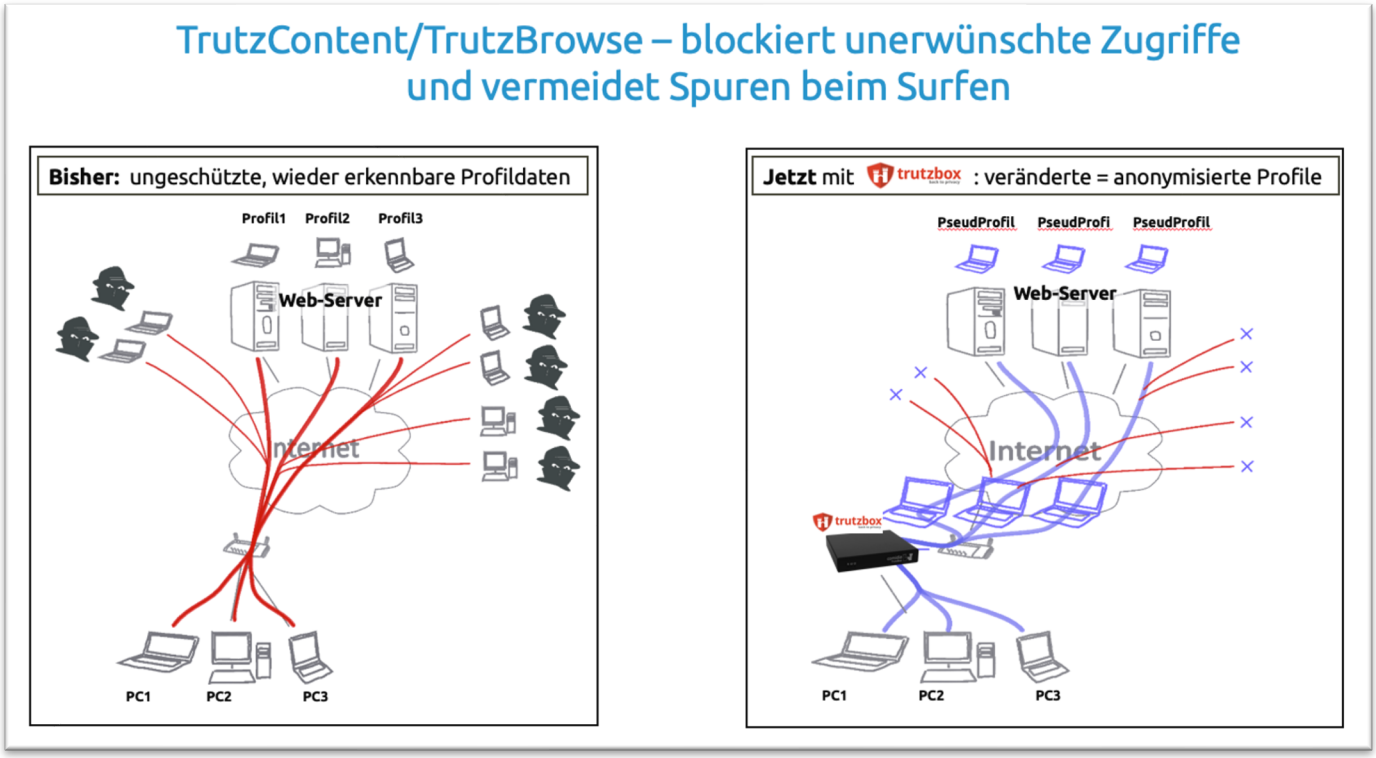
- viele Browser-Sicherheitseinstellungen den Laien überfordern oder die Bedienung für den Anwender zu umständlich ist (z.B. Flash abschalten, Third Party Cookie-Handling, Chronik-Handling.
- IP-Adress-Verschleierungs-Tools wie Tor den Web-Browser nicht daran hindern, dem aufgerufenen Web-Server und den Daten-Trackern weiterhin Daten zu liefern. Und bei VPNs gibt es keine Garantie, dass der VPN-Betreiber nicht auch noch die Benutzer ausspäht.
- Browser ohne Aufforderung des Anwenders HTTP-Zugriffe auf Web-Server durchführen, sodass ein Browser-Plugin das gar nicht mitbekommt und somit auch nicht analysieren oder blocken kann (z.B. Zugriffe auf Browser- und Plugin-Updates, auf mozilla.org oder Googles 10e100 Domain211 o.ä.).
- Irgendwelche anderen Geräte im Haushalt Web-Zugriffe durchführen, für die es gar keine Plugins gibt (z.B. für Spielekonsolen und Fernseher).

Die TrutzBox umgeht durch ihre einzigartigen TrutzContent/TrutzBrowse Architektur diese Einschränkungen. Mit ihrer Hilfe ist auch jeder Laie in der Lage, sich vor ungewolltem Ausspähen zu schützen. Für einen Daten-Tracker ist es nicht mehr so einfach möglich, diesen Schutz zu umgehen.
Die TrutzBox Funktionen TrutzBrowse und TrutzContent wurden durch einen intelligenten Proxy (Stellvertreter) implementiert, der an zentraler Stelle (in der TrutzBox) jeglichen HTTP-Datenaustausch zwischen dem gesamten Heimnetz und dem Internet überwacht. Dieser Proxy fasst Funktionen der gängigen Browser-Plugins zusammen und bietet darüber hinaus vieles mehr. Er stellt sicher, dass

- alle Anfragen auf verräterische HTTP-Header-Daten hin untersucht und nach Bedarf verschleiert werden, indem der Proxy diese HTTP-Header blockiert oder verfälscht,
- unerwünschte Cookies blockiert werden und
- alle Server-Verbindungen mit auf der TrutzBox gespeicherten Blacklists vergleicht und bei Bedarf unerwünschte oder sogar gefährliche Verbindungen blockiert werden. Oftmals sind dies Verbindungen, die gar nicht bewusst aufgerufen wurden, sondern solche, auf die die aufgerufene Webseite verlinkt ist. Das können einerseits Werbe- oder Statistik-Server sein aber andererseits auch gefährliche Web-Server, die bekanntermaßen Schad-Software verteilen.

Damit ist es Trittbrettfahrern, denen die von Ihnen aufgerufene Webseite Zugang zu Ihren Daten gewähren wollte, nicht mehr so einfach möglich, an diese Informationen zu gelangen. Außerdem erhält auch der Web-Server, den Sie aufgerufen haben, nur noch die Daten, die er für seine Arbeit unbedingt benötigt.

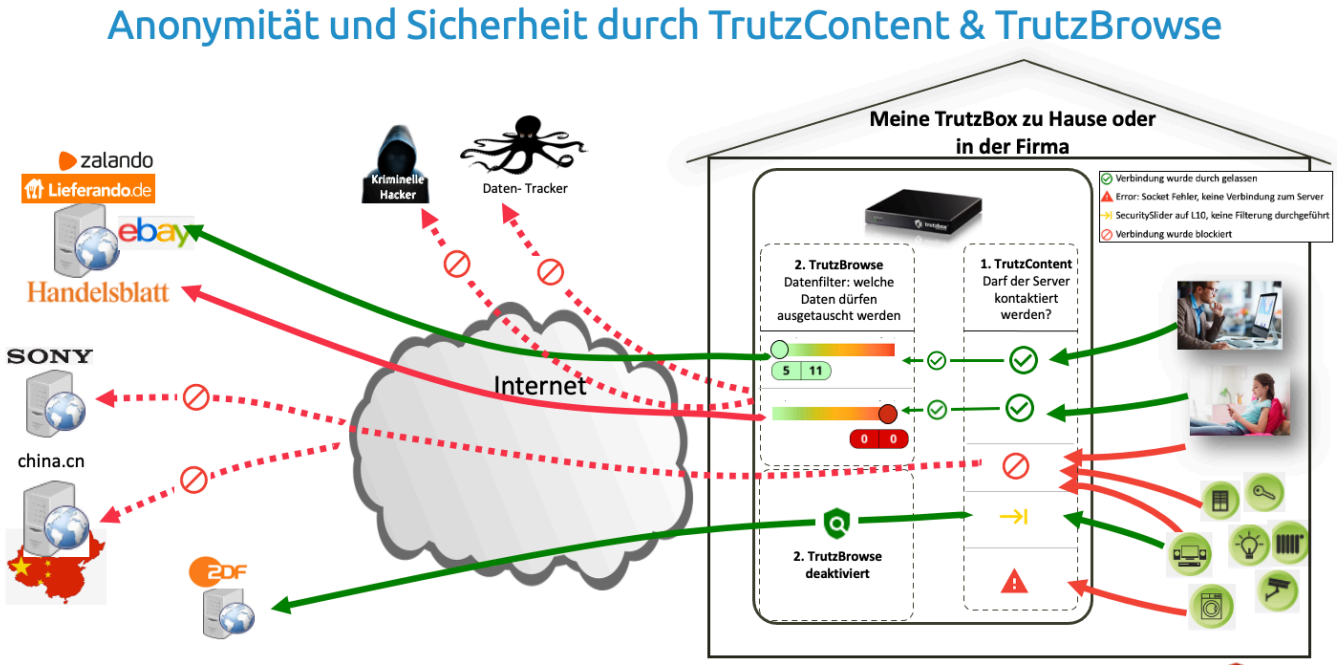
[211] https://www.webmasterworld.com/google/4050443.htm



(© 2020 Comidio GmbH)

Wie genau funktioniert die TrutzContent/TrutzBrowse-Funktion (der TrutzBox-Proxy)?

Internet-Zugriffe gehen immer von einem Gerät im internen Netzwerk aus. Das kann irgendeine Anwendung, also eine App auf einem Smartphone oder IoT-Gerät, oder ein Browser sein. Wenn der Internet-Zugriff, der über Port 80 (http) oder verschlüsselt über Port 443 (https) über die TrutzBox geleitet wird, wird dieser vom TrutzBox-Proxy verarbeitet. Proxy ist der englische Begriff für „Stellvertreter“. Dieser Proxy verhält sich gegenüber dem aufrufenden Programm wie ein Web-Server und führt dann den eigentlichen Zugriff auf den angeforderten Web-Server durch. Die Antwort vom Web-Server geht in umgekehrter Richtung auch wieder durch den TrutzBox-Proxy, der auch die Antwort des Servers kontrolliert.



(© 2021 Comidio GmbH)

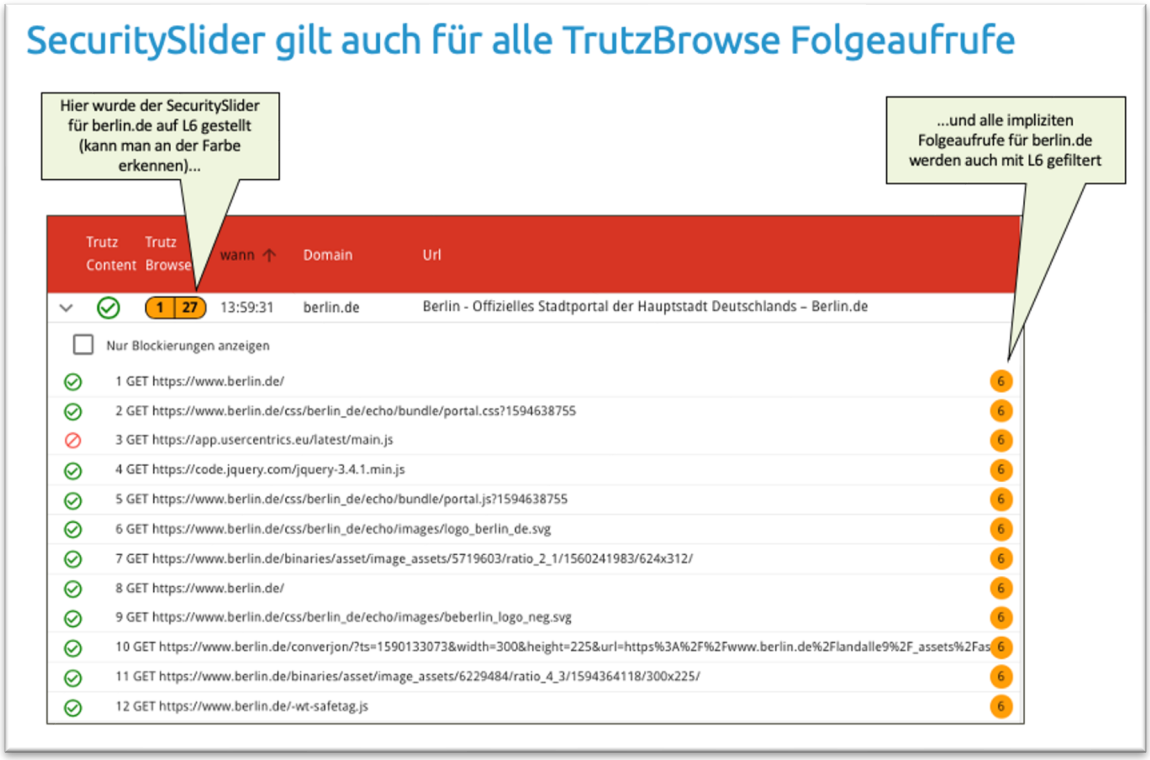
Der TrutzBox-Proxy verarbeitet den angeforderten Zugriff in der TrutzBox in zwei Schritten:

- 1. **TrutzContent** prüft zunächst auf Basis der für dieses Gerät eingestellten Filtergruppe, ob der adressierte Server kontaktiert werden darf. Wenn nicht, wird der Zugriff von der TrutzBox blockiert. Welche Filterlisten für ein Gerät genutzt werden sollen, hängt davon ab, welche in welcher Filtergruppe ein Gerät zugeordnet wurde. TrutzContent wird durch die Zuordnung eines Geräts zu einer Filtergruppe eingestellt.
- 2. Wenn der Server kontaktiert werden darf, wird eine evtl. verschlüsselte Kommunikation entschlüsselt und **TrutzBrowse** filtert die ausgetauschten Daten mehr oder weniger, je nach Einstellung des Security-Sliders. Dieser zweite Schritt wird nur dann durchgeführt, wenn TrutzBrowse für das entsprechende Gerät aktiviert wurde.

Im Bild oben, gibt zunächst TrutzContent den Zugriff auf **ebay** frei. Da der Securityslider auf Level 1 steht, werden die Daten, die zwischen Browser und ebay ausgetauscht werden, durch die TrutzBrowse Funktion anonymisiert.
Auch beim Zugriff auf das **Handelblatt** hat TrutzContent den Zugriff frei gegeben., Da allerdings für das Handelsblatt der SecuritySlder auf Level 9 steht, werden die Daten hier kaum weiter anonymisiert.
Auch der Zugriff auf das **ZDF** hat TrutzContent erlaubt, aber da für das ZDF TrutzBrowse abgeschaltet wurde (SeuritySlider steht auf Level 10), werden die ausgetauschten Daten hier nicht kontrolliert.
Für die IoT-Geräte wurde hier der Zugriff auf china.cn und Sony gesperrt.

Der SecuritySlider gilt auch für alle TrutzBrowse Folgeaufrufe

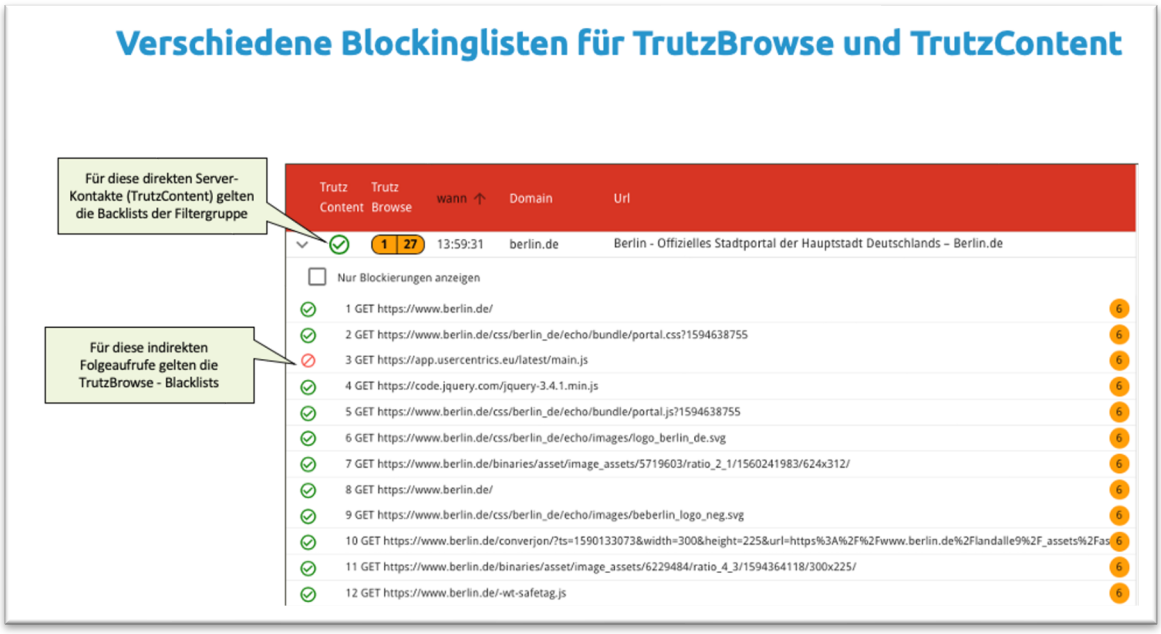
TrutzBrowse kontrolliert und anonymisiert Server-Zugriffe in Abhängigkeit des SecuritySliders. Jedoch nicht nur die Daten des gerade abgerufenen Servers. Die Einstellungen des SecuritySliders gelten sowohl für den gerade abgerufenen Server, als auch immer für alle „Folgeaufrufe einer Webseite“ des ursprünglich aufgerufenen Servers.



(© 2020 Comidio GmbH)

Verschiedene Blockinglisten für TrutzBrowse und TrutzContent

Die Unterscheidung, ob ein Server-Kontakt zu TrutzBrowse oder TrutzContent gehört, ist eines der Alleinstellungsmerkmale der TrutzBox. Sie ist derzeit die einzige Anonymisierungslösung, die diese Unterscheidung machen kann. Somit ist es möglich, verschiedene Blockinglisten zu nutzen. Z.B. möchte man zwar facebook.com im Browser aufrufen können, aber bei Aufruf eines Shops, soll nicht erlaubt sein, dass diese Shop-Seite implizit facebook.com kontaktiert und persönliche Daten an Facebook liefert. Deswegen ist es möglich, verschiedene Blockinglisten (engl. Blacklists) für TrutzBrowse und TrutzContent anzugeben. Die Blockinglisten für solche „impliziten Folgeaufrufe“ werden durch die TrutzBrowse-Blacklists bestimmt.



(© 2020 Comidio GmbH)

Da die TrutzBox jedoch in beiden Fällen lediglich den Aufruf des facebook.com Servers „sieht“, und nicht „wissen“ kann, ob dieser Aufruf durch einen Benutzer bewusst abgerufen wurde oder ein impli-zierter Aufruf ist, wurden für diese Unterscheidung im TrutzBox-Proxy einige komplexe Algorithmen implementiert.

Die TrutzBox nutzt mehrere Informationen, um zu erkennen, ob ein aufgerufener Server vom Anwender bewusst eingegeben oder angeklickt wurde (TrutzContent), oder ob es ein implizierter Aufruf einer Webseite ist (TrutzBrowse). Das wichtigste Kriterium für diese TrutzBrowse/ TrutzContent Unterschei-dung ist der http-Parameter "Referer", aber auch das Timing zwischen zwei Server-Aufrufen spielt eine Rolle. So kann es vorkommen, dass bei fehlendem Referer-Hinweis eine zu schnell angeklickte zweite Webseite irrtümlich als TrutzBrowse erkannt wird. In diesem Fall übernimmt die TrutzBox dann irrtüm-licher Weise den SecLevel der vorherigen Seite.

Die TrutzBox kann somit nicht immer mit 100% Sicherheit feststellen, ob der Anwender die Seite be-wusst aufgerufen hat oder ob sie implizit nachgeladen wurde. Wenn man z.B. zu schnell nach dem La-den einer Seite einen Link dieser Seite in einer Mail anklickt, dann kann es vorkommen, dass die Trutz-Box diesen Server-Abruf als TrutzBrowse erkennt, obwohl es ein bewusster Aufruf des Anwenders war und somit unter TrutzContent fallen sollte. Da die TrutzBox dann „denkt“, dass dies jetzt ein implizierter Aufruf sei, kann es vorkommen, dass sie den SecSlider-Level der vorherigen Seite übernimmt.

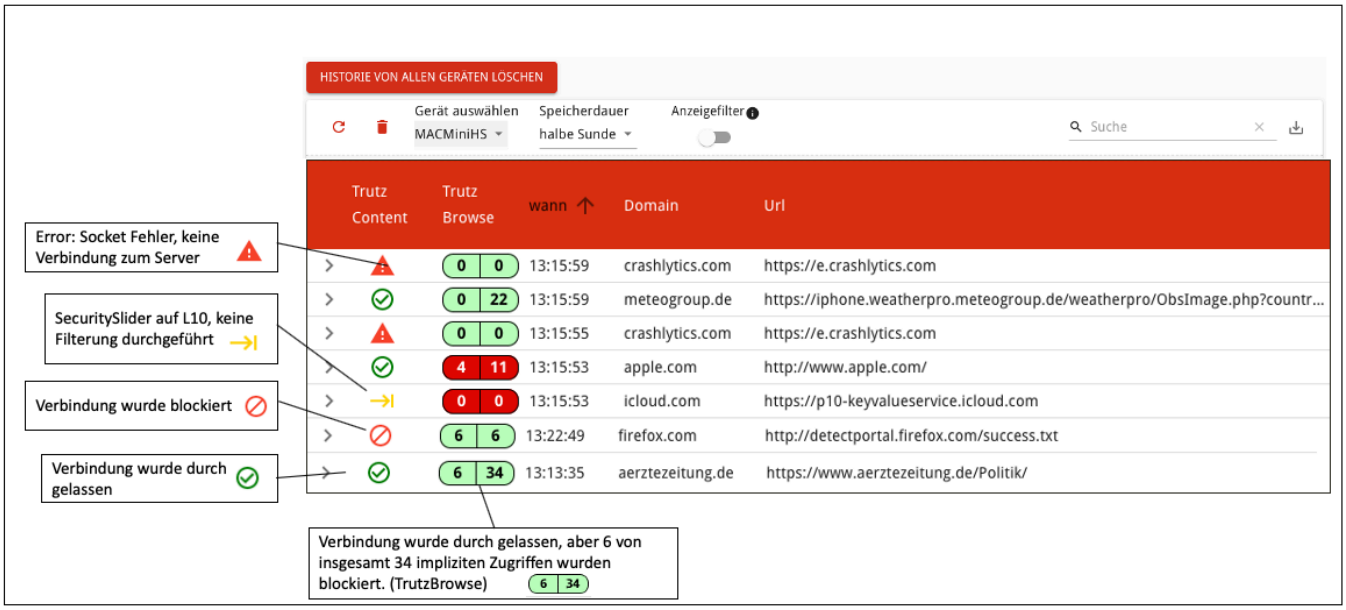
Auch wenn ein bewusst aufgerufener Link auf eine weitere Web-Seite verweist, kann die TrutzBox evtl. nicht erkennen, dass der zweite Aufruf ein impliziter Aufruf des ersten Links ist. Das kommt z.B. dann vor, wenn man im Google-Suchergebnis einen Link anklickt. Google verlinkt die Suchergebnisse immer so, dass man gar nicht einen Link direkt anklickt, sondern erst einmal eine Google-Seite, die dann erst an den eigentlichen Server weiterleitet. So kann Google genau sehen, welchen Server man in der Ergebnis-liste angeklickt hat.

Ist diese angeklickte Seite im TrutzBrowse-Filter aktiviert, kann es auch vorkommen, dass dadurch auf dem Bildschirm die TrutzContent Blockierungsmeldung erscheint, obwohl sie gar nicht im TrutzCon-tent-Filter aktiviert ist. Dieser „Nebeneffekt“ kann manchmal durch ein Browser-Refresh umgangen werden.

Zugriffsprotokoll – TrutzContent/TrutzBrowse

Der Proxy ist in der Lage, alle aus- und eingehenden Netzwerkverbindungen, die über http (Port 80) oder https (Port 443) von allen angeschlossenen Geräten gehen, zu kontrollieren. Dabei ist es möglich, diese Verbindungen aufzuzeichnen und nachträglich aufzulisten. Da die TrutzBox dabei auch genau aufzeichnet, welche Anpassungen sie bei jeder Verbindung vorgenommen hat, ist diese Aufzeichnung ein zentrales Instrument um ungewöhnlichen Datenverkehr aufzuspüren oder Verbindungsprobleme zu analysieren und zu beheben.

Zugriffsprotokoll – TrutzContent/TrutzBrowse, TrutzBrowse aktiviert



(© 2020 Comidio GmbH)

Um das Zugriffsprotokoll zu aktivieren, muss zunächst die Speicherdauer des Protokolls eingestellt werden. Danach kann für jedes Gerät das Zugriffsprotokoll abgerufen werden.

Um wirklich alle Verbindungsdaten zu sehen, sollte der Anzeigefilter de-aktiviert sein. Wenn der Anzeigefilter aktiviert ist, dann werden nur solche Datenverbindungen angezeigt, die der Datenfilter angepasst hat. Blockierte oder unveränderte Datenverbindungen werden nicht angezeigt.

Jede TrutzContent-Verbindung entspricht einem Eintrag in diesem Protokoll. Wobei in der **Spalte TrutzContent** angezeigt wird, ob

- ein Socket Fehler aufgetreten ist, somit keine Verbindung zum Server hergestellt werden konnte,
- der SecuritySlider auf L10 steht, somit keine Filterung durchgeführt wurde,
- die Verbindung aufgrund einer TrutzContent-Regel blockiert wurde, oder ob
- die Verbindung durchgelassen wurde

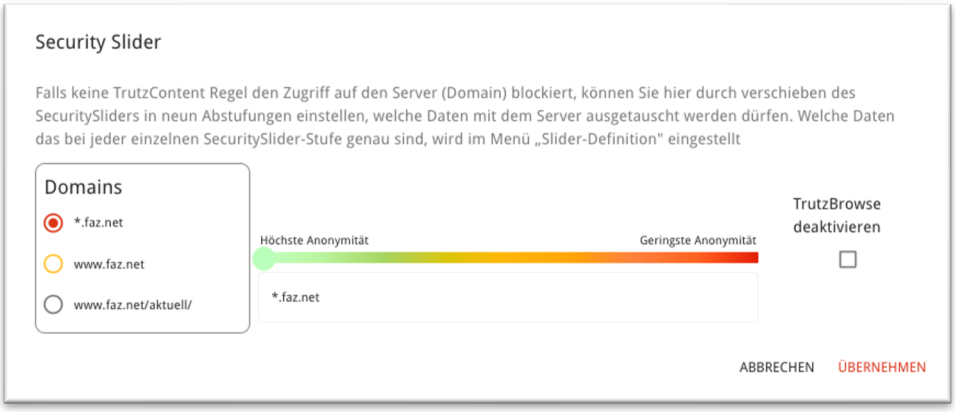
Mit einem Klick auf eines der Symbole oder , ist es möglich, eine blockierte Verbindung für zukünftige Zugriffe frei zu schalten bzw. zu blockieren. Dazu wird ein Menü angeboten, in der es möglich ist, die frei zu schaltende oder zu blockende Domain noch mal genauer zu spezifizieren.

(© 2020 Comidio GmbH)

Falls in der Geräteeinstellung für dieses Gerät TrutzBrowse aktiviert wurde, wird in der **Spalte TrutzBrowse** angezeigt, welche Filter für diesen Server-Kontakt und allen folgenden impliziten Serverzugriffen die Anonymität sichergestellt haben.

Die Farbe der Symbols 13 104 gibt an, mit welchen SecurityLevel ein Serverzugriff stattfinden durfte und somit, welche Daten die TrutzBox gefiltert hat. Die erste Zahl in der Box zeigt die Anzahl der geblockten impliziten Aufrufe, die zweite Zahl zeigt die Gesamtanzahl der angeforderten impliziten Server-Kontakten.

Mit einem Klick auf das TrutzBrowse-Symbol kann man die SecuritySlider Einstellung für diesen Server-Kontakt anpassen.



(© 2020 Comidio GmbH)

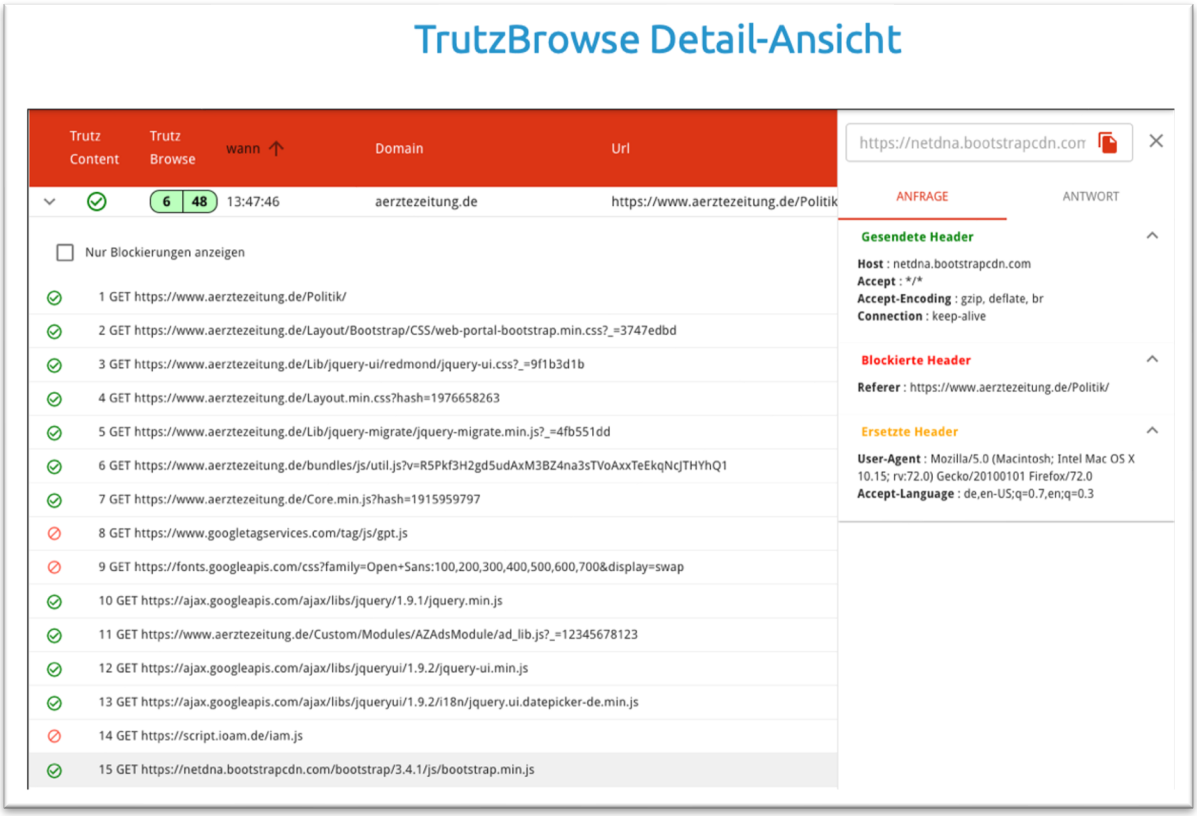
Auch hier gibt der anschließende Dialog die Möglichkeit die URL/Domain genauer zu spezifizieren, die man auf einen anderen SecuritySlider-Level setzen möchte.

Eine Slidereinstellung kann auch unqualifiziert erfolgen, indem linksbündig vor dem „.“ ein „*“ angehängt wird. So kann man nicht nur die Domain „apple.com“, sondern mit „*.apple.com“ auch alle Sub-Domains wie z.B. „cdn.apple.com“ auf eine SecuritySlider-Position stellen.

Weitere Details darüber, wie TrutzBrowse genau funktioniert, wird im Kapitel „TrutzBrowse – verräterische Daten aus der Internet-Kommunikation herausfiltern“ beschrieben.

TrutzBrowse-Detail-Ansicht

In der ersten Spalte des Zugriffsprotokolls kann man mit einem Klick auf „>“ die impliziten Aufrufe des Serverkontakts abrufen (TrutzBrowse-Detail-Ansicht).



(© 2020 Comidio GmbH)

In dieser Detail-Ansicht werden alle impliziten Server Kontakte aufgelistet. In der ersten Spalte wird mit dem Symbol

- ✓ angezeigt, dass dieser Serverkontakt nach der TrutzBrowse-Regel durchgelassen, oder mit
- ⊘ blockiert wurde.

Mit Klick auf eine Zeile werden die Zugriffs-Details für die Server-Anfrage und die Server-Antwort eingeblendet. Falls ein Zugriff blockiert wurde, es also keine Antwort vom Server geben kann, wird anstatt der Server-Antwort die Blockierungs-Regel angezeigt, die hier die Blockierung veranlasst hat.

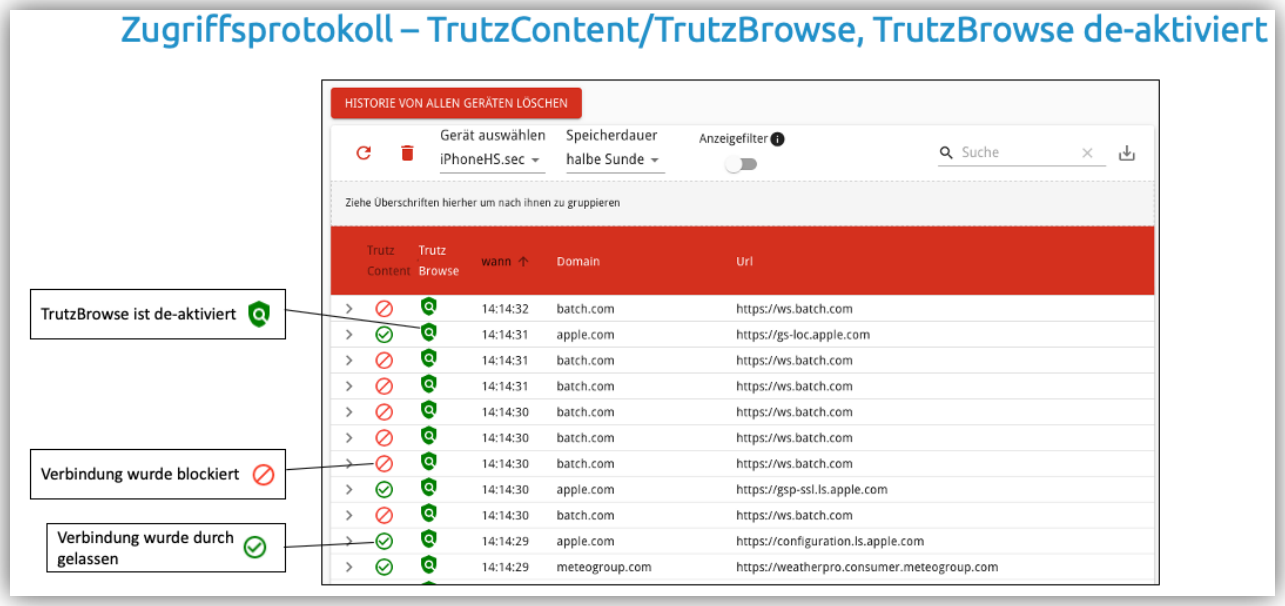
Mit einem Klick auf das Symbol ⊘ ist es möglich, eine blockierte Verbindung für zukünftige implizite Zugriffe frei zu schalten. Dadurch wird die URL/Domain, die die Blockierungs-Regel ausgelöst hat, aus Standard-TrutzBrowse-BL ausgetragen (wenn es sich um eine selbst erstellte Blacklist handelt), oder in die Standard-TrutzContent-WL eingetragen, wenn es sich um eine von Comidio vorgegebene Standard-Blacklist handelt.

(© 2020 Comidio GmbH)

Mit einem Klick auf das Symbol kann eine bisher erlaubte Verbindung für zukünftige implizite Zugriffe blockiert werden. Dadurch wird eine URL/Domain in die Standard-TrutzBrowse-BL eingetragen. Dazu wird ein Menü angeboten, in der es möglich ist, die frei zu schaltende oder zu blockende URL/Domain noch mal genauer zu spezifizieren.

(© 2020 Comidio GmbH)

Wenn in den Geräte-Einstellungen TrutzBrowse de-aktiviert wurde, wird dies im Zugriffsprotokoll in der Spalte „TrutzBrowse“ mit dem Symbol gekennzeichnet.



(© 2020 Comidio GmbH)

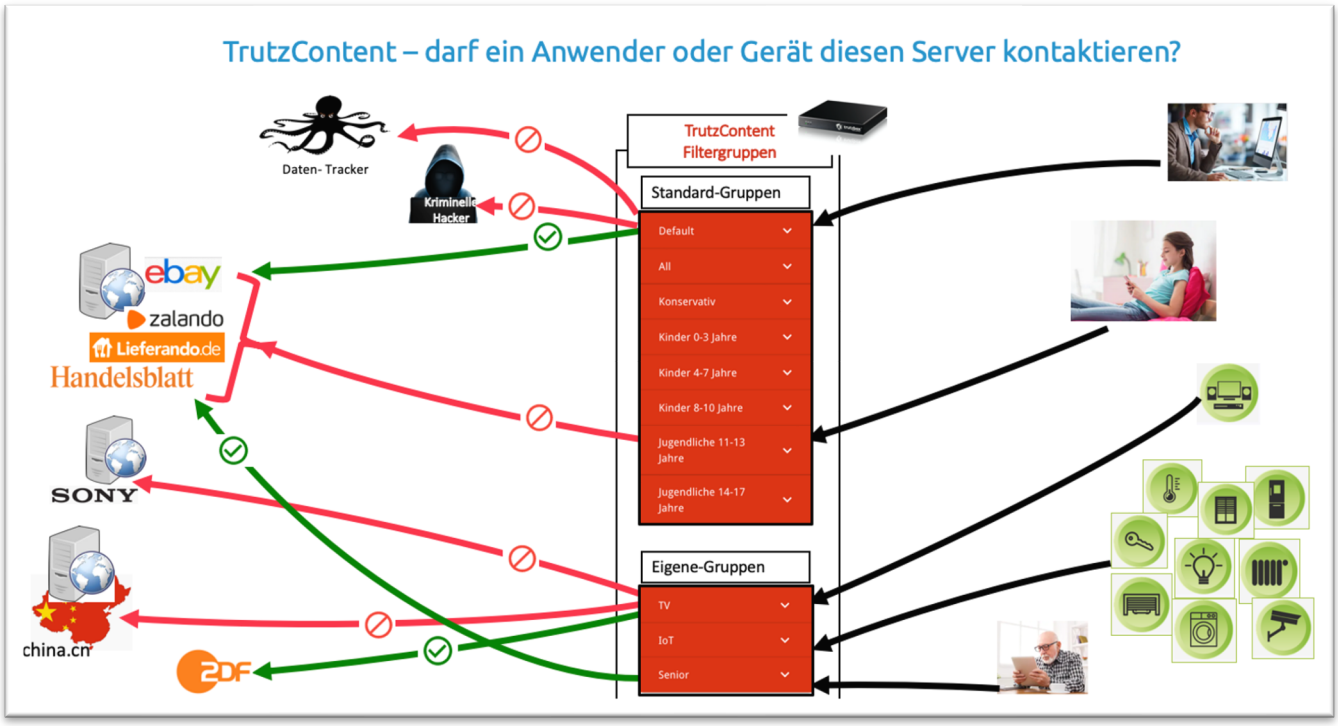
In diesem Fall werden alle impliziten Aufrufe wie explizite Aufrufe behandelt und somit über die Trutz-Content-Filtergruppe geprüft, ob der Serverkontakt erlaubt ist. Bei de-aktiviertem TrutzBrowse ist es nicht möglich den SecuritySlider zu nutzen.

TrutzContent – Filtergruppen, Themengebiete und Filterlisten

Um die Kontaktaufnahme von Geräten oder TrutzBox -Benutzern zu bestimmten Servern zu blockieren, kann ein Gerät oder einen TrutzBox-Benutzer einer Filtergruppe zuordnet werden.
Hier ein paar sinnvolle Anwendungsmöglichkeiten des Zugriffblockers:

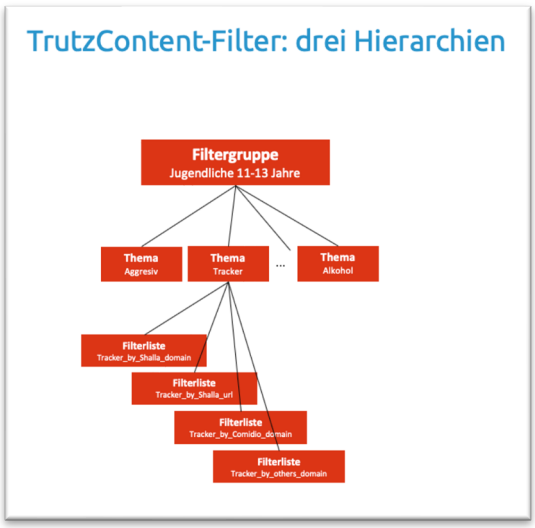
- Jugendliche vor ungeeigneten Internet-Seiten schützen
- Personen, die die Folgen ihres Handelns nicht abschätzen können vor Web-Seiten wie „Kostenfallen“ oder „Web-Shops“ schützen (z.B. Einsatz in Seniorenheimen)
- IoT-Geräte (Video-Kamera, Heizung, Fernseher usw.) daran hindern, dass diese Geräte zu unerwünschten Servern Kontakt aufnehmen
- Apps auf Smartphones oder das Smartphone selbst daran hindern, dass es zu unerwünschten Servern Kontakt aufnimmt. Z.B. Kontakt zum Hersteller oder einer Tracking-Firma
- Da aber alle Betriebssysteme ständig Kontakt zum Hersteller aufnehmen, kann man hiermit diesen Datenaustausch kontrollieren und einschränken.

Wenn ein Gerät von der TrutzBox neu erkannt wird, dann gehört dieses Gerät zunächst automatisch zur Filtergruppe „Default“. Danach kann man z.B. den PC und das iPhone der zwölfjährigen Tochter der Gruppe „Kinder 11-13 Jahren“ zuordnen, oder den Fernseher der selbst definierten Gruppe „TV“.



(© 2020 Comidio GmbH)

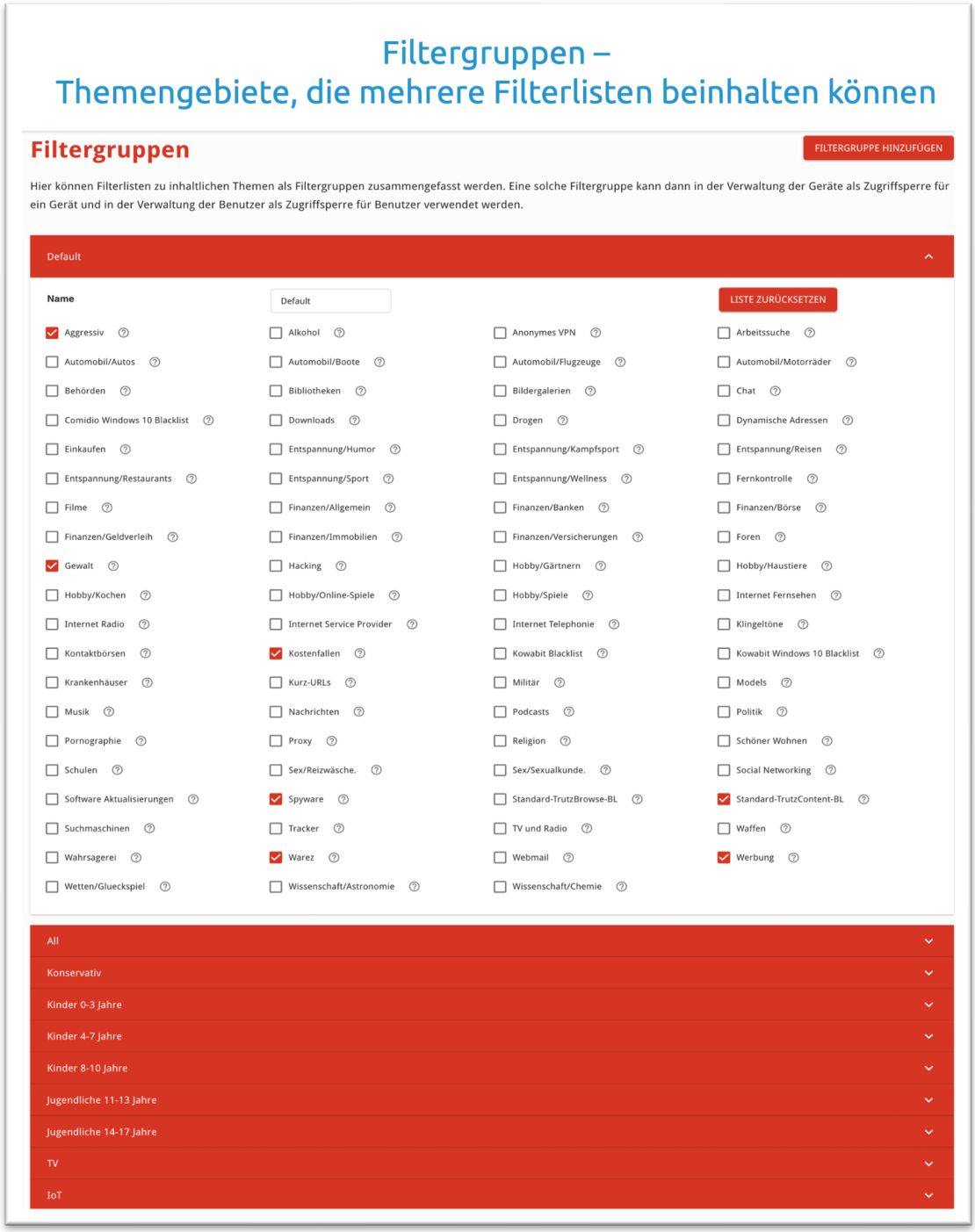
Die TrutzBox wird mit sehr vielen Filterlisten ausgeliefert, die regelmäßig durch die automatische Update-Funktion der TrutzBox von Comidio auf dem neuesten Stand gehalten werden. Natürlich kann der Administrator auf der TrutzBox auch eigene Filterlisten anlegen. Für ein Themengebiet, z.B. „Tracker“ oder „Werbung“ kann es mehrere Filterlisten geben. Filterlisten sind somit nach Themengebieten zusammengefasst.
Eine Filtergruppe besteht aus selbst angelegte Filterlisten und Themengebieten. Somit gibt es diese drei Hierarchien:



(© 2020 Comidio GmbH)

Filtergruppen

Über das TrutzBox-Menü Filtergruppen können vorhandene Filtergruppen editiert und neue Filtergruppen angelegt werden.



(© 2020 Comidio GmbH)

Filterlisten

Comidio liefert ca. 100 Filterlisten an alle TrutzBoxen aus. Diese Filterlisten stammen aus unterschiedlichen Quellen und werden mit unterschiedlicher Häufigkeit automatisch upgedatet. Einige Filterlisten werden von Comidio selbst erstellt und auf dem neuesten Stand gehalten. In den Filtergruppen, sind diese Listen nach Themengebieten zusammengefasst.
Der TrutzBox-Administrator kann aber auch eigene Filterlisten erstellen. Bei der Erstellung einer Filterliste muss angegeben werden, ob diese Liste als White- oder als Blacklist verwendet werden soll. Whitelisten dienen dazu, in der Geräte-Einstellung geblockte Zugriffe zu überschreiben, also Ausnahmen zu den angegebenen TrutzContent- und TrutzBrowse Filtern zuzulassen. Blacklists werden verwendet um bestimmte Zugriffe bei TrutzContent- und TrutzBrowse zu blockieren, die nicht in den vorgegebenen Listen schon geblockt werden.

(© 2021 Comidio GmbH)

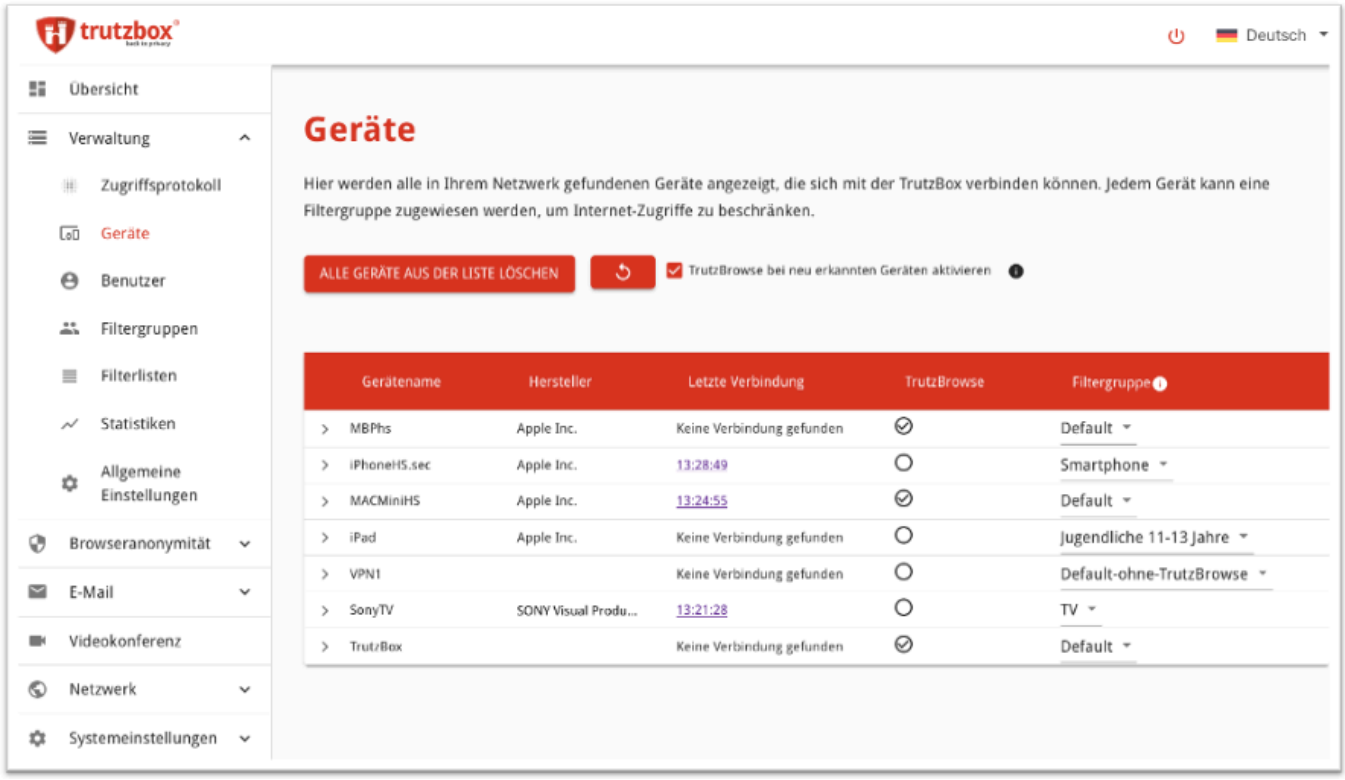
Die Einträge eine Filterliste dürfen keine unqualifizierten Einträge sein. Ein * vor einer URL/Domain ist somit nicht erlaubt.

Geräte - Verwaltung

In der Geräte-Verwaltung werden automatisch alle bisher erkannten Geräte aufgelistet. Jedes erkannte Gerät ist einer TrutzContent-Filtergruppe zugeordnet. Standardmäßig ist das die Gruppe „Default“. Hier ist es möglich, Geräte einer Benutzergruppe zuzuordnen und damit die Zugriffsbeschränkung der Benutzergruppe zu aktivieren.
Die TrutzBox erkennt und speichert die Einstellungen eines Gerätes aufgrund der MAC-Adresse des Geräts (Hardware-Kennung). Es kommt jedoch gelegentlich vor, dass die TrutzBox die MAC-Adresse des

Geräts nicht ermitteln kann. In diesem Fall merkt sich die TrutzBox den Hostnamen des Geräts und wenn auch kein Hostname bekannt ist, dann wird das Gerät unter seiner IP-Adresse in der TrutzBox gespeichert.

Geräte, die die TrutzBox erkannt hat



(© 2020 Comidio GmbH)

Mit dem Knopf „**Alle Geräte aus der Liste löschen**“ wird die Liste der erkannten Geräte komplett gelöscht. Danach werden alle Geräte, die die TrutzBox nutzen, automatisch wieder in der Liste aufgeführt. Die Einstellungen für die jeweiligen Geräte müssen dann evtl. erneut vorgenommen werden.
Mit  wird die Liste neu geladen.

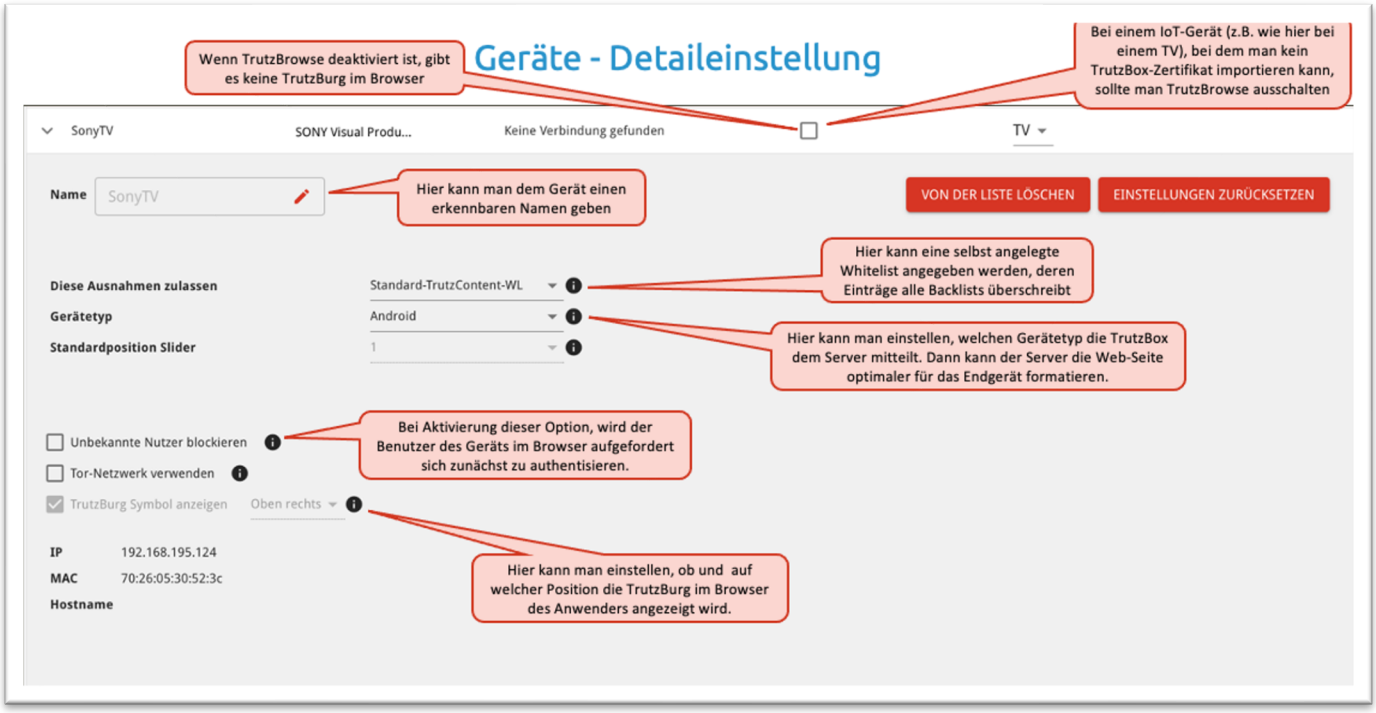
Mit dem Schalter „**TrutzBrowse bei neu erkannten Geräten aktivieren**“ wird festgelegt, ob bei neu erkannten Geräten TrutzBrowse aktiviert werden soll oder nicht. Da für die TrutzBrowse-Funktion im Endgerät das TrutzBox-Root-Zertifikat gespeichert sein sollte, sollte diese Option deaktiviert sein, falls die TrutzBox im öffentlichen Raum eingesetzt wird. Wenn z.B. in einem Krankenhaus, Seniorenheim oder im öffentlichen Raum das Netzwerk mit der TrutzBox abgesichert wird, besteht keine Kontrolle über die Geräte, die sich mit der TrutzBox verbinden. Und somit kann in solchen Einsatzgebieten auch kein TrutzBox-Root-Zertifikat auf dem Endgerät gespeichert werden.
Wenn standardmäßig TrutzBrowse für alle erkannten Geräte aktiviert werden soll, ist es jedoch auch möglich, TrutzBrowse nachträglich für ein einzelnes Gerät zu de-aktivieren.

Wenn für ein Gerät Daten im Zugriffsprotokoll gespeichert sind, wird hier unter „Letzte Verbindung“ ein Link zu dessen Verbindungsdaten angezeigt. Da Verbindungsdaten nur dann gespeichert werden,

wenn dies zuvor im Menü „Zugriffsprotokoll“ aktiviert wurde, wird hier ein Aktivierungsschalter angezeigt, falls das Zugriffsprotokoll nicht aktiviert ist.
In der Spalte „TrutzBrowse“ ist ersichtlich, ob für das Gerät TrutzBrowse ⊘ aktiviert oder ○ de-aktiviert ist.
Über die Filtergruppe wird gesteuert, auf welche Server im Internet ein Gerät nicht zugreifen darf.

Geräte-Detaileinstellungen

Mit dem Knopf „>“ vor dem Gerätenamen können Detail-Einstellungen des Gerätes vorgenommen werden. Dort werden nicht nur Netzwerk-Parameter des Geräts angezeigt, sondern hier kann man auch individuelle Zugriffskontrollen des Geräts verwalten. Hier ein Beispiel für das Gerät „SonyTV“:



(© 2021 Comidio GmbH)

Im Feld „Name“ wird Anfangs der Hostname des Geräts angezeigt, mit dem es sich im Netzwerk bekannt gemacht hat. Hier ist es möglich, einen verständlicheren Namen des Geräts zu vergeben. Der eigentliche Hostnamen des Geräts wird dabei nicht verändert.
Falls ein Zugriff über die Fernverbindung (VPN) stattgefunden hat, wird das Gerät hier zwar auch aufführt, aber aus technischen Gründen kann in diesem Fall oft kein Host-Name ermittelt werden.

Diese Ausnahmen zulassen

Über das Feld „Diese Ausnahmen zulassen“ ist möglich, dem Gerät eine „Whitelist“ zuzuweisen, also eine Liste erlaubter Domains. Mit einer solchen Whitelist können z.B. Standard-Blockierungen, die von

Comidio vorgegeben werden, aufgehoben werden. Eine Whitelist muss zuvor in „Filterlisten“ als Whitelist angelegt sein und kann dann hier direkt unter „Diese Ausnahmen zulassen“ für ein Gerät aktiviert werden.

Gerätetyp festlegen

Unter „Gerätetyp“ kann für jedes Gerät eingestellt werden, ob es sich um ein Desktop-, Android- oder iOS-Gerät handelt. Sodass damit ein passender „user-agend“ Wert dem Server anzeigen kann, für welchen Gerätetyp die Webseite aufbereitet werden soll. Der tatsächlich zum Server gesendete „user-agend“ Wert kann unter „Browseranonymität“ -> „Slider-Definition“ -> “immer dieser user-agend Wert senden“ angepasst werden.

Standardposition Slider

Die Einstellung "Standardposition Slider" bietet bei eingeschaltetem TrutzBrowse eine Möglichkeit, einen fest definierten SecSlider Wert für alle Server-Zugriffe dieses Geräts fest zu legen. Diese Funktion ermöglicht es, selbst solche Geräte zu kontrollieren, die auf ständig wechselnde Server eines Dienstleisters zugreifen.

Unbekannte Nutzer blockieren

Normalerweise werden Zugriffsbeschränkungen für ein Gerät durch die Eingruppierung in eine Filtergruppe eingeschränkt. Durch Aktivierung dieser Option, kann man einen Benutzer dieses Geräts im Zugriffe einschränken. Der Benutzer wird dann zunächst zum Einloggen auf dem Gerät aufgefordert. Im Menü „Benutzer“ kann die Zugriffsbeschränkungen (TrutzContent) für den Benutzer eingestellt werden.

Tor-Netzwerk verwenden

Mit dem Schalter „Tor Netzwerk verwenden“ kann die Pseudonymisierung der IP-Adresse aktiviert werden, indem dieses Gerät das Tor-Netzwerk[212] für Internet-Zugrifee verwendet. Allerdings ist hierbei zu beachten, dass die Internet-Nutzung langsamer sein kann und manche Web-Server bei der Benutzung von Tor zusätzliche Probleme bereiten können. Hinweis: die IP-Adresse kann unter Umständen trotz aktiviertem Tor-Netzwerk vom Server ermittelt werden. Siehe hierzu das Kapitel über Tor.
Im Browser ist es dann auch möglich, Tor-Hidden-Services, also Web-Adressen die mit „.onion“ enden, aufzurufen. Alle sonstigen TrutzContent und TrutzBrowse Funktionen sind weiterhin zusätzlich aktiv.

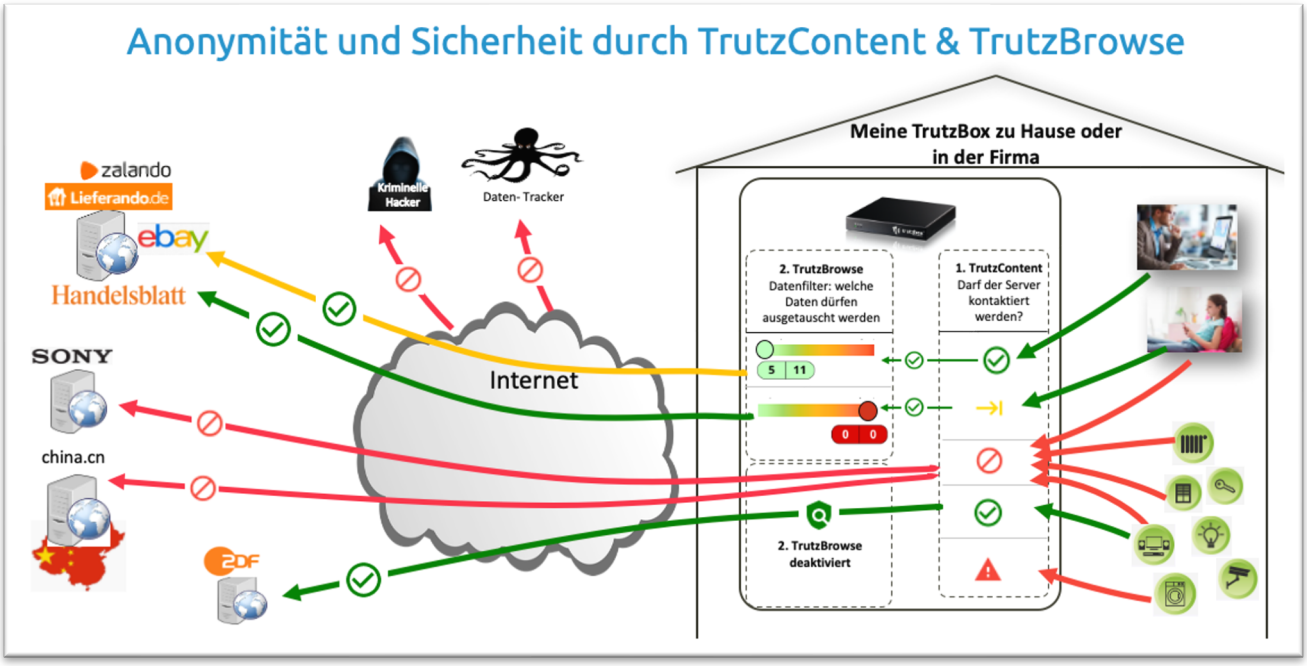
TrutzBrowse aktivieren

Mit dem Schalter „TrutzBrowse aktivieren” wird für dieses Gerät TrutzBrowse aktiviert oder komplett deaktiviert.
Wenn ein Gerät einen Server im Internet kontaktieren möchte wird bei **de-aktiviertem** TrutzBrowse-Schalter, nachdem die TrutzContent-Prüfung den Zugriff erlaubt hat, der Zugriff auf einen Server unverändert durch gelassen. Das Zertifikat des Servers wird dabei bis zum Endgerät (z.B. Browser oder App) durch gereicht. Bei de-aktiviertem TrutzBrowse sind die TrutzContent-Filter der Benutzergruppe weiterhin aktiv.

[212] https://de.wikipedia.org/wiki/Tor_(Netzwerk)

Was genau ist der Unterschied, wenn TrutzBrowse ein- oder ausgeschaltet ist?

Bei **aktiviertem** TrutzBrowse-Schalter, wird, nachdem die TrutzContent-Prüfung den Zugriff erlaubt hat, der Datenaustausch mit einem Server anonymisiert. Der Anonymisierungsgrad ist abhängig von der SecuritySlider-Position für den jeweiligen Server. Für alle TrutzBrowse-Einstellungen gelten die Einstellungen unter dem Menü „Browseranonymität“.
Damit TrutzBrowse den Datenverkehr auch bei verschlüsselter Verbindung kontrollieren kann, muss auf dem jeweiligen Gerät das TrutzBox-Stammzertifikat installiert sein. Für angeschlossene Geräte, bei denen es nicht möglich ist das TrutzBox-Stammzertifikat zu importieren (.z.B. bei ein TV oder Kamera), sollte TrutzBrowse **abgeschaltet** werden.
Wenn TrutzBrowse **abgeschaltet** ist, sollte man für dieses Gerät eine TrutzContent-Gruppe aktivieren, die strenger filtert. Also das Gerät einer Gruppe mit mehr Blacklists zuzuordnen. In dieser Gruppe sollten zumindest auch die Tracker blockiert werden.



(© 2020 Comidio GmbH)

TrutzBurg Symbol anzeigen

Falls TrutzBrowse für dieses Gerät aktiviert ist, wird im Browser des Anwenders i.d.R. oben rechts das TrutzBox-Symbol, die TrutzBurg angezeigt. Dann ist es hier möglich, die Anzeige der TrutzBurg abzuschalten. Das ist dann immer sinnvoll, wenn das TrutzBurg Symbol im Browser stört. Z.B. wenn eine Seite ohne TrutzBurg gedruckt werden soll, oder wenn man Filme auf dem Fernseher über die TrutzBox schauen möchte. Dazu kann hier für das gewünschte Gerät das Flag "TrutzBurg Symbol anzeigen" deaktiviert“ werden. Die TrutzBrowse-Filterfunktionen der TrutzBox werden dadurch nicht verändert.
Hier kann auch festgelegt werden, an welcher Ecke im Browser das TrutzBurg Symbol angezeigt werden soll. Wenn nichts anderes festgelegt wurde, ist das Symbol immer oben rechts im Browser-Fenster angeordnet.

TrutzBrowse – verräterische Daten aus der Internet-Kommunikation herausfiltern

Falls die TrutzContent-Prüfung den Zugriff auf einen angeforderten Server „erlaubt“, kontaktiert der TrutzBox-Proxy, stellvertretend für das angeforderte Gerät, den Server. Falls TrutzBrowse für das Gerät, das diesen Server kontaktieren möchte aktiviert ist, werden die gesendeten Daten jedoch vom TrutzBox-Proxy soweit möglich „neutralisiert“ (TrutzBrowse). Somit wird es dem Server möglichst erschwert, ein Profil des Aufrufers zu erstellen und eine verbesserte „Browseranonymität“ erreicht. Diese Anonymisierung wird jedoch nicht nur bei Browser-Zugriffen durchgeführt, sondern bei allen Zugriffen auf einen Web-Server. Also auch Zugriffe von Apps auf Smartphones und IoT-Geräten.
Im Folgenden werden die Bestandteile von TrutzBrowse näher beschrieben.

HTTP-Header korrigieren

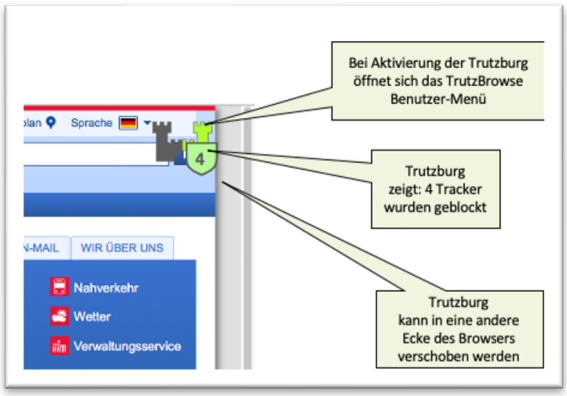
Beim Aufruf einer Webseite sendet der Browser im HTTP-Header-Daten an den Server. In der weiteren Kommunikation zwischen Web-Server und Browser, liefert der Server auch Daten an den Browser zurück und kann im HTTP-Header weitere Daten vom Browser abfragen[213]. Über diese Kommunikation kann ein Web-Server die einzigartigen Daten des Clients und des Umfelds des Clients einsammeln (z.B. Betriebssystem Version des Rechners). Damit kann der Server einen Client-basierten Fingerprint erstellen. Beim späteren Aufruf weiterer Webseiten kann ein Server den Internet-Nutzer nun wiedererkennen. Im Laufe der Zeit kann ein Tracking-Server auf diese Weise ein umfangreiches Nutzerprofil erstellen. Einem Web-Server gar keine Header-Daten zu liefern ist manchmal keine gute Alternative, da diese Daten gelegentlich dazu verwendet werden, die einzelnen Elemente auf der angeforderten Webseite so aufzubereiten, dass sie optimal auf dem Endgerät angezeigt werden können. Außerdem könnte der Tracking-Server merken, dass ihm keine brauchbaren Fingerprints mehr geliefert werden und der Tracker-Betreiber könnte sein Fingerprinting daraufhin optimieren. Manchmal ist es besser, dem Web-Server möglichst solche Informationen zu liefern, deren individuelle Zusammenstellung bei möglichst vielen anderen Internet Benutzern ebenso auftritt. Somit ist der einzelne Nutzer nicht mehr von der Menge anderer Nutzer mit gleichem Nutzerprofil zu unterscheiden.
Manche Webseiten sind wiederum so programmiert, dass sie diese HTTP-Header Informationen für die richtige Funktionsweise der Webseite benötigen. Dann kann es vorkommen, dass solche Webseiten nicht mehr richtig funktionieren, wenn man diesen Webseiten nicht alle Informationen zurückgibt. Es kann also passieren, dass plötzlich einzelne Bereiche auf einer Webseite fehlen oder ein Login nicht funktioniert.

Intelligenter SecuritySlider

Dank der TrutzBrowse Technology kann der Sicherheitsgrad einer jeden Webseite mit Hilfe des intelligenten Sicherheits-Schieberegler (Security-Sliders) jederzeit individuell für einen Server angepasst werden. Falls der Server-Kontakt über einen Browser statt findet, schleust der TrutzBox-Proxy extra Code in die html-Seite ein, so dass die TrutzBurg im Browser angezeigt wird.

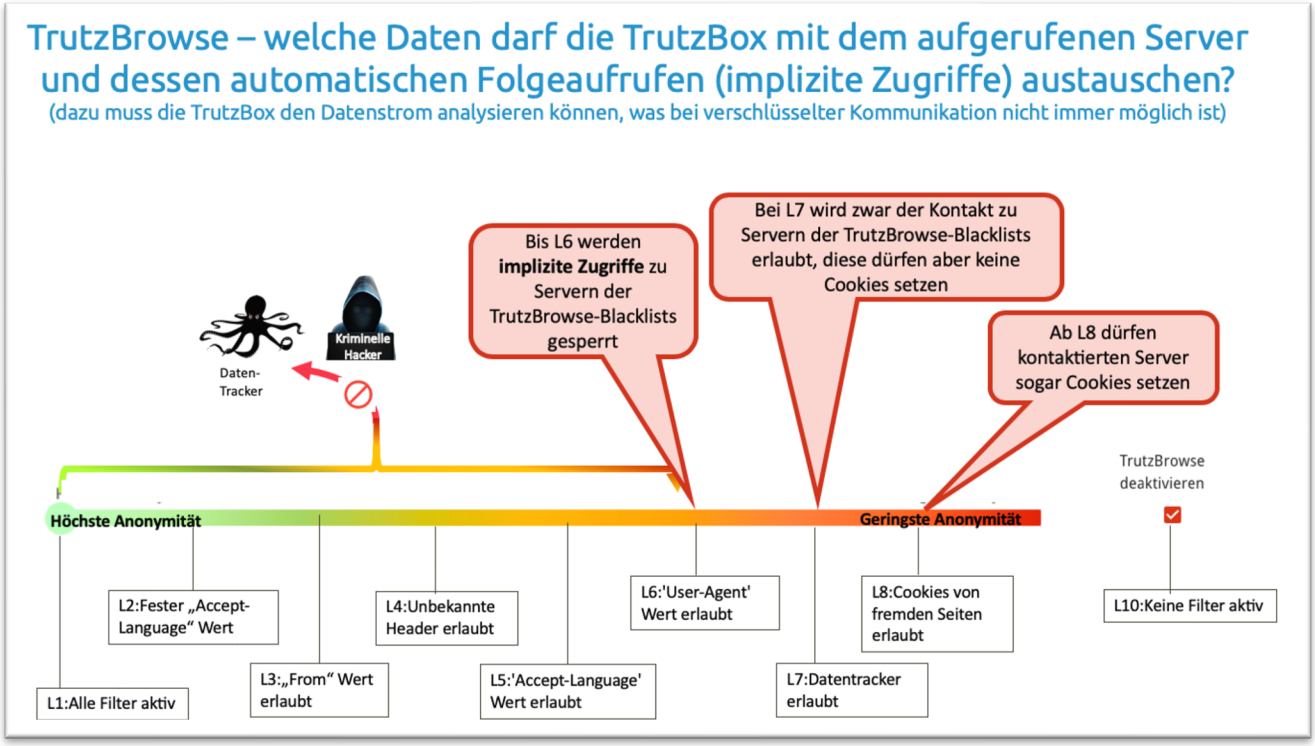
213 http://www.iana.org/assignments/message-headers/message-headers.xhtml

http://de.wikipedia.org/wiki/Liste_der_HTTP-Headerfelder



(© 2020 Comidio GmbH)

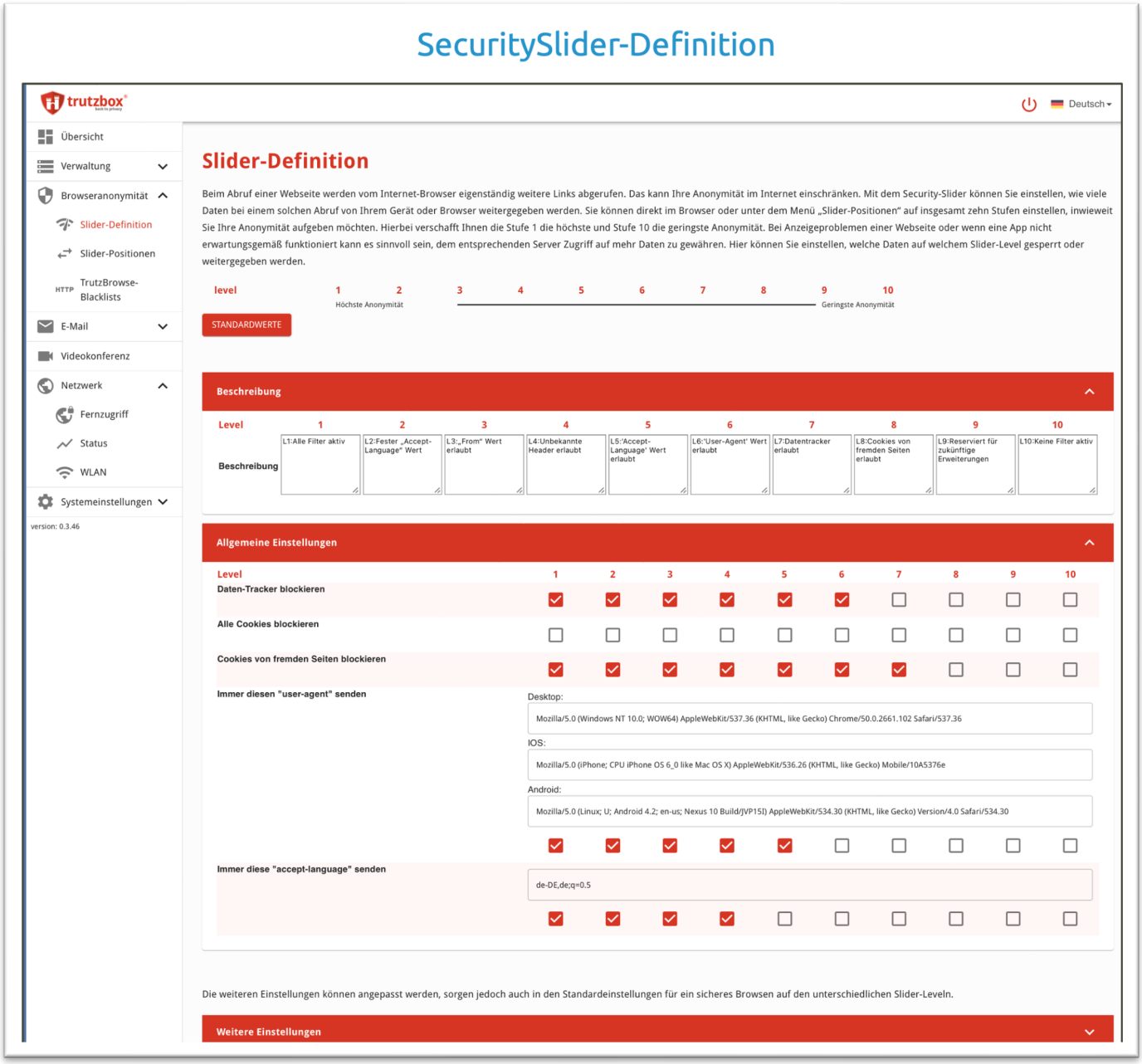
Wenn der Benutzer die TrutzBurg anklickt, wird ein Auswahl-Menü angezeigt, das es unter anderem auch erlaubt. Den Sicherheits-Schieberegler (SecuritySlider) zu verschieben.
Mit diesem Sicherheits-Schieberegler kann der Nutzer die Sicherheitsstufe der gerade angesteuerten Webseite kontinuierlich reduzieren bzw. erhöhen. Je weniger Sicherheit er für diese Seite einstellt, umso weniger Daten werden von TrutzBrowse gefiltert, und im Gegenzug eventuelle Funktionsstörungen der Seite vermieden.



(© 2020 Comidio GmbH)

Der SecuritySlider kann in neun Positionen verschoben werden. Je weiter der SecuritySlider nach rechts verschoben wird, um so mehr „echte Daten“ werden mit dem Server ausgetauscht. Somit bietet die linke Position 1 höchste Anonymität und die rechte Position 9 die niedrigste Anonymität für eine Webseite.
In Position 1 bis einschließlich 6 werden implizite Kontakte zu bekannten Datentrackern blockiert.

Ab Position 7 werden implizite Kontakte zu bekannten Datentrackern erlaubt. Jedoch ohne dass diese einen Cookie setzen dürfen. Diese sind erst ab Position 8 möglich.
Die SecuritySlider Position 10 hat eine Sonderstellung und kann nicht durch verschieben des Sliders erreicht werden. In dieser Position wird der Proxy komplett umgangen. D.h., der Proxy kann auch das TrutzBurg-Symbol nicht mehr zur Anzeige im Browser in die aufgerufene Web-Seite einsetzen. Deswegen kann Position 10 nur durch Aktivierung der entsprechenden Option gesetzt werden.
Was TrutzBrowse in jeder einzelnen Sliderstellung genau filtert, kann der TrutzBox-Administrator im Menü „Slider-Definition“ genau sehen und einstellen.



(© 2020 Comidio GmbH)

Comidio hat nach vielen Tests eine Standard Konfiguration festgelegt, die allerdings vom Administrator der TrutzBox flexibel für seine Sicherheitsbedürfnisse verändert werden kann.
In diesem Standard wurden folgende 10 Sicherheitsstufen festgelegt:

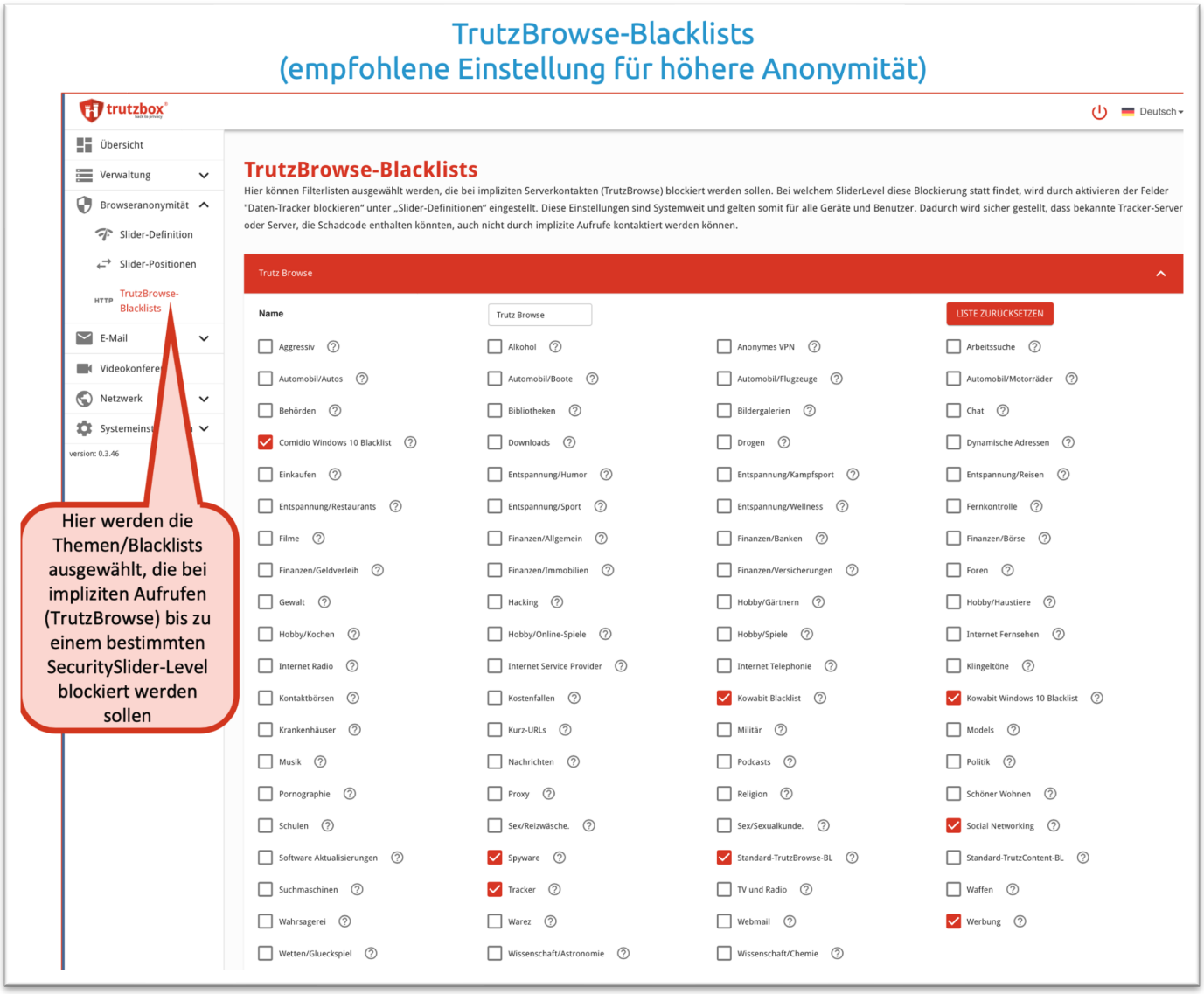
- L1: Alle Filter aktiv
- L2: Fester „Accept-Language“ Wert
- L3: „From“ Wert erlaubt
- L4: Unbekannte Header erlaubt
- L5: 'Accept-Language' Wert erlaubt
- L6: 'User-Agent' Wert erlaubt
- L7: Datentracker erlaubt
- L8: Cookies von fremden Seiten erlaubt
- L9: Reserviert für zukünftige Erweiterungen
- L10: keine Filter aktiv

Bei der Slider-Stellung L10 greift der TrutzBox Proxy nicht mehr in die Kommunikation ein. Bei einer verschlüsselten Verbindung (SSL, https) wird der Proxy komplett umgangen. Bei nicht verschlüsselten Verbindungen durchläuft die Kommunikation zwar noch den Proxy, aber es sind keinerlei Filter aktiv.
In der Standard-Einstellung sind folgende Einstellungen eingestellt:

- Daten-Tracker sind bis Slider-Position L7 geblockt
- Cookies sind zunächst auf allen Level erlaubt, aber
- Cookies von fremden Seiten (Third-Party-Cookies) bis einschließlich L8 geblockt. Dadurch können Webseiten, die ohne Tracker nicht funktionieren, auf L7 angezeigt werden. Die dann aktiven Tracker können allerdings keine Cookies setzen und sind somit meist recht unwirksam.
- Der „user-agent“ Wert des http-Protokolls, mit dem ein Server den Hardware- und Betriebssystem-Typ des Clients ermittelt, ist auf ein „Allerwelts-Profil“ der drei verschiedenen Geräte-Typen Desktop, IOS und Android voreingestellt.
- Der "accept-language" Wert des http-Protokolls ist auf ein „Allerwelts-Profil“ eingestelt.

TrutzBrowse-Blacklists – Implizit aufgerufene Tracker oder Werbung blockieren

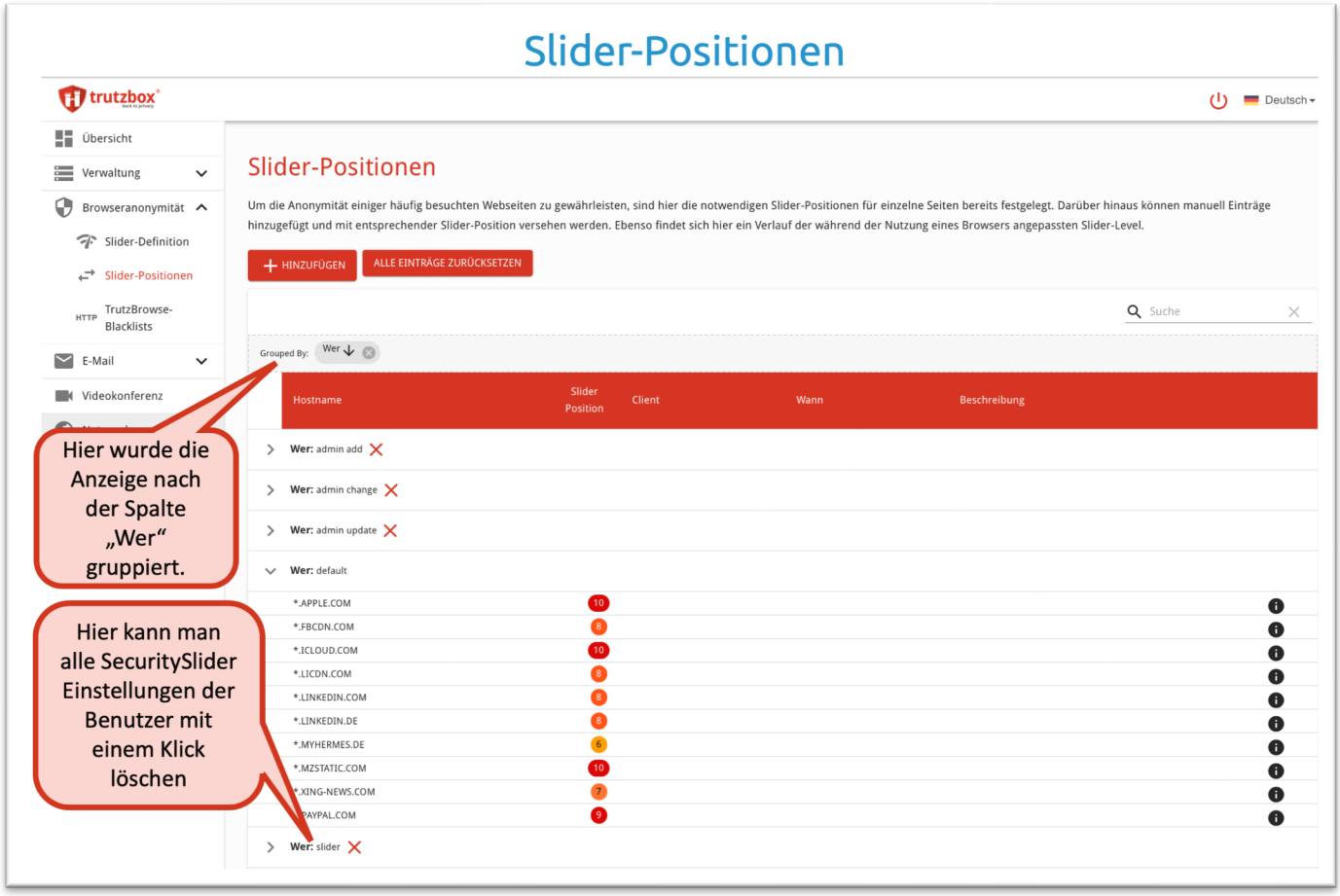
In den allgemeinen Einstellungen der Slider-Definition gibt es die Funktion „Daten-Tracker blockieren“. Standardmässig werden bis SliderPosition 6 Datentracker blockiert. Welche Server hier blockiert werden sollen, kann im Menü TrutzBrowse-Blacklists eingestellt werden. Ähnlich wie auch bei den TrutzContent Filtergruppen Einstellung, werden dazu die zu blockierenden Filterlisten aus einer Liste von Content-Gruppen ausgewählt.



(© 2020 Comidio GmbH)

Slider-Positionen

Für welche Server der Slider schon einmal von seiner Standard-Einstellung 1 verschoben wurde, kann der TrutzBox-Administrator im Menü „Slider-Positionen" sehen und anpassen.

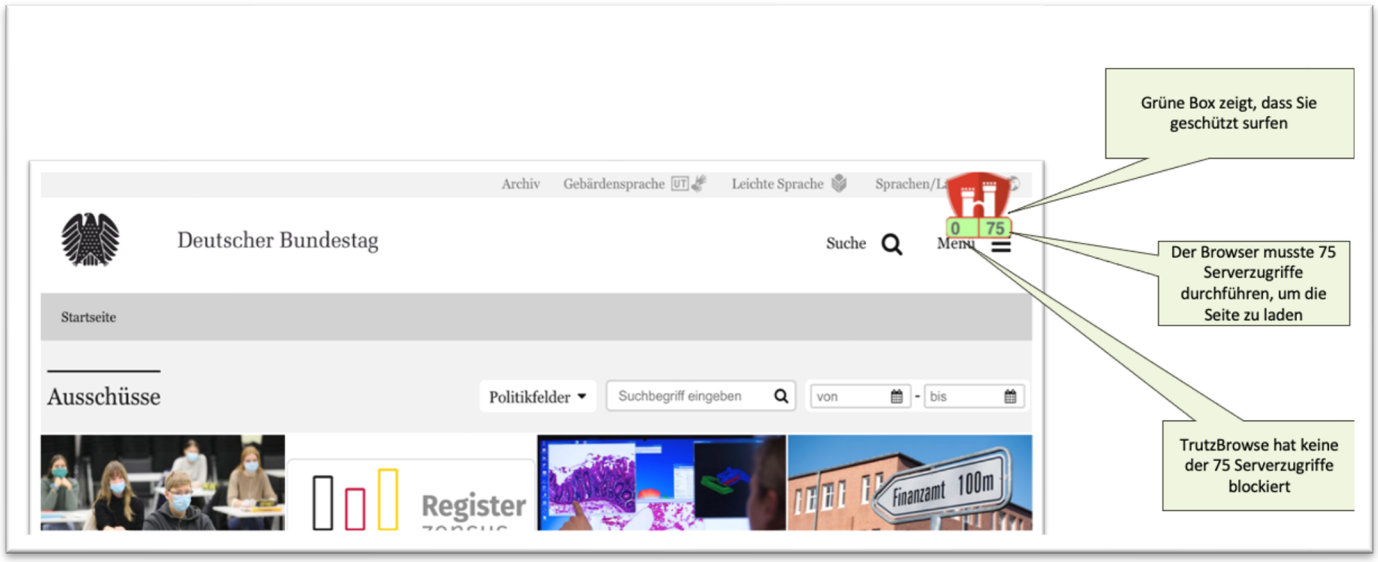


(© 2020 Comidio GmbH)

Durch Ziehen der Überschrift dieser Auflistung in den grauen Balken „Grouped by“ zeigt die Tabelle die Slider-Positionen gruppiert nach dieser Tabellen-Spalte an. So kann man mit der Gruppierung nach „wer“ mit einem Klick alle Einstellungen von einem „Verursacher“ löschen.
Comidio liefert in den Standardeinstellungen für ein paar wenige Webserver ein paar oft benötigte Slidereinstellungen aus. Des Weiteren kann der TrutzBox-Administrator Slider-Einstellungen vornehmen und der Benutzer der TrutzBox ist evtl. auch in der Lage über das eingeblendete TrutzBurg-Symbol im Browser des Anwenders die Position des Sliders zu verändern.
Sämtliche Einstellungen bei TrutzBrowse wirken sich auf alle Geräte und Benutzer der TrutzBox aus. Es ist nicht möglich TrutzBrowse Einstellungen pro Benutzer oder Gerät unterschiedlich zu konfigurieren.
Es ist lediglich möglich, für eine aufgerufene Webseite die TrutzBrowse Filter zu variieren indem der Anwender für diese Webseite den Security-Slider wie gewünscht verstellt. Diese Einstellung für eine Webseite wird gespeichert und wirkt sich auf alle TrutzBox Anwender aus.
Eine Slidereinstellung kann auch unqualifiziert erfolgen, indem linksbündig vor dem „.“ ein „*“ angehängt wird. So kann man nicht nur die Domain „apple.com“, sondern mit „*.apple.com“ auch alle Sub-Domains wie z.B. „cdn.apple.com“ auf eine SecuritySlider-Position stellen.

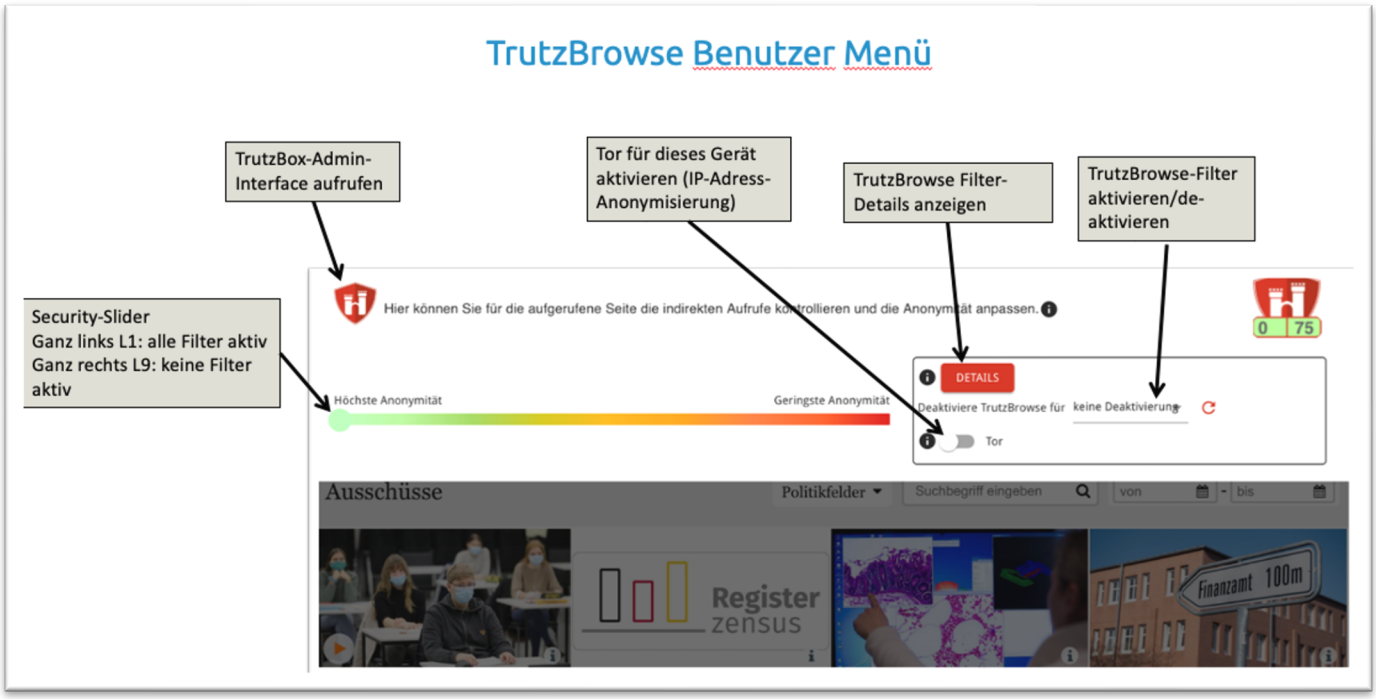
TrutzBurg-Symbol im Browser des Anwenders

Immer wenn beim Surfen TrutzBrowse verwendet und somit die TrutzBox Anonymitätsfunktionen genutzt wurden, zeigt der Browser oben rechts das TrutzBurg Symbol an. Des Weiteren wird auf dem TrutzBurg Symbol angezeigt, ob Tor aktiv ist (also auch die IP-Adresse anonymisiert wurde), wie viele indirekten weitere Server-Zugriffe der Browser benötigte um die Seite zu laden und wie viele Zugriffe dabei auf Tracker-Server komplett blockiert wurden. Die Farbe der SecuritySlider-Box entspricht dem aktuellen Security Level für diese Seite.



(© 2021 Comidio GmbH)

Falls sich Bedienelemente auf der Webseite befinden, die durch die TrutzBurg verdeckt werden und somit nicht mehr bedienbar sind, kann die TrutzBurg auf eine andere Ecke des Browser-Fensters verschoben werden. Bei Touch-Screens dazu einfach das Symbol länger als eine Sekunde berühren.
Eine veränderte TrutzBurg-Position wird pro Seite gespeichert, sodass die TrutzBurg-Position nur einmal angepasst werden muss.
Nach Anklicken der TrutzBurg stehen der Security-Slider und weitere Funktionen zur Verfügung:

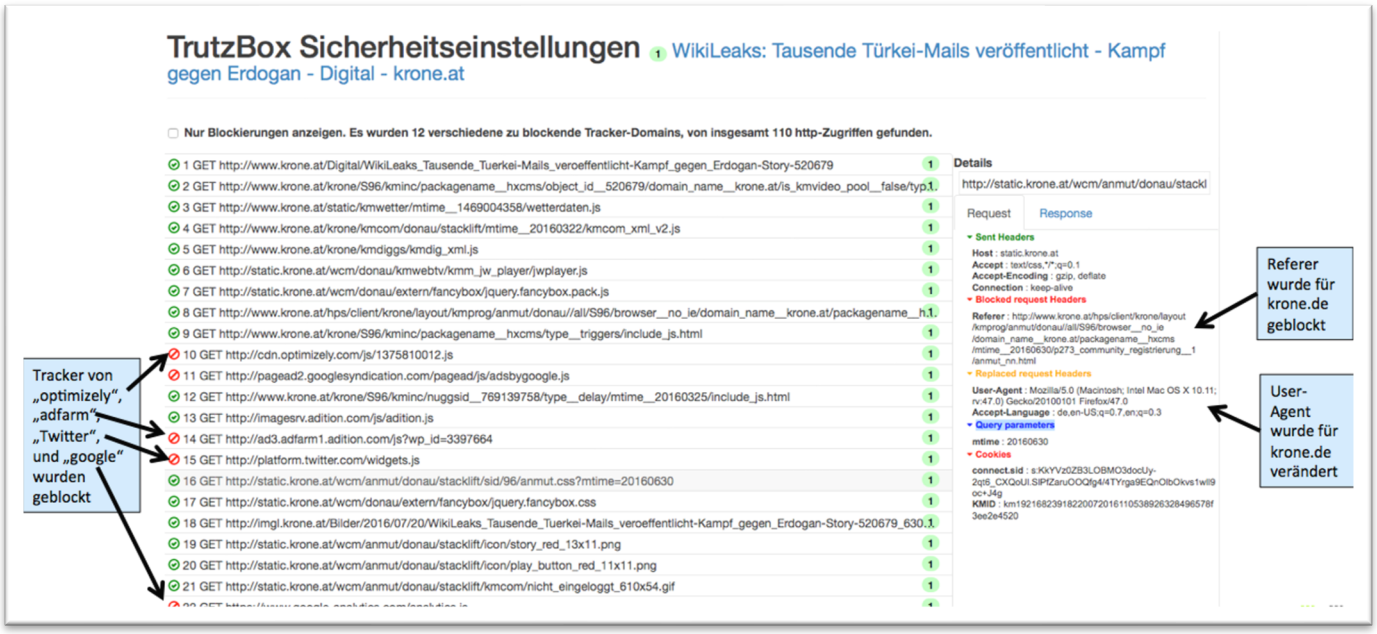


(© 2021 Comidio GmbH)

Standardmäßig steht der Security-Slider ganz links auf Stufe 1 (grün); auf dieser Stufe ist die größtmögliche Sicherheit eingestellt. D.h. alle Sicherheits- und Anonymisierungs-Möglichkeiten der TrutzBox sind aktiv. Falls die Webseite Funktionsstörungen zeigt, weil sie z.B. einen Cookie speichern möchte den TrutzBrowse verhindert, kann der Anwender durch Ziehen des Security-Sliders nach rechts (in Richtung rot) stufenweise einzelne Sicherheits- und Anonymisierungs-Vorkehrungen deaktivieren, um somit die Funktionsfähigkeit der Webseite wiederherzustellen.

TrutzBrowse HTTP-Header-Filter

Bei Aktivierung des Details-Knopfes zeigt TrutzBrowse eine Liste aller von dieser Seite aufgerufenen Web-Zugriffe; hier für einen Artikel der Webseite krone.de (abgerufen am 20.7.2016):

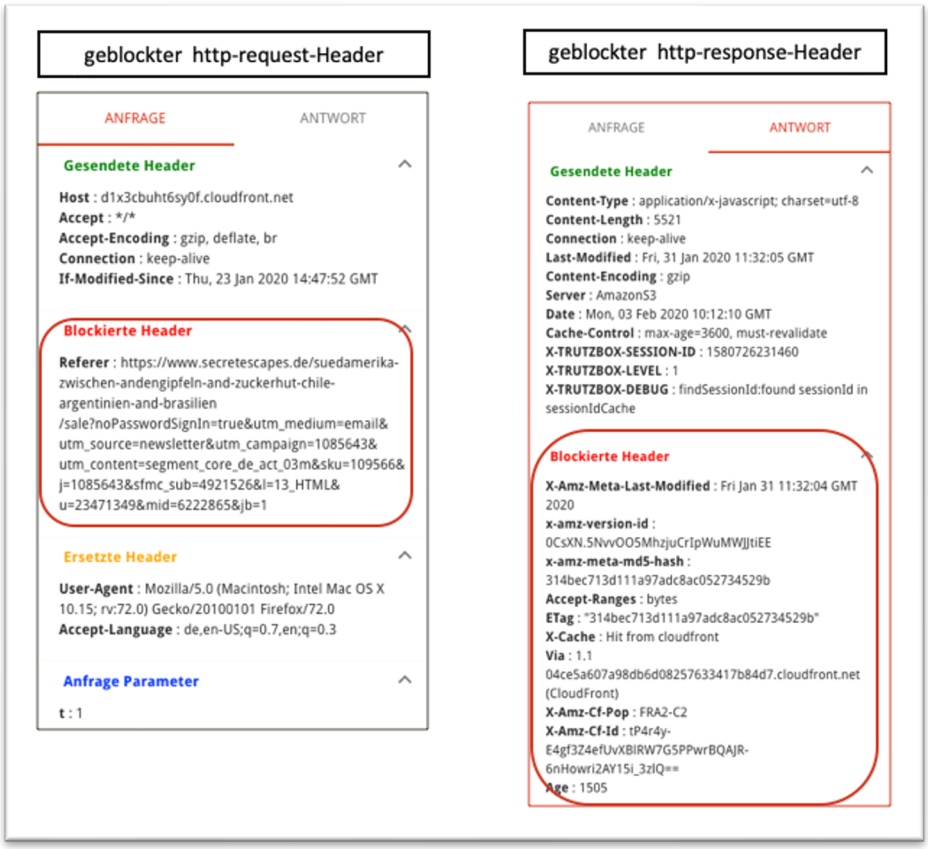


(© 2016 Comidio GmbH)

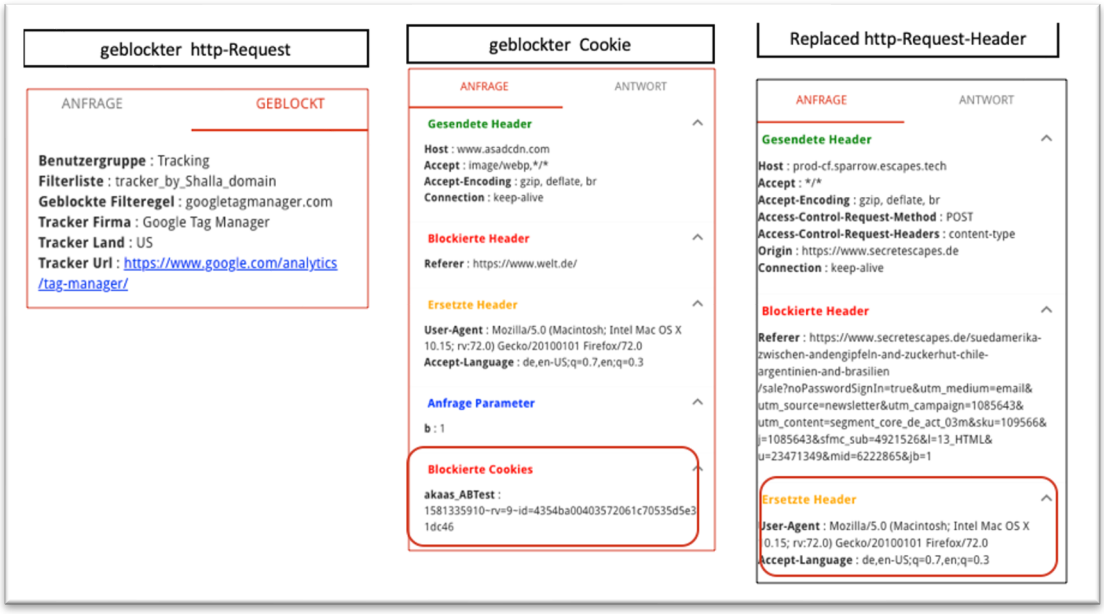
Geblockte HTTP-Aufrufe sind durch ⊘ gekennzeichnet.

Die Übersicht zeigt auch die HTTP-Aufrufe an, die nicht komplett geblockt wurden (durch ✓ gekennzeichnet). Dadurch ist offensichtlich, welche Daten vom Browser an einen Web-Server übermittelt wurden (Tab Request) und welche Daten von einem Web-Server zum Browser gingen (Tab Response).

Für jeden http-Zugriff, werden auf der rechten Seite unter „Details“ die bei jedem Aufruf übertragenen „http-Query Parameter“ und „http-header“ angezeigt. Je nachdem, welche Position des Security-Sliders für diesen Zugriff gilt, werden bestimmte HTTP-Header-Daten gar nicht (Blocked Headers) oder veränderte (Replaced Headers) an den Web-Server übermittelt:



(© 2020 Comidio GmbH)



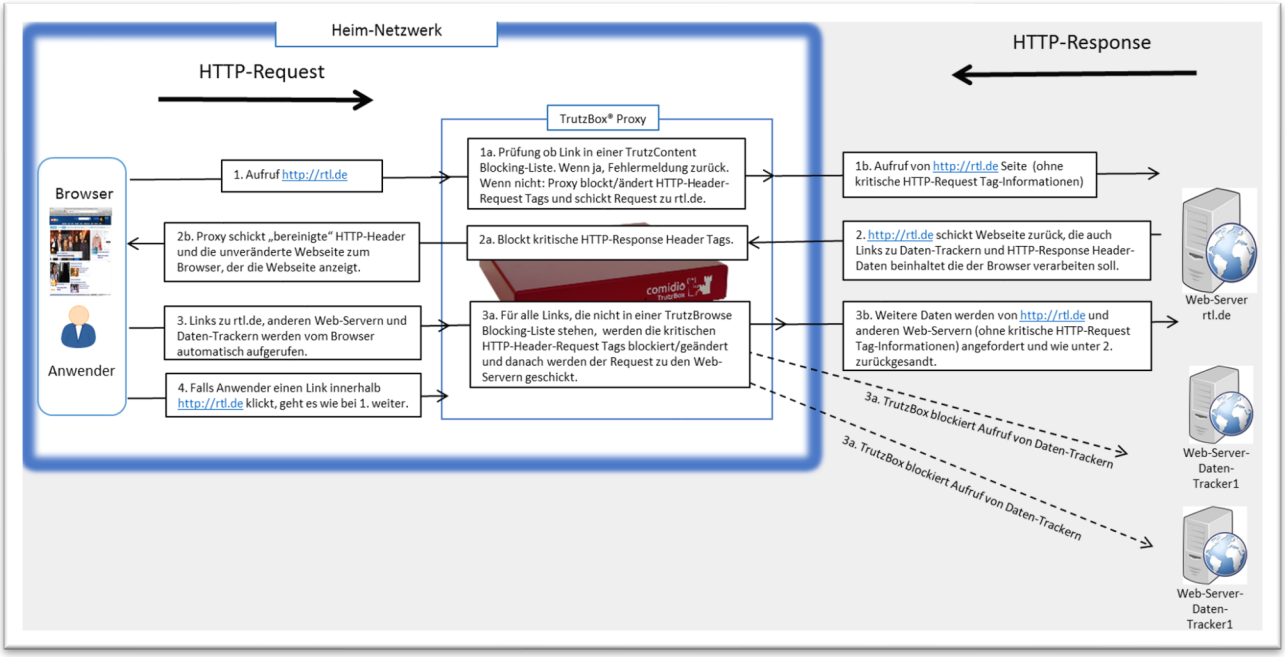
(© 2020 Comidio GmbH)

Dabei haben die Farben der Überschriften folgende Bedeutung:

- Rote Überschriften wie „Blocked request Headers“ oder „Cookies“ bedeuten, dass diese Daten komplett blockiert wurden, also nicht übertragen wurden.

- Grüne Überschriften wie „Sent Headers“ bedeuten, dass diese Daten unverändert übertragen wurden.
- Orange Überschriften wie „Replaced request Headers“ bedeuten, dass der Proxy diese Daten angepasst hat.
- Blaue Überschriften wie „Query parameters“ stehen für die Query-Parameter, die derzeit noch vom Proxy nicht verarbeitet werden.

Bei jedem (erlaubten) Zugriff auf einen Web-Server werden vom Web-Browser über den HTTP-Header Informationen an den Web-Server gesandt (http-request-header). Ohne die TrutzBox würde der Browser diese angeforderten Daten dann unverändert an den Web-Server liefern. Das können sehr persönliche Daten sein, wie z.B. welche weiteren Seiten riefen Sie in der letzten Zeit auf, sind Sie gerade bei Facebook eingeloggt oder wie sieht Ihre PC/Browser Konfiguration genau aus, um Sie bei weiteren Aufrufen wiederzuerkennen. Mit dem HTTP-Header-Filter wird auch das Setzen und Abrufen von Cookies kontrolliert.
Die TrutzBox ist mit ihrer TrutzContent/TrutzBrowse Funktion somit in der Lage, den gesamten HTTP Datenaustausch im Internet zu kontrollieren und zu blockieren bzw. zu verfälschen, soweit diese HTTP-Header-Daten nicht unbedingt benötigt werden.



(© 2015 Comidio GmbH)

Die optimale TrutzBrowse- und TrutzContent-Einstellung

TrutzContent ist immer für alle Geräte aktiviert. TrutzBrowse ist standardmäßig für alle Geräte deaktiviert. Da die TrutzContent-Funktion schon die meisten Tracker und schädlichen Internet-Zugriffe blockiert, muss TrutzBrowse nicht unbedingt aktiviert werden. In den meisten Fällen genügt somit die TrutzContent-Funktion in den Standard-Einstellungen.
Die TrutzBrowse-Funktion ist als zusätzliche Anonymisierungsfunktion zu verstehen. Jedoch sollte man bedenken, dass die Aktivierung von TrutzBrowse für ein Gerät dazu führen kann, dass bestimmte Funktionen bzw. Internet-Verbindungen nicht 100% funktionieren und man einzelne Zugriffe auf der TrutzBox nachjustieren muß.
Die in der TrutzBrowse-Funktion per Default eingestellten Header-Filter basieren auf umfangreichen Comidio Tests. Diese Filterwerte sind je nach Security-Slider-Stellung ein guter Kompromiss zwischen möglichst wenig Funktionalitätseinschränkung bei typischen Webseiten einerseits und Schutz der Privatsphäre andererseits. Um einen Browser wieder erkennen zu können, ist für einen Tracker besonders der Wert im Feld „user-agent“ wichtig. In diesem HTTP-Header teilt der Browser dem Tracker mit, welcher Browser und welches Betriebssystem gerade genutzt wird. Hier sollte möglichst ein Wert eingesetzt werden, der im Internet am häufigsten Verwendung findet. Im Blog „most-common-user-agents“[214] findet man dazu gute Anregungen.
Weitere Hinweise auf HTTP-Header Anonymisierung sind bei der Beschreibung von Squid[215], JonDo[216] und bei Lutz Donnerhacke[217] zu finden.
Auch die standardmäßig eingestellten TrutzBrowse- und TrutzContent-Filterlisten sind Erfahrungswerte, die einen Kompromiss zwischen möglichst hoher Bedienerfreundlichkeit (möglichst wenig den SecSlider verschieben müssen) und hoher Anonymität im Internet darstellen.
Wer noch mehr Anonymität und Schutz im Internet möchte, der kann folgende weitere Punkte „strenger“ einstellen:

- Cookies auch für aufgerufene Seiten auf L1 Sperren

- in der Filtergruppe „Default“ (TrutzContent) zusätzlich die beiden Windows 10 Blacklisten aktivieren.
- in der TrutzBrowse-Blacklist (TrutzBrowse) zusätzlich „Werbung“, die beiden „Kowabit“ und die beiden Windows 10 Blacklisten aktivieren.
- In den Allgemeinen Einstellungen „Falls SSL-Fehler auftreten, Filtering für angesteuerte Domain automatisch ausschalten“ de-aktivieren.
- Im Zugriffsprotokoll regelmäßig überprüfen, ob irgendwelche Geräte immer wieder auf Server des Herstellers zugreifen und diese Zugriffe sperren. Siehe auch Kapitel „Browser und andere Programme daran hindern, dass sie Daten „nach Hause“ liefern“.

[214] https://techblog.willshouse.com/2012/01/03/most-common-user-agents/

[215] http://www.squid-cache.org/Versions/v2/HEAD/cfgman/header_access.html

http://wiki.squid-cache.org/SquidFaq/ConfiguringSquid#Can_Squid_anonymize_HTTP_requests.3F

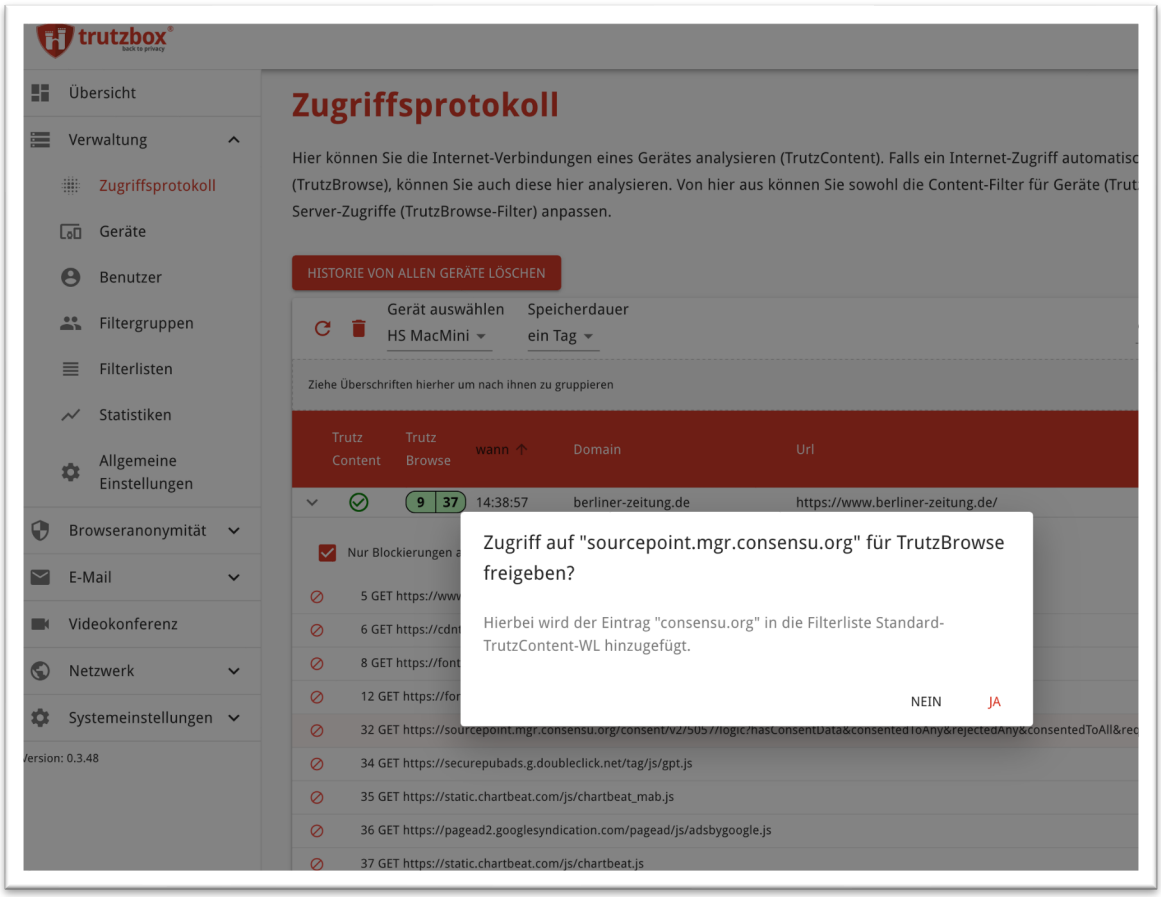
[216] http://ip-check.info/description.php?lang=de

[217] http://altlasten.lutz.donnerhacke.de/mitarb/lutz/anon/web.en.html

Kann die TrutzBox auch zu viel filtern?

Es kann vorkommen, dass die TrutzBox mehr filtert, als der Anwender das wünscht oder so viel, dass eine Anwendung (App) oder der Seitenaufbau im Browser nicht mehr richtig funktioniert.
In diesem Fall kann der Anwender meist über den SecuritySlider im Browser, die an den Server gelieferten Daten so weit anpassen, dass das Problem gelöst wird. Wenn man den SecuritySlider allerdings weiter als Level7 zieht, werden alle Tracker zugelassen. Es kann allerdings manchmal sinnvoll sein, dass man lediglich einen Tracker zulassen möchte.

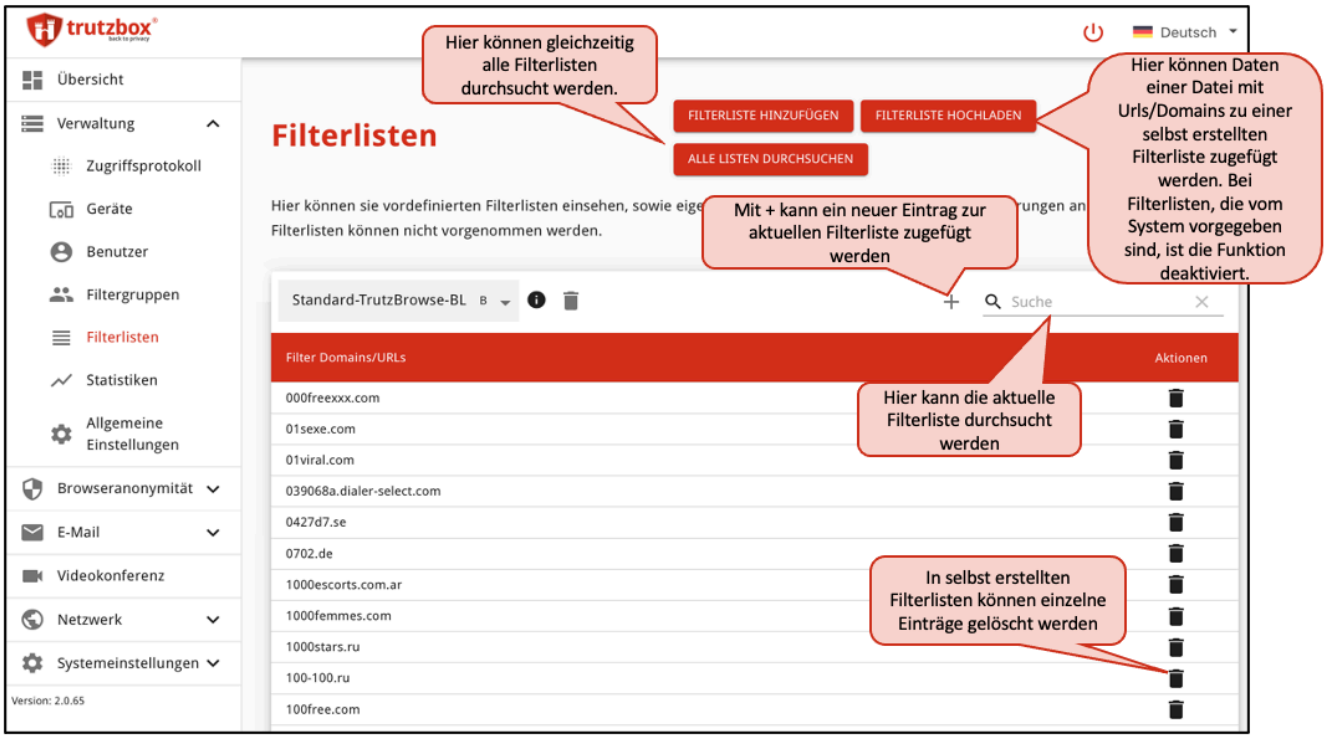
Es kann aber auch vorkommen, dass weitere Anpassungen der TrutzBox-Filter notwendig sind, die ein Anwender nicht durchführen kann. Manche Filter-Anpassungen kann nur der TrutzBox-Administrator vornehmen.
Dazu hier ein Beispiel: in den Standard-Einstellungen werden evtl. auch Consent-Management-Links geblockt. Unter Consent-Management versteht man das Einverständnis des Benutzers, z.B. die Benutzung von Cookies einzuholen (also einen Konsens finden). Wenn der Entwickler der Webseite, diese Funktion an eine Firma ausgelagert hat, die evtl. den Benutzer tracken könnte, dann kann es vorkommen, dass der Link zu diesem Dienstleister von der TrutzBox blockiert wird. Dann wird dem Benutzer evtl. nicht mehr die Frage nach der Benutzung von Cookies angezeigt, Das kann der TrutzBox-Administrator im Menü „Zugriffsprotokoll“ sehen. Wenn er möchte, kann er diese Blockierung aufheben und der Nutzer der Webseite würde die Consent-Anfrage wieder bekommen.
In diesem Beispiel unten nutzt berliner-zeitung.de den Dienstleister consensu.org für das Consent-Management, das die TrutzBox blockiert. Durch Klick auf das ⊘ Symbol des blockierten Aufrufs von sourcepoint.mgr.consensu.org, kann der TrutzBox-Administrator die Domain sourcepoint.mgr.consensu.org in die Standard_TrutzConent-WL eintragen und somit frei geben.



TrutzBox Filterlisten

Unter dem Menüpunkt „Verwaltung“ -> „Filterlisten“ kann der TrutzBox Administrator einzelne Filterlisten, die Internet-Domains oder Internet-URLs beinhalten, verwalten. Comidio liefert dazu ca. 110 Filterlisten, die 55 unterschiedliche Internet-Themengebiete beinhalten, aus. Diese Filterlisten werden von Comidio eingekauft und dazu in kurzen Zeitabständen auf die TrutzBoxen überspielt. Der Administrator ist mit diesem Menüpunkt in der Lage, diese von Comidio ausgelieferten Standardlisten einzusehen, sie zu durchsuchen oder eigene, neue Black- und White-Listen zu erstellen.
Zusätzlich liefert Comidio zusätzlich eigene Blocking-Listen aus.
Die von der TrutzBox verwalteten Filterlisten finden sowohl bei TrutzBrowse als auch bei TrutzContent Verwendung:

Filterlisten –
Liste von Server-Domains oder URLs die Gesperrt (Blacklist) oder frei gegeben werden sollen (Whitelist)



(© 2021 Comidio GmbH)

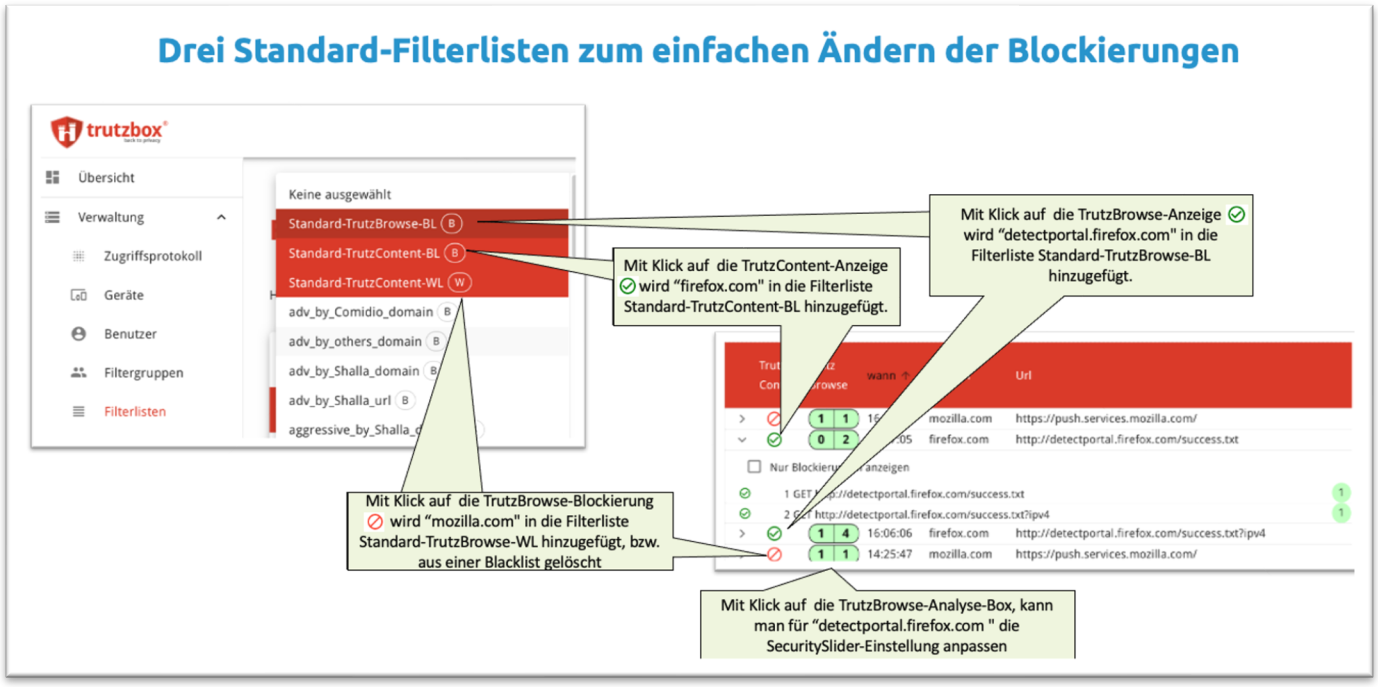
Im Menü „Filterlisten“ können vom TrutzBox Administrator auch selbst neue Black- und White-Listen angelegt werden, die dann sowohl bei TrutzBrowse als auch bei TrutzContent verwendet werden können. Des weiteren kann eine solche Filterliste auch in den Geräte- und Benutzereinstellungen als Whitelist zugefügt werden.
Bei den täglichen automatischen Systemupdates durch Comidio werden nur Standard-TrutzBox Black-Listen angepasst, die selbst verwalteten Listen werden dadurch nicht verändert.
Bei selbsterstellten Filterlisten können sowohl Einträge manuell editiert als auch Listen komplett gelöscht, oder durch Upload einer Datei mit vielen Einträgen ergänzt werden.
Einträge in den Black- und Whitelists dürfen keine unqualifizierten Angaben beinhalten, da hier lediglich ein Stringvergleich durchgeführt wird. Sollen z.B. alle Domains gesperrt werden, die mit facebook.com enden, dann nur facebook.com eintragen. Bitte auch nicht „http“ vor die Domain schreiben, da der Vergleich nur auf die URL wirkt.
Wie in diesem Kapitel beschrieben, bietet die TrutzBox sehr viele Möglichkeiten, den Datenverkehr zwischen einem Gerät und einem Internet-Server zu kontrollieren. Aber es gibt weitere unzählige Möglichkeiten, im Internet ausgespäht zu werden. Noch sind nicht alle dieser technischen Varianten in TrutzBrowse abgebildet. Comidio vertritt den Standpunkt, dass eine vollständige Abdeckung aller Ausspähungsvarianten nicht praktikabel ist, weil sich auch die technischen Möglichkeiten potentieller Datendiebe immer weiterentwickeln.
Aber Comidio ist angetreten, sich diesem Hase-Igel-Spiel zu stellen und den TrutzBox Nutzern weitere Analyseverfahren und zusätzliche Blockungs-Varianten sukzessive als TrutzBox Updates auszuliefern.

Drei Standard TrutzBox Filterlisten

Es gibt drei Filterlisten mit besonderen Eigenschaften, die vom TrutzBox-Administrator angepasst werden können. Alle drei Filterlisten beginnen mit dem Namen „Standard“:

- **Standard-TrutzBrowse-BL**: diese Liste ist als „TrutzBrowse-Blacklist“ aktiviert. Wenn die TrutzBox einen impliziten Zugriff auf einen Server anzeigt, kann man diesen Server direkt mit einem Klick sperren, indem die Url/Domian in diese Liste übernommen wird.
- **Standard-TrutzContent-BL**: diese Liste ist in der Filtergruppe „Default“ aktiviert. Wenn die TrutzBox einen Zugriff auf einen Server anzeigt, kann man diesen Server direkt mit einem Klick sperren, indem die Url/Domian in diese Liste übernommen wird.
- **Standard-TrutzContent-WL**: diese Liste ist bei allen Geräten und Benutzern als Ausnahme aktiviert (Whitelist). Wenn die TrutzBox einen impliziten oder direkten Zugriff auf einen Server blockiert, kann man diesen Server direkt mit einem Klick frei geben (entsperren), indem die Url/Domian in diese Liste übernommen wird.

Der TrutzBox-Administrator kann diese Listen im Menü „Filterlisten“ verwalten oder im Menü „Zugriffsprotokoll“ ist es einfacher möglich, in die richtige Liste einen Eintrag vorzunehmen. Dazu können einzelne TrutzBrowse/TrutzContent-Symbole direkt angeklickt werden.



(© 2021 Comidio GmbH)

Welchem Browser kann man am meisten vertrauen?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Mindeststandard nach §8 BSI-Gesetz (BSIG) zum Thema sichere Web-Browser veröffentlicht[218]. Leider berücksichtigen die vom BSI festgelegten Anforderungen nicht, ob und in welchem Umfang der Browser Benutzer-Daten an den Hersteller übermittelt.
Alle Standard Browser sind nicht nur sehr „mitteilungsbereit“ gegenüber einem Server, sie schicken auch von sich aus, regelmäßig oder sogar bei jedem Seitenabruf, Nutzungsdaten des Anwenders an ihre „Erschaffer“.
So meldet sich z.B. **FireFox** unbeobachtet vom Anwender[219] (stand 2020), bei

- self-repair.mozilla.org,
- telemetry.mozilla.org,
- shavar.services.mozilla.com (Shavar spricht Google's safe-browsing protocol),
- safebrowsing.google.com,
- safebrowsing.google.de,
- safebrowsing-cache.google.com.

Safari meldet Daten zu Apple, **Internet-Explorer** zu Microsoft und **Chrome** tauscht Daten mit mehreren Google-Servern aus. Selbst der angeblich so anonyme Browser CLIQZ[220], der auch auf dem Firefox Code basiert, tauscht regelmäßig Daten mit seinen Erschaffern aus. Selbst der angeblich sehr Daten-Sparsame Browser „Brave“, ist in seinen Standardeinstellungen sehr kommunikationsfreudig und sendet Daten an den Hersteller und an Google[221].
Aber genauso „gesprächig“ sind die Standard Browser beim Surfen. Bereitwillig geben sie IP-Adresse und Informationen über den PC oder das Smart-Phone des Anwenders an jeden im Internet weiter, der sich dafür interessiert. Und genau mit diesen Daten werden dann Profile des Anwenders erstellt. Somit lässt sich feststellen, dass es zwischen den Standard-Browsern kaum Unterschiede bzgl. der Geheimhaltung persönlicher Daten gibt. Dazu kommt noch, dass jeder Browser mittlerweile ein sehr komplexes Software-Produkt ist, das auch Sicherheitslücken haben kann[222].
Es ist zwar möglich, diese Standard Browser mit entsprechenden Plugins etwas weniger auskunftsfreudig zu konfigurieren, aber bei der Menge an Möglichkeiten und Parametern, ist es selbst für einen Experten sehr schwierig, hier die optimalen Plugins und die richtigen Einstellungen zu finden. Allerdings gibt es glücklicherweise kostenlose Browser, für die die von sich aus erst mal keine Daten an ihre Hersteller liefern. Das sind z.B. Chromium, Iridium, Librewolf und der Tor-Browser.
Mittlerweile haben zwar fast alle Browser Funktionen eingebaut die das Tracking erschweren sollen[223], jedoch zeigen Tests, die Comidio regelmäßig durchführt, dass diese mehr oder weniger nutzlos sind.

[218] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Mindeststandard-sichere-Webbrowser_13042017.html

[219] https://support.mozilla.org/de/kb/Firefox-baut-unaufgeforderte-Verbindungen-auf

[220] https://cliqz.com/

[221] https://www.kuketz-blog.de/brave-datensendeverhalten-desktop-version-browser-check-teil1/

[222] http://www.heise.de/security/meldung/Mozilla-verlangt-vom-FBI-Informationen-ueber-potenzielle-Sicherheitsluecken-im-Tor-Browser-3207142.html?wt_mc=nl.heisec-summary.2016-05-16

[223] https://webkit.org/blog/7675/intelligent-tracking-prevention/

Im Kuketz-Blog werden regelmässig alle gängigen Browser auf ihr Datenschutzfreundliches Verhalten hin untersucht[224].

Browser und andere Programme daran hindern, dass sie Daten „nach Hause“ liefern

Sowohl fast alle Internet-Browser, als auch sonstige Apps, liefern recht häufig Tracker-Daten ungefragt an ihre Hersteller. So nehmen fast alle Fernseher regelmäßig Kontakt mit dem Hersteller auf und teilen ihm den aktuellen Standort des Fernsehers mit oder holen sich dort Updates. Der Firefox Browser kontaktiert in recht kurzen Zeitabständen Mozilla, der Internet-Explorer/Edge-Browser kontaktiert Microsoft und der Chrome-Browser liefert regelmäßig Daten an Google.
Das alles kann man im TrutzBox-Menüpunkt „Zugriffsprotokoll“ sehen, wenn die Datenkommunikation über die TrutzBox geleitet wird. Dort kann man auch direkt einen solchen ungewollten Serverzugriff in die Blacklist „Standard-TrutzContent-BL“ übernehmen.

Hier eine Liste von Domains, die zumindest die meisten Verbindungen des Firefox und Chrome-Browsers unterbindet:

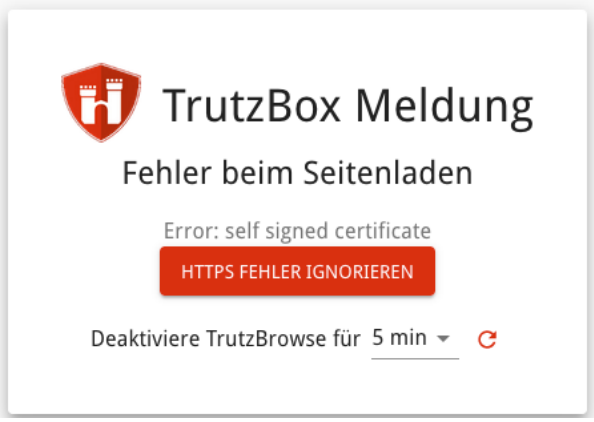
- *telemetry.mozilla.org*
- *google-analytics.com*
- *gameanalytics.com*
- *firebaseio.com*
- *detectportal.firefox.com*
- *telemetry.mozilla.org*
- *shavar.services.mozilla.com*
- *safebrowsing.google.com*
- *safebrowsing.googleapis.com*
- *getpocket.cdn.mozilla.net*
- *img-getpocket.cdn.mozilla.net*

Verschlüsselte Browser (SSL)-Verbindungen

Immer mehr Web-Server unterstützen eine verschlüsselte Verbindung mit dem Browser (SSL/TLS). Das ist gut so, damit niemand, der Daten zwischen Browser und Web-Server abfangen kann in der Lage ist, Daten mitzulesen oder sogar zu manipulieren. Dadurch wird das Surfen im Internet sicherer.

[224] https://www.kuketz-blog.de/tag/browser/

Da die TrutzContent-Funktion lediglich prüft ob ein Link aufgerufen werden darf und dazu nicht in die übertragenden Daten rein schauen muß, hat TrutzContent auch kein Problem mit verschlüsselten Daten. Die TrutzBrowse-Funktion kann jedoch den Datenstrom zwischen Browser, App oder IoT-Gerät und einem Server im Internet analysieren und anonymisieren. Eigentlich wäre die TrutzBox nicht in der Lage, diese verschlüsselten Daten zu analysieren, da die Verschlüsselung Ende-zu-Ende stattfindet, also zwischen Web-Browser und Web-Server. Um eine Datenanalyse dennoch zu ermöglichen, verhält sich die TrutzBox zu dem Browser des Teilnehmers wie ein Server und baut in diesem Fall auf der einen Seite eine verschlüsselte Verbindung zum Browser (Proxy-Funktion) und zur anderen Seite zum Web-Surfer auf. Dies ist eigentlich typisch für einen „Man-in-the-Middle“ Angriff. Allerdings stellt ein der TrutzBox zugeordnetes Root-Zertifikat sicher, dass die Verbindung vom Endgerät als Sicher anerkannt wird.
Nur für Geräte bzw. Browser, bei denen es möglich ist das TrutzBox-Root-Zertifikat zu importieren, kann die TrutzBrowse Analyse der ausgetauschten Daten durchgeführt werden. Für Geräte, bei denen kein Root-Zertifikat importiert werden kann, sollte man TrutzBrowse in der Geräte-Verwaltung abschalten.
Wenn die TrutzBrowse Funktion aktiv ist, verhält sich die TrutzBox gegenüber dem Server wie ein Browser und akzeptiert alle ihr bekannten Zertifikate (genauer gesagt, sie akzeptiert alle Zertifikate, die mit einem ihr bekannten Root-Zertifikat signiert wurden). Die Liste der Root-Zertifikate, die die TrutzBox im Namen des Nutzers akzeptieren soll, kann der Benutzer in der TrutzBox derzeit noch nicht selbst verwalten. In der Grundeinstellung sind alle Root-Zertifikate, die durch den Debian-Update automatisch verteilt werden geladen. Dadurch werden sie auch von der TrutzBox akzeptiert. Die Liste dieser Stamm-Zertifikate wird von der TrutzBox regelmäßig aus dem Debian „ca-certificates Paket“[225] übernommen.
Falls die TrutzBox ein Server-Zertifikat nicht als vertrauenswürdig erkennt, wird der Anwender gefragt, ob er trotzdem diese Seite laden möchte. Solche Zertifikats-Fehler können mit badssl.com sehr gut simuliert werden.



(© 2021 Comidio GmbH)

Wenn ein solcher Fehler von einem Browser erkannt wird, kann man den Fehler ignorieren oder TrutzBrowse für eine ausgewählte Zeit ausschalten.

[225] https://packages.debian.org/de/jessie/ca-certificates

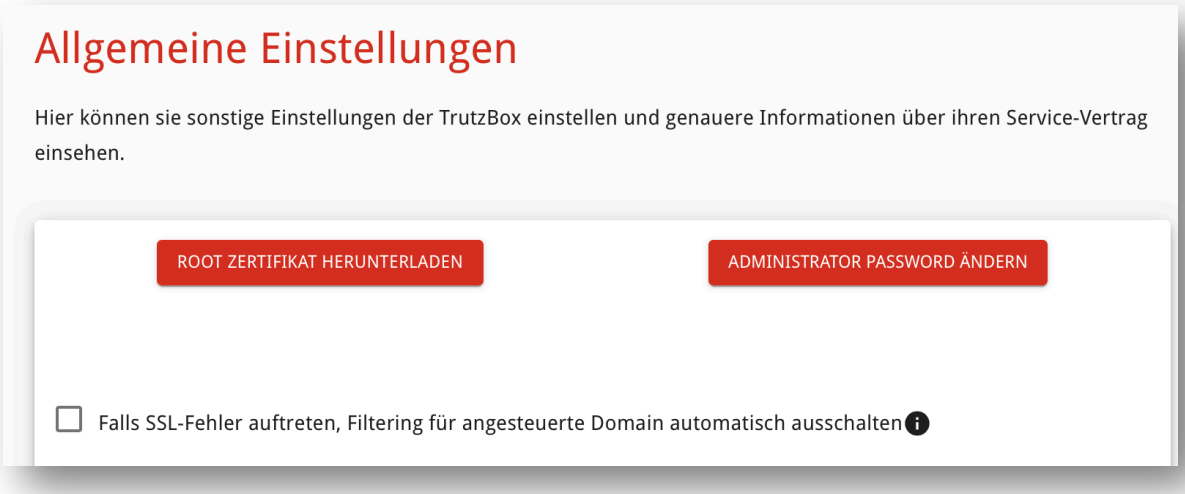
Was muss auf Client- bzw. auf Geräte-Seite sichergestellt werden, damit die TrutzBox verschlüsselten Datenverkehr analysieren kann (TrutzBrowse)?

Die TrutzBox generiert beim Setup der TrutzBox ein Root-Zertifikat (Stamm-Zertifikat), das über die TrutzBox Bedienoberfläche heruntergeladen werden kann. Jede von einem Gerät angesteuerte Webseite, wird von der TrutzBox (genau genommen vom Proxy der TrutzBox) mit diesem Root-Zertifikat signiert, bevor die Daten an den Client weiter geleitet werden. Dieses Root-Zertifikat sollte bei Nutzung von TrutzBrowse dem Client-Programm bekannt sein. Wenn der Client dieses Root-Zertifikat kennt wird verhindert, dass der Browser oder andere Programme wie z.B. ein E-Mail-Client bei jeder Verbindung zur TrutzBox nachfragen muss, ob diese Verbindung vertrauenswürdig ist.
Leider verwaltet jedes Betriebssystem und jedes Programm auf Client-Seite diese Root-Zertifikate unterschiedlich. Somit ist es in manchen Fällen nicht nur notwendig, das TrutzBox Server-Zertifikat auf jedes Gerät zu laden, sondern abhängig davon, welcher Browser und welches Mail-Programm benutzt wird, muss das Zertifikat evtl. auch noch zusätzlich, einmalig in ein Programm importiert und bestätigt werden.
Glücklicher weise nutzen die meisten Programme den Zertifikatsspeicher des Betriebssystems. Dann muss es nur einmalig in den Zertifikatsspeicher des Betriebssystems geladen werden. Die Software von Mozilla nutzen jedoch einen eigenen Zertifikatsspeicher. Sowohl der Firefox-Browser als auch der Thunderbird Mail-Client, verwalten ihre Root-Zertifikate selbst.
Diese Übersicht zeigt, welche Programme die Zertifikate selbst verwalten und welche den zentralen Schlüsselbund des Betriebssystems nutzen:

	Mac OS							Windows							Android				IOS		
	Browser			Mail			App	Browser				Mail		Apps	Browser		Mail	Apps	Browser	Mail	Apps
	Safari	Firefox	Chrome	Apple Mail	Thund erbird	Outlook	z.B. App Store	Internet Explorer (IE)	Firefox	Edge	Chrome	Thund erbird	Outlook		Chrome	Firefox		Play-store			App-Store
Zertifikat wird vom System-Schlüsselbund genommen	x		x	x				x		x	x		x		x		x		x	x	
Zertifikat muss extra in die Applikation geladen werden		x							x							x mit extra Plugin					
Zertifikat muss nur beim ersten Mal bestätigt werden				x	x	x						x									
Zertifikat ist in der App fest eingestellt und akzeptiert kein anderes Zertifikat							x							x				x			x
Bemerkungen	Mit dem Konsolen-Befehl: open -a "Google Chrome" --args --proxy-pac-url="https://trutzbox/api/proxy/pac" kann man Chrome auch mit Nutzung des Proxies öffnen, ohne dass Chrome die System-Einstellungen für den Proxy nutzt. Wenn man in Chrome den Befehl: chrome://net-internals/#proxy absetzt, dann kann man sehen, ob der Proxy aktiv ist. Wenn der Proxy aus irgendeinem Grund nicht funktioniert, schaltet chrome auf direct-mode um (anders als in firefox).																				

Apps auf Smartphones (nicht Browser), die eine Verbindung immer zu ihrem gleichen Server aufbauen, haben das Zertifikat des Servers, mit dem sie kommunizieren, oft fest im Programm einprogrammiert. Das Zertifikat kann die TrutzBox nicht ändern und auch nicht mit dem TrutzBox-Root-Zertifikat signieren und somit ist es für die TrutzBox technisch nicht möglich, die Daten zu entschlüsseln.
Die TrutzBox hat in diesem Fall zwei Möglichkeiten:
- die Verbindung standardmäßig nicht erlauben, also sperren und es dem TrutzBox Administrator frei stellen, den angesteuerten Server frei zu schalten
- oder die Verbindung erst mal zu erlauben und es dem TrutzBox Administrator frei stellen, den angesteuerten Server zu sperren

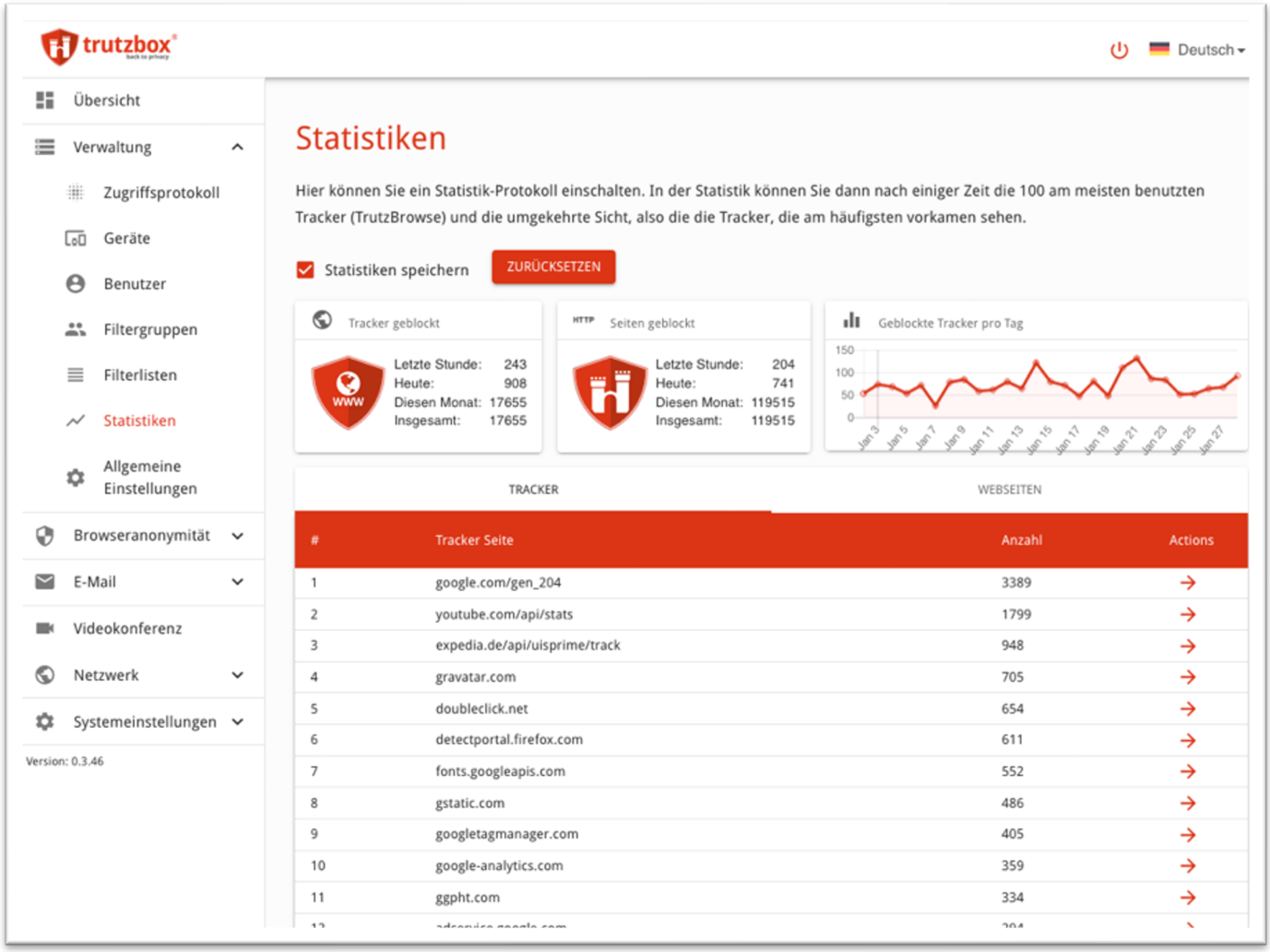
Welche dieser beiden Alternativen gewünscht wird, wird im TrutzBox-Menü „Allgemeine Einstellungen“ durch den Schalter "Falls SSL-Fehler auftreten, Filtering für angesteuerte Domain automatisch ausschalten", gesteuert.



Standardmäßig ist dieser Schalter so gesetzt, dass im Falle, dass die TrutzBox solche verschlüsselte Verbindungen nicht aufbrechen kann, der aufgerufene Server automatisch auf L10 gesetzt wird. Beim zweiten Versuch auf diesen Server zuzugreifen, wird das dann auch funktionieren. So ist die Administration der TrutzBox einfacher.
Sie können diesen Schalter auch deaktivieren. Dann kann es aber vorkommen, dass Sie, um die Funktionsfähigkeit einer App herzustellen, einen verschlüsselten Zugriff manuell auf L10 setzen müssen. Das ist etwas sicherer, aber auch etwas höherer administrativer Aufwand.

TrutzBrowse- / TrutzContent Statistiken

Tracker sind besonders effektiv, wenn sie uns beim Surfen im Internet über längere Zeit und damit auch webseitenübergreifend beobachten können. Erst dann ergibt sich für einen Tracker ein umfassendes Benutzerprofil mit vielen Eigenschaften und Interessen des Nutzers. Um den Nutzen und die Effektivität der TrutzBox besser sichtbar zu machen, bietet die TrutzBox eine Übersicht, über alle geblockten Tracker in einem bestimmten Zeitraum an (Tracker-Statistik). Standardmässig ist die Statistik deaktiviert und muß, falls gewünscht, vom Administrator zunächst aktiviert werden.
Mit Hilfe dieser Statistik-Übersicht kann man erkennen, welche Tracker am häufigsten geblockt wurden (linke Spalte) und somit das umfangreichste Nutzer-Profil erstellt hätten, wenn die TrutzBox das nicht verhindert hätte. Die Statistik-Übersicht zeigt auch, welche Webseiten am meisten Tracker beinhaltet hatten (rechte Spalte).
Hier ein Beispiel über eine Laufzeit von ca. 2 Monaten. Erstaunlich ist die riesige Anzahl geblockter Tracker (TrutzBrowse) von über 17.000 und über 119.000 geblockten Server-Zugriffen (TrutzContent) für einen einzelnen Internet Benutzer:



(© 2020 Comidio GmbH)

Bei Aktivierung des Pfeils rechts neben eines Trackers, werden alle Webseiten mit diesem Tracker aufgelistet. Beim Aktivieren des Pfeils rechts neben der Webseite, werden alle jemals gefundenen Blockungen dieser Webseite aufgelistet.

TrutzBrowse/TrutzContent interner Aufbau

Um die http-Zugriffe kontrollieren zu können, werden Zugriffe, die über die TrutzBox geleitet werden, vom TrutzBox-Proxy analysiert und mit den aktivierten TrutzBox Filtern abgeglichen. Ein Proxy (engl. „Stellvertreter“) ist, allgemein erklärt, eine Funktion, die stellvertretend für den Browser eine Webseite beim Server anfordert und diese an den Browser weiter gibt.
Nach intensiven Tests mit Open-Source Proxys wie Apache-Traffic-Server, Privoxy, Squid, ModSecurity u.a. kam Comidio zu dem Schluss, dass keiner dieser Open-Source Proxy-Alternativen den hohen Anforderungen bzgl. Anonymisierungsgrad, Performance, Ressourcen-Verbrauch, Bedienung durch Technik-Laien und benötigten Features, genügen würde. Aus diesem Grunde wurde von Comidio

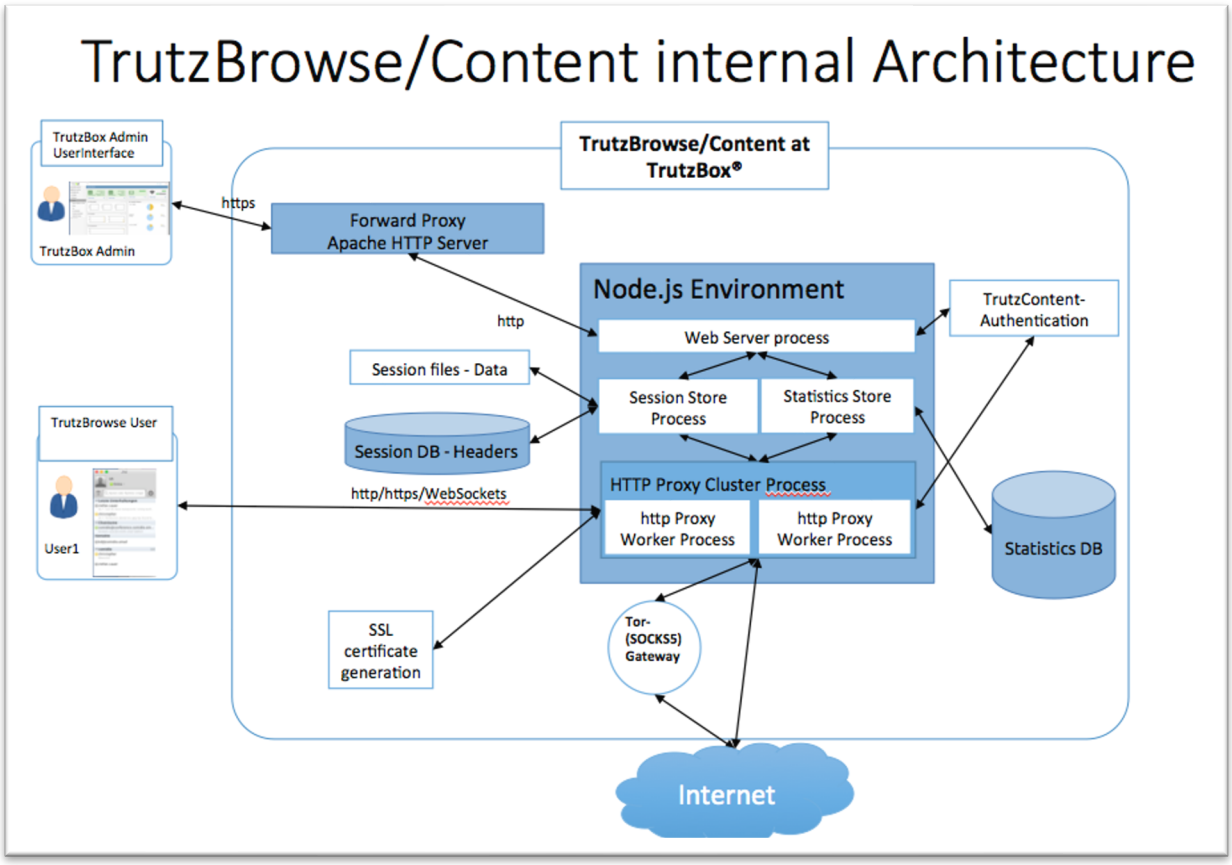
eine auf node.js[226] Server-Technology basierende Lösung selbst entwickelt. Nur durch diese eigene Implementierung war Comidio in der Lage, einen so leistungsfähigen und doch einfach zu bedienenden Anonymisierungs-Proxy zur Verfügung zu stellen. Um z.B. den „Intelligenten Security-Slider“ zu entwickeln, mit dem auch ein Laie in der Lage ist, ganz einfach die Sicherheitseinstellung für eine aufgerufene Webseite nach Bedarf zu korrigieren.
Um die Einstellungen des Proxys für den TrutzBox Administrator (TrutzBox Userinterface) und die Bedienung dieser Einstellungen durch den Benutzer (SecuritySlider) möglichst benutzerfreundlich zu gestalten, wurde das TrutzBox UserInterface und der SecuritySlider eng mit dem Proxy integriert.
Neben der Generierung der SSL-Zertifikate, der Kontrolle der jeweilig zu blockierenden Seiten und der Anpassung der http-Header übernimmt dieser auch:

- die Authentisierung eines Benutzers beim: Admin-Login und TrutzContent auf Benutzerebene
- die Browser-Sessions, um die Browser Zugriffe im SecSlider anzuzeigen und in Status zu speichern
- die SecSlider Positionen für die jeweiligen Webserver
- die Unterscheidung, ob ein Server bewusst (TrutzContent) oder indirekt (TrutzBrowse) aufgerufen wurde und nutzt dazu die jeweilig eingestellten Blocking-Listen
- für verschlüsselte (TLS) Zugriffe die Daten entschlüsselt, für den aufgerufenen Server einen neuen Schlüssel generiert und die Seite damit neu verschlüsselt an den Browser liefert
- das Sammeln der Statistikdaten

Gerade bei verschlüsselten Webseiten stellt dieser ganze Vorgang eine erhebliche Ressourcenbelastung für die Proxy-Hardware dar. Deswegen ist es umso wichtiger, dass die Proxy-Hardware über genügend Rechenpower verfügt. Das ist bei der TrutzBox-Hardware der Fall, zumal diese zusätzlich auch noch über eine AES-NI Unterstützung auf Prozessor-Ebene verfügt[227], die gerade die Ver- und Entschlüsselung beschleunigt und den Prozessor entlastet.
Um eine bessere Ausfallsicherheit und den Zugriffs-Durchsatz zu erhöhen, wurde der eigentliche http-Proxy, der die angeforderten http-Zugriffe durchführt, mehrfach instanziiert.

226 http://nodejs.org

227 https://de.wikipedia.org/wiki/AES_(Befehlssatzerweiterung)



(© 2015 Comidio GmbH)

Der TrutzBox-Proxy schreibt seine Logs in diese Files:
/var/log/comidio/proxyServer.log
/var/log/comidio/statisticsServer.log
/var/log/comidio/trutzbox-node.log
/var/log/comidio/webServer.log

TrutzMail – derzeit die wohl sicherste und am einfachsten zu bedienende E-Mail

Wie in den vorangegangenen Kapiteln bereits dargestellt worden ist, sollte vor allem der E-Mail-Verkehr sehr sicher verschlüsselt und die Identität des Absenders eindeutig erkennbar sein. Die derzeit in fast allen Mail-Programmen angebotene E-Mail-Verschlüsselungslösungen basieren alle auf PGP[228] oder S/MIME[229]. Sowohl PGP als auch S/MIME Lösungen, sind zwar bei sachgemäßer Verwendung recht sicher, aber kompliziert und umständlich anzuwenden. Vor allem die Verwaltung der Schlüsselpaare stellt im täglichen Gebrauch, nicht nur für den Technik-Laien, oft eine zu große Komplexität dar.
PGP und S/MIME E-Mail-Verschlüsselung ist deswegen in der Bedienung zu kompliziert, da der Benutzer zunächst einmal eine funktionale Erweiterung (Plugin) in seinem E-Mail-Programmen installieren muss. Und das auf allen seinen Geräten. Er muss deren zusätzliche Funktionalität verstehen und ein eigenes Schlüsselpaar generieren und verwalten. Schließlich muss er auch noch die öffentlichen Schlüssel seiner Kommunikationspartner erfragen und verwalten. Und gerade diese Verwaltung der Schlüssel seiner Kommunikationspartner, das der Nutzer ja auf allen seinen Geräten aktuell halten muss, gestaltet sich in der Praxis als kaum durchführbar.
Er sollte außerdem gewährleisten, dass er weder die eigenen Schlüssel noch die seiner Kommunikationspartner verliert. Ein zusätzliches Problem ist, dass sich jeder für eine beliebige E-Mail-Adresse ein PGP Schlüsselpaar auf irgendeinem PGP Schlüsselserver generieren kann und zwar auch dann, wenn ihm diese E-Mail-Adresse gar nicht gehört. Somit kann irgend jemand mit meiner E-Mail-Adresse ein Schlüsselpaar generieren und dieses auf einem globalen Schlüsselserver als meinen Schlüssel für alle Internet-Nutzer bekannt geben.
Darüber hinaus werden bei der E-Mail-Verschlüsselung mit PGP die Metadaten selbst nicht verschlüsselt. In den vorangegangenen Kapiteln wurde schon dargestellt: gerade bei direkter Kommunikation mit anderen Internet-Nutzern sind die Metadaten für Datenspione oftmals interessanter als der eigentliche Inhalt der E-Mail.
Aus diesem Grunde nutzen sogar IT-Fachleute, die das geschilderte Verfahren verstehen, installieren und bedienen können, diese Art der Verschlüsselung nur als Notbehelf. In Verbindung mit der PGP Verschlüsselung gibt es weitere Probleme, die auf der Webseite „15 reasons not to start using PGP“[230] und in den folgenden Abschnitten, beschrieben worden sind[231]. Dazu kommt, dass die PGP-ID mit ihren 32Bit zu klein ist, um wirklich immer eindeutig zu sein. Somit ist es auch möglich, gefälschte Schlüssel zu generieren[232].
E-Mails werden im Internet nicht direkt zwischen Sender und Empfänger ausgetauscht. Der E-Mail-Sender übergibt zunächst die E-Mail dem E-Mail-Server seines E-Mail-Provider (z.B. gmx oder Goolge-Mail), der dann diese E-Mail (direkt oder manchmal auch indirekt) über mehrere Netzwerkknoten dem E-Mail-Provider des Empfängers zustellt. Dieser speichert die E-Mail so lange, bis der Empfänger die E-Mail mit seinem E-Mail-Programm abholt. Die E-Mail-Provider müssen, um die E-Mail ausliefern zu können, natürlich wissen, für wen die E-Mail bestimmt ist. Die diesbezüglichen E-Mail Metadaten können deswegen nicht verschlüsselt werden.

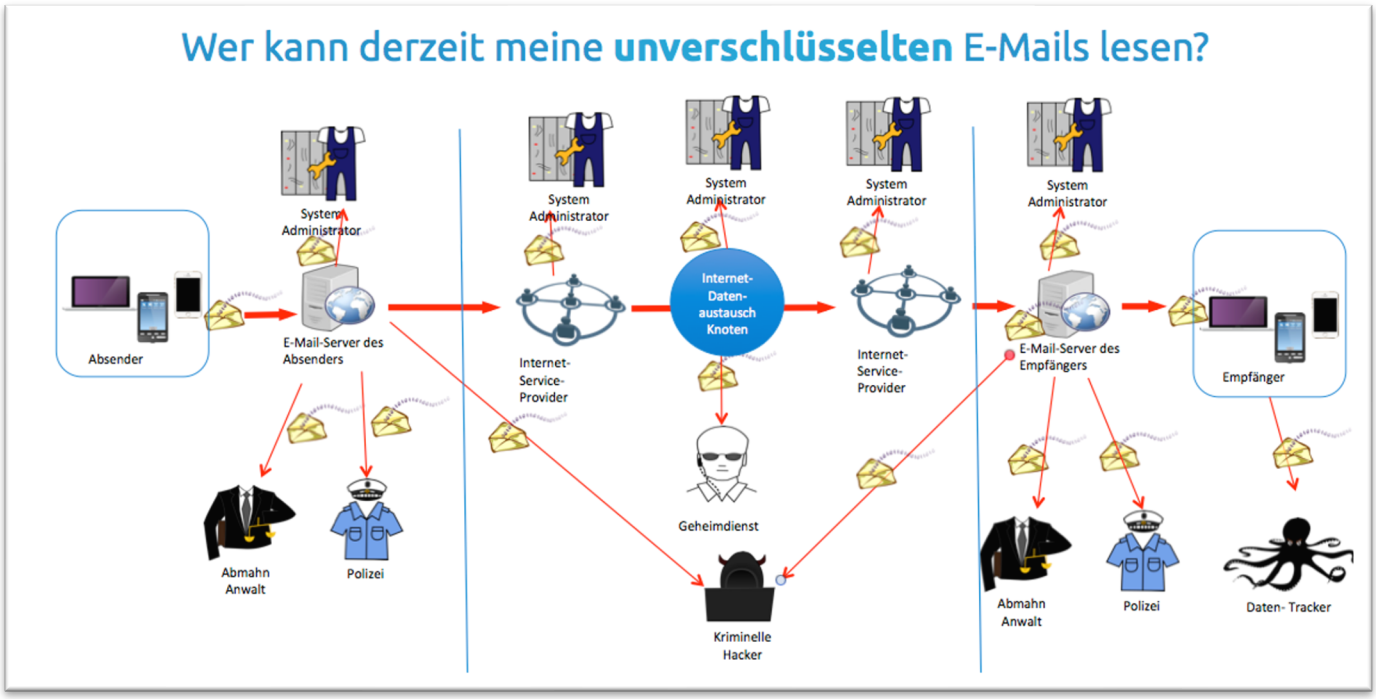
228 http://de.wikipedia.org/wiki/Pretty_Good_Privacy

229 https://de.wikipedia.org/wiki/S/MIME

230 http://secushare.org/PGP

231 http://www.heise.de/security/meldung/Massentaugliche-E-Mail-Verschluesselung-gesucht-2557237.html?wt_mc=nl.heisec-summary.2015-02-23

232 http://www.heise.de/security/meldung/Haufenweise-Fake-PGP-Schluessel-im-Umlauf-3297175.html?wt_mc=nl.heisec-summary.2016-08-18



(© 2016 Comidio GmbH)

Ein weiteres Sicherheitsproblem des heutigen E-Mail-Systems ist, dass man nicht darauf vertrauen kann, dass die E-Mail tatsächlich von dem genannten Absender oder dem versendenden Mail-Server stammt. Wer heute eine Nachricht verschicken möchte, kann in die E-Mail eine x-beliebige Absender-Adresse eintragen. Oft kommen Spam E-Mails von gekaperten Servern, die zum Versenden von Massen E-Mails genutzt werden. Das kann sogar der eigene PC oder ein IoT-Gerät im Haushalt sein, wenn dieser gehackt wurde (und Teil eines Bot-Netzes wurde). So kann der eigentliche Versender von Spam E-Mails weder mit Hilfe der Schadcode enthaltenden E-Mail noch über die IP-Adresse des Servers ausfindig gemacht werden. Eine gute Übersicht über die Gefahren bei E-Mails und deren Lösungen gibt das „Privacy-Handbuch“[233].

Die allgemeinen Security-Anforderungen bei Kommunikation über öffentliche Netze und deren Trutz-Box-Lösung sind:

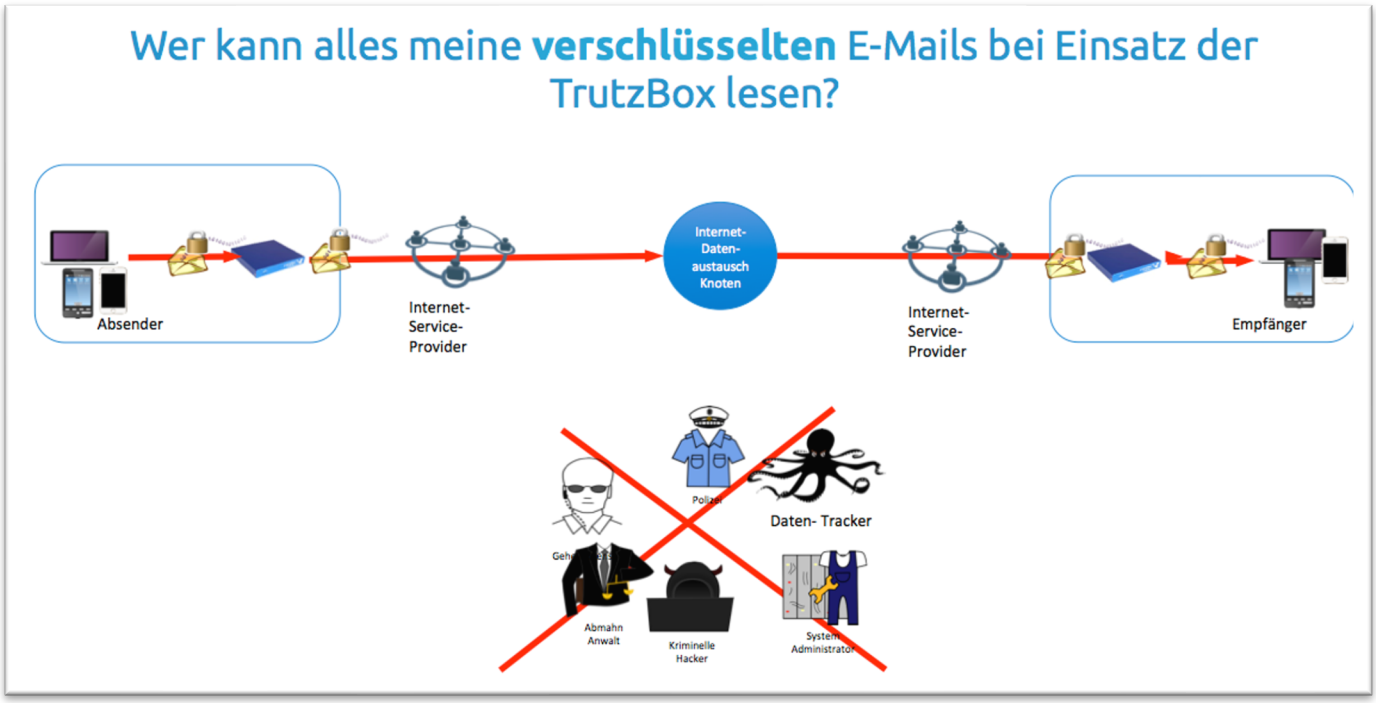
- **Authentizität** - die Gesprächspartner wissen zuverlässig, mit wem sie kommunizieren
- **Vertraulichkeit** - kein Dritter kann mithören oder Daten ändern
- **Perfect Forward Secrecy** - (*Folgenlosigkeit)* - bei abgefangenen Nachrichten kann niemand nach Beendigung der Sitzung den geheimen Langzeitschlüsseln rekonstruieren.
- **Abstreitbarkeit** - der Absender kann Dritte nicht für den Inhalt der Nachricht verantwortlich machen.
- Mit diesen Security-Anforderungen und weiteren Anforderungen bzgl. einfachster Bedienbarkeit und Verfügbarkeit auf allen Clients, wurden von Comidio folgende Anforderungen an die TrutzMail Architektur gestellt und implementiert:

233 http://de.wikibooks.org/wiki/Privacy-Handbuch:_E-Mail_Kommunikation

- **Einfachste Bedienung** in der Art, dass der Nutzer nicht mit wie auch immer gearteten Schlüsseln in Berührung kommt und (nach der Installation) sich nichts an seiner gewohnten E-Mail Bedienung ändert.
- **Komplette Verschlüsselung** der gesamten E-Mail samt Metadaten.
- **Sicherste Verschlüsselung** durch Nutzung neuester kryptografischer Methoden.
- **die Authentizität der E-Mail-Absenderadresse und des E-Mail-Servers sind überprüfbar** und werden verifiziert. Beim ersten Mail-Kontakt lädt der Adressat das Zertifikat des Absenders vom zentralen Comidio Server. Dadurch wird verhindert, dass sich ein Absender als jemand anderes ausgibt als er in Wirklichkeit ist. Des Weiteren kann ein E-Mail-Absender nur von seiner TrutzBox E-Mails versenden. Spam ist deswegen nicht mehr möglich. Betrügerische E-Mails können nicht mehr von gefälschten Absendern kommen.
- Es gibt beim Austausch von E-Mails **keine zentrale Instanz**, weder für die Verwaltung der geheimen Schlüssel noch für die Verifizierung der E-Mail-Absender oder E-Mail-Server.
- **E-Mail-Adressen sind nur Absender und Empfänger bekannt**. Niemand, der alle Daten im Internet „mithören“ kann, ist in der Lage, E-Mail-Adressen zu sammeln und diese zu missbrauchen.
- **Das E-Mail-System darf kein geschlossenes System sein**. Da nicht davon auszugehen ist, dass alle Kommunikationspartner durch diese sichere E-Mail erreichbar sind, muss es weiterhin möglich sein, auch unsichere E-Mails mit anderen Kommunikationspartnern auszutauschen.
- Es muss einem Benutzer möglich sein, sein **E-Mail-Konto zu löschen** und die E-Mail-Adresse danach erneut anzulegen. Da sich dadurch das Zertifikat der E-Mail ändert, die alten Zertifikate aber noch in Umlauf sind, ist die Umsetzung dieser Anforderung nicht trivial.
- Es muss möglich sein, **kompromittierte E-Mail-Adressen** (Accounts) im gesamten System zu **sperren.**

Austausch von sicheren E-Mails über die TrutzBox

Die Verschlüsselung der Metadaten kann nur gewährleitstet werden, wenn die gesamte E-Mail verschlüsselt ist und wenn zwischen Absender und Empfänger keine weitere Instanz die E-Mail Adresse benötigt um die E-Mail ausliefern zu können, somit bei einem „Vermittler“ auch keine Meta-daten anfallen. Eine Lösung wäre, die E-Mails direkt zwischen Absender und Empfänger auszutauschen (p2p – peer-to-peer). Dass E-Mail-Programme Nachrichten direkt untereinander austauschen ist allerdings keine gute Lösung, da dann sowohl der Absender als auch der Empfänger das Mail-Endgerät zur selben Zeit eingeschaltet haben und online sein müssten. Da man einerseits davon ausgehen kann, dass dies sehr selten der Fall ist, und man andererseits sicherstellen will, dass TrutzMail auf allen Endgeräten nutzbar ist, wurde TrutzMail auf einer dedizierten Server-Hardware implementiert (Eigenhosting).



(© 2016 Comidio GmbH)

Dieser Server (die TrutzBox) sollte immer eingeschaltet sein, sodass TrutzMails jederzeit empfangen werden können. Auf der TrutzBox läuft ein ganz normaler Standard-Mail-Server, mit dem sich das gewohnte E-Mail-Programm des Benutzers verbinden kann. Der Anwender ist damit beim Austausch über sichere E-Mails nicht mehr auf einen fremden E-Mail-Provider angewiesen. Der Benutzer wird sozusagen zu seinem eigenen E-Mail-Anbieter (Stichwort „Eigenhosting““ oder „Edge-Computing“. Und wird ein großer E-Mail-Anbieter gehackt und dabei viele Millionen E-Mail-Adressen einschließlich Passwörtern entwendet, dann sind die E-Mail oder Login-Daten von TrutzBox Nutzern nicht mehr dabei.
Wenn mit der TrutzBox eine E-Mail an einen anderen TrutzBox Besitzer verschickt wird, muss nichts zusätzlich konfiguriert werden. Die Verwaltung der Schlüssel, sowie die Ver- und Entschlüsselung selbst, wird von der TrutzBox automatisch durchgeführt.
In manchen Ländern kommt es vor, dass Behörden die E-Mail-Provider auf Herausgabe von E-Mail-Passwörtern zwingen (Lavabit[234]). Da Comidio keinerlei geheime Daten von seinen Kunden hat, kann Comidio derartigen behördlichen Informationsersuchen zwar Folge leisten, aber Behörden können so nicht an die geheimen Schlüssel oder E-Mails gelangen.
Mit dem Link https://trutzbox/mail kann der Nutzer von jedem Gerät den eingebauten WEB-Mailer aufrufen und seine TrutzMails bearbeiten. Der Anwender nutzt dann den auf der TrutzBox installierten Web-Mailer (RoundCube), der es dem Nutzer erlaubt, mit Hilfe eines Web-Browsers seine E-Mails zu verwalten.
Falls er seinen gewohnten E-Mail-Client weiter verwenden möchten, kann der Benutzer den TrutzMail Server als weiteren Mail-Server in seinem E-Mail-Client eintragen und wie gewohnt alle E-Mail Funktionen seines E-Mail-Clients weiter verwenden (Server-Parameter siehe TrutzBox Handbuch). Dabei nutzt der Anwender den auf der TrutzBox installierten Mail-Server „Dovecot“, um seine Mails über das IMAP

234 http://bits.blogs.nytimes.com/2013/08/08/two-providers-of-encrypted-e-mail-shut-down/?_r=1

Protokoll von seinem E-Mail-Client abzuholen. Für das Versenden von E-Mails mit Hilfe des SMTP Protokolls kommt ein Mail-Submission-Agent Server (MSA-Server) auf der TrutzBox zum Einsatz. Folgende beiden alternativen Ports und Protokolle sollten im Mail-Client konfiguriert werden:

Posteingang IMAP Server: trutzbox

Port	Protokoll	Bezeichnung
143	STARTTLS	TLS oder SSL
993	TLS	TLS oder SSL

Postausgang SMTP Server: trutzbox

Port	Protokoll	Bezeichnung
587	STARTTLS	TLS
465	TLS	TLS

Maximalgröße einer TrutzMail

Bevor eine E-Mail versendet werden kann, müssen die Anhänge der E-Mail in lesbare Zeichen umcodiert werden. Dadurch wird eine E-Mail immer erheblich größer, als die ursprüngliche Summe der Anhänge. Da die Größe einer E-Mail nur durch die aktuelle Größe des derzeit verfügbaren Hauptspeichers begrenzt ist, lässt sich kaum voraus sagen, ob eine große E-Mail noch gesendet (oder auch durch die TrutzBox des Empfängers) empfangen werden kann. Falls es zu Problemen aufgrund der Mailgröße kommen sollte, hilft oft ein Neustart der TrutzBox. Dadurch wird der Hauptspeicher „geleert“.

Technische TrutzMail Implementierung

Bei der ersten Auslieferung der TrutzBox (August 2015) wurde für TrutzMail eine technische Umsetzung zum Finden der Empfänger IP-Adresse und der Übertragung der eigentlichen sicheren E-Mails gewählt, die auch im Internet andere verbreitete peer-to-peer Netzwerke nutzen, um größere Datenmengen zu verteilen. Die sogenannten DHTs[235] . DHTs (distributed hash tables) sind im Internet verteilte Tabellen, die einen beliebigen Schlüssel einer IP-Adresse zuordnen. Diese Tabellen werden von den teilnehmenden Systemen, die untereinander vernetzt sind, permanent ausgetauscht.
In dieser ersten TrutzMail Version wurde die Empfänger-IP-Adresse über eine solche DHT ermittelt und die E-Mail, nach Authentisierung des Empfängers über sein Mail-Zertifikat, per TLS-Verschlüsselung übertragen.
Diese Methode war zwar sicher und damit konnte auch die komplette E-Mail verschlüsselt übertragen werden, allerdings hatte diese Lösung auch ein paar Nachteile:

- nach Absenden einer E-Mail dauerte es einige Zeit bis die IP-Adresse der Empfänger TrutzBox ermittelt werden kann. Da die Dauer auch noch recht unterschiedlich war (zwischen einigen Sekunden und einigen Stunden), war das für den Benutzer sehr verwirrend.
- Um TrutzMails empfangen zu können, musste auf dem Internet-Router ein Port sowohl für TCP als auch für UDP geöffnet werden.
- Wer der in der Lage ist, den gesamten Internetverkehr zu überwachen, ist zwar nicht in der Lage eine E-Mail zu entschlüsseln, aber er ist evtl. in der Lage, zumindest zu erkennen,

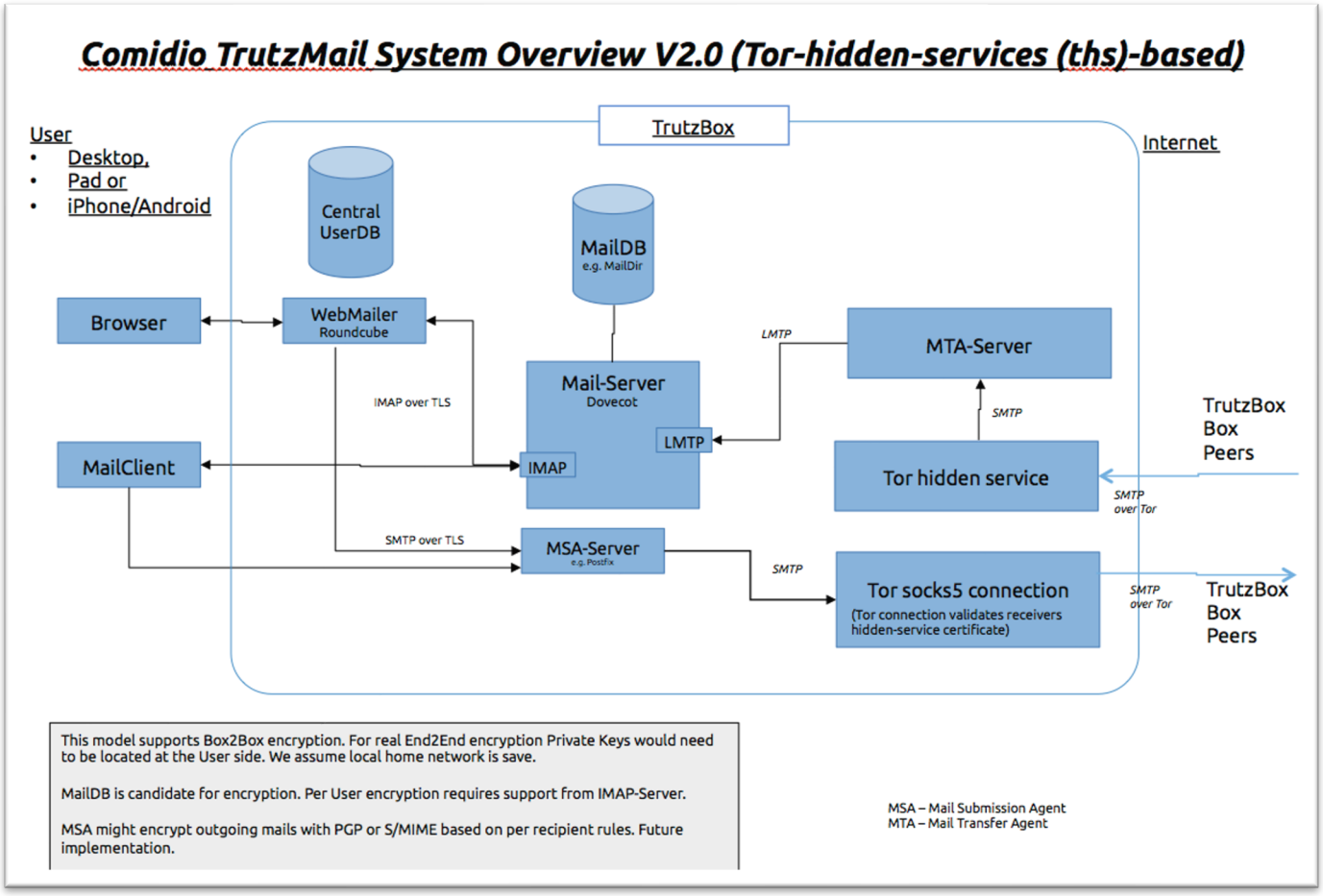
[235] https://de.wikipedia.org/wiki/Verteilte_Hashtabelle

dass hier eine TrutzMail verschickt wird und könnte auch die IP-Adressen beider Beteiligten sehen.

Um diese drei Nachteile auch noch zu eliminieren, entwickelte Comidio eine optimierte Architektur für den E-Mail Austausch. Diese neue Version basiert auf Tor-hidden-services (ths), ist seit Ende Oktober 2015 bei allen Kunden in Betrieb und ersetzt die bisherige DHT-Version.
Das Tor-Netzwerk bietet nicht nur die Möglichkeit seine eigene IP-Adresse im Internet zu verschleiern, sondern auch eigene Services im Tor Netzwerk anzubieten: die sogenannten Tor-hidden-services (versteckte Dienste)[236],[237]. Domain-Namen im Tor Netzwerk haben keine gewöhnlichen Domain-Namen wie google.de sondern enden mit .onion. Die .onion Adressen werden im Tor-Netzwerk, unabhängig vom „normalen Internet“ vergeben und verwaltet.
Beim Anlegen einer neuen TrutzMail Adresse wird auf der TrutzBox ein neuer Tor-hidden-service konfiguriert und im Tor-Netzwerk bekanntgegeben. Dabei bekommt jede TrutzMail Adresse auch eine .onion-Adresse zugeordnet. Falls dann eine andere TrutzBox Kontakt aufnehmen möchte, um eine TrutzMail zu übermitteln, muss diese sendende TrutzBox zunächst die .onion Adresse der Ziel TrutzBox ermitteln. Diese Ziel-Adresse ist im Public-Key Zertifikat des zentralen Comidio-Adressbuchs gespeichert und kann dort von der Absender-TrutzBox bezogen werden. Mit dieser .onion Adresse kann dann die sendende TrutzBox Kontakt mit der Empfänger TrutzBox aufnehmen. Dabei authentisiert das Tor Netzwerk automatisch diese Empfänger TrutzBox und baut eine TrutzBox-zu-TrutzBox verschlüsselte Verbindung auf, über die dann die Mail-Server der beiden TrutzBoxen über Standard-SMTP die Mail austauschen.
Nachstehend ist eine Übersicht der Comidio TrutzMail Architektur abgebildet:

[236] https://www.torproject.org/docs/hidden-services.html.en

[237] https://de.wikipedia.org/wiki/Tor_(Netzwerk)#Versteckte_Dienste



(© 2015 Comidio GmbH)

Die meisten TrutzMail Funktionen wurden mit Hilfe standardisierter Open-Source E-Mail-Programme umgesetzt. Damit kann gewährleistet werden, dass sich an der Schnittstelle zum Nutzer nichts bzgl. seines gewohnten E-Mail-Programms ändert. Durch Einsatz dieses Standard Mail-Servers kann der E-Mail-Nutzer sich mit jedem Standard E-Mail-Programm verbinden und ohne Anpassungen im E-Mail-Client sichere, verschlüsselte E-Mail-Nachrichten senden und empfangen.

Alle dazu notwendigen Erweiterungen und die Verwaltung der Schlüssel übernimmt die TrutzBox. Der Nutzer kann sowohl seine gewohnten E-Mail-Clients, als auch seine Adressverwaltung weiterverwenden. Er muss lediglich einen neuen E-Mail-Account in seinem E-Mail-Programm konfigurieren. Für unsichere E-Mails kann er weiterhin seine alten E-Mail-Accounts des öffentlichen Mail-Providers nutzen.

Die Verwaltung der Schlüssel findet auf der TrutzBox statt. Die TrutzBox generiert und verwaltet die persönlichen Schlüssel. Weder Comidio, noch irgendeine andere zentrale Instanz sind bei der Ver- noch bei der späteren Entschlüsselung und auch nicht während der Übertragung der E-Mails involviert. Comidio verwaltet lediglich ein globales Adressbuch, das die öffentlichen Schlüssel (Zertifikate) beinhaltet. Um sichere von unsicheren E-Mails besser unterscheiden zu können, haben sichere E-Mail-Adressen die Endung (Domain) @comidio.email. Comidio nennt diese Art der E-Mail-Adresse die „TrutzMail Adresse“.

E-Mails senden

Alle E-Mails, die über die TrutzBox gesendet werden, werden automatisch von der TrutzBox verschlüsselt, falls der Empfänger eine TrutzBox ist (und somit die Mail-Adresse mit @comidio.email endet). Dann besorgt sich die TrutzBox automatisch den benötigten öffentlichen Schlüssel des Empfängers. Falls der Empfänger keine TrutzBox ist (und somit eine normale E-Mail Adresse adressiert wurde), dann muss der TrutzBox Administrator zuvor der TrutzBox den öffentlichen PGP-Schlüssel des Empfängers mitteilen. Aus Sicherheitsgründen ist es nicht möglich, eine E-Mail an einen Empfänger zu versenden, wenn der öffentliche Schlüssel des Empfängers unbekannt ist.

E-Mails empfangen

Alle verschlüsselten E-Mails, die von der TrutzBox empfangen werden, werden von der TrutzBox automatisch entschlüsselt und zur Abholung eines E-Mail-Programms bereitgestellt.
Die TrutzBox kann auch von normalen E-Mail-Servern E-Mails empfangen. Diese können sowohl verschlüsselt oder auch unverschlüsselt sein. Um dem Empfänger der E-Mail anzuzeigen, ob die E-Mail verschlüsselt oder unverschlüsselt war, und ob die TrutzBox die Signatur des Absenders prüfen konnte, passt die TrutzBox das Mail-Betreff-Feld in der E-Mail an. Die TrutzBox setzt dazu vor dem Mail-Betreff-Text in eckigen Klammern eingerahmt
als ersten Buchstaben die Absender-Bestätigung

- U – für unsigniert (die TrutzBox konnte den Absender nicht bestätigen), oder
- S – für signiert (die TrutzBox konnte den Absender bestätigen)

und als zweiten Buchstaben die E-Mail Verschlüsselung

- U – für unverschlüsselt (der Mailinhalt war unterwegs lesbar), oder
- E – für encrypted (der Mailinhalt war unterwegs nicht lesbar)

ein.
Beispiele:

- Eine unverschlüsselte E-Mail, die von einem normalen Mail-Account an die TrutzBox gesendet wurde, hat im Betreff-Feld [UU], also unsigniert, unverschlüsselt.
- Eine verschlüsselte TrutzMail, die von einer TrutzBox an eine TrutzBox gesendet wurde, hat im Betreff-Feld [SE], signiert, encrypted.
- Eine verschlüsselte E-Mail, die von einem normalen Mail-Account an die TrutzBox gesendet wurde, hat im Betreff-Feld [UE], unsigniert, encrypted.

Austausch von E-Mails mit (Standard) Mail-Servern (mit jemanden, der keine TrutzBox besitzt)

Mit der TrutzBox ist es auch möglich, verschlüsselte E-Mails mit jemanden auszutauschen, der keine TrutzBox besitzt. Dabei ist jedoch jeweils ein Gateway zu „normalen“ E-Mail-Servern notwendig. Da die TrutzBox ihre sicheren E-Mails mit Standard-PGP-Verschlüsselung verschlüsselt, ist es somit sogar

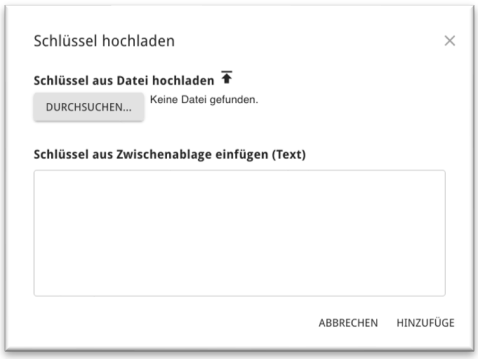
möglich, mit jemanden verschlüsselte E-Mails auszutauschen, der keine TrutzBox hat. Falls die TrutzBox den Public-Key des Empfängers kennt, wird die Mail automatisch PGP-verschlüsselt.

TrutzBox Schlüssel-Verwaltung

Um auch PGP-verschlüsselte E-Mails mit jemanden auszutauschen der keine TrutzBox besitzt, muss die TrutzBox den öffentlichen Schlüssel des Empfängers kennen. Dazu muss zuvor auf der TrutzBox dieser öffentliche Schlüssel der TrutzBox unter „E-Mail“ -> „Schlüsselverwaltung“ bekannt gemacht werden:

(© 2020 Comidio GmbH)

Mit dem Menüpunkt „Schlüssel Hinzufügen“ kann dieser neue Schlüssel importiert werden, indem er aus einer Datei geladen oder indem er aus der Zwischenablage eingefügt wird:



(© 2020 Comidio GmbH)

Sobald die TrutzBox einen öffentlichen Schlüssel für einen Mail-Empfänger kennt, dessen Mail-Adresse nicht mit @comidio.email endet, wird diese E-Mal mit diesem öffentlichen Schlüssel des Empfängers verschlüsselt.
Ein „TrutzBox Besitzer“ kann von einem „Nicht TrutzBox Besitzer“, eine PGP-verschlüsselte E-Mail empfangen, wenn der Absender den öffentlichen Schlüssel des „TrutzBox Accounts“ kennt. Damit kann dann der Absender („Nicht TrutzBox Besitzer“) die E-Mail verschlüsseln. Der öffentliche Schlüssel jeder TrutzMail-Adresse kann mit Klick auf den lokalen Account unter „E-Mail“ -> „Schlüsselverwaltung“ heruntergeladen und an einen anderen Mail-Versender geschickt werden:

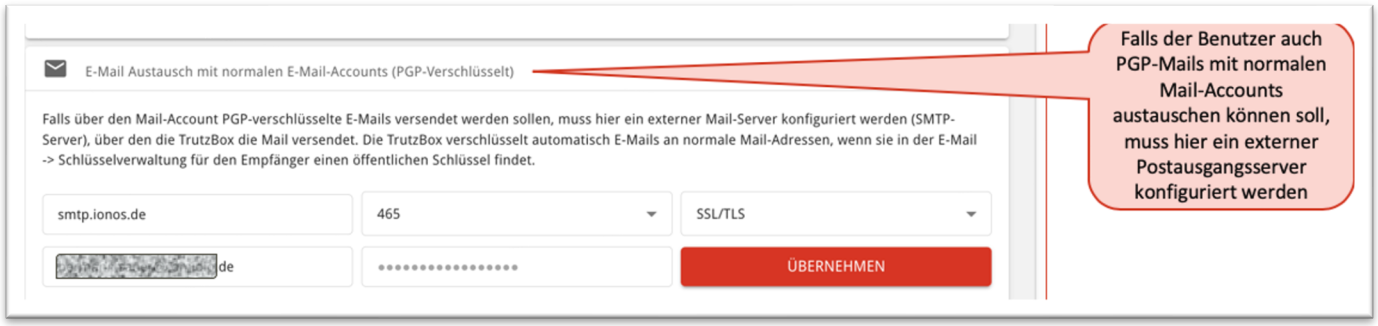
(© 2020 Comidio GmbH)
Die TrutzBox entschlüsselt automatisch alle E-Mails, auch E-Mails, die Sie von einem normalen E-Mail Server bekommen (siehe nächstes Kapitel).

Empfangen von Standard-E-Mails

Um unverschlüsselte oder PGP-verschlüsselte E-Mails auch von normalen Mail-Servern (Nicht-TrutzMail Adressen) empfangen zu können, hat Comidio ein Gateway zu Standard E-Mail-Servern eingerichtet. Dieses Gateway leitet alle an eine @comidio.email gerichteten E-Mails aus dem Internet an die zuständige TrutzBox weiter, auch unverschlüsselte E-Mails. Nach außen fungiert dieser Server wie ein ganz normaler Standard E-Mail-Server und nach innen wie eine TrutzBox, die E-Mails verschlüsselt und über das Tor-Netzwerk an den richtigen TrutzMail Account (die richtige TrutzBox) weiterleitet.

Senden von PGP-verschlüsselten E-Mails an Standard-E-Mail-Accounts

Das von Comidio betriebene E-Mail-Gateway kann jedoch aus Sicherheitsgründen keine E-Mails von einer TrutzBox an einen „normalen“ E-Mail-Account weiterleiten. Eine TrutzBox kann über dieses Gateway somit keine Mail an einen normalen Mail-Account senden. Um von der TrutzBox aus auch normale Standard-Mail-Accounts adressieren zu können, muss zuvor für den TrutzBox-Benutzer auf der TrutzBox ein anderes, externes Mail-Gateway eingerichtet werden. Dieses Mail-Gateway kann ein ganz normaler SMTP-Server eines Standard-Mail Accounts bei einem öffentlichen Mail-Anbieter sein.
Unter dem Menüpunkt „Benutzer verwalten“ kann dazu für jeden TrutzBox Nutzer ein eigenes, externes Mail-Gateway eingetragen werden (z.B. seines t-online Mail-Accounts):



(© 2020 Comidio GmbH)

Nachdem die SMTP-Daten des externen E-Mail Accounts eingetragen wurden, bitte „übernehmen“ drücken. Dabei versucht die TrutzBox testweise eine Verbindung zu diesem SMTP-Server aufzubauen. Falls zuvor für eine Standard-E-Mail-Adresse ein Public-Key eingetragen wurde, verschlüsselt die TrutzBox dann automatisch die Mail mit dem PGP-Verschlüsselungsverfahren. Somit kann auch eine Nicht-TrutzMail Adresse über die TrutzBox adressiert werden.
Aus Sicherheits-Gründen ist es nicht möglich, eine nicht verschlüsselte E-Mail von der TrutzBox aus zu versenden. In diesem Fall gibt die TrutzBox eine Fehlermeldung zurück an den Absender.

Austausch von sicheren TrutzMails zwischen TrutzBoxen

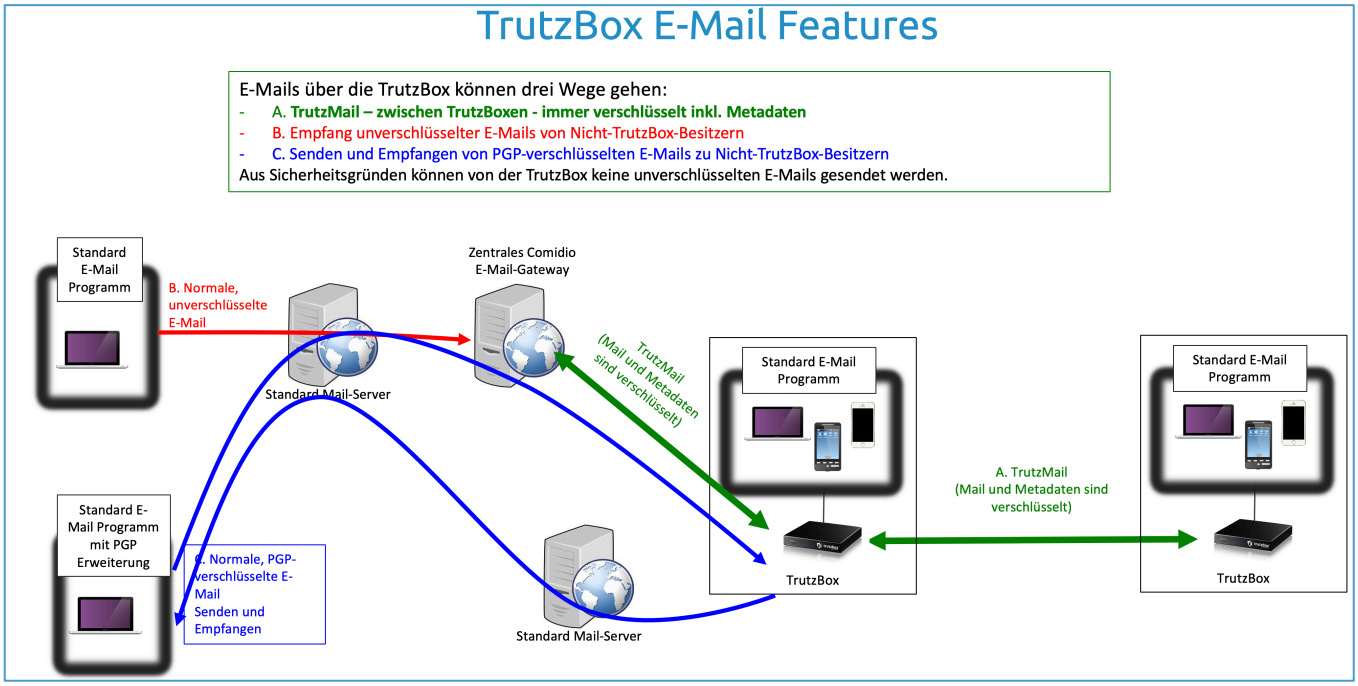
Beim Senden einer TrutzMail wird zunächst das TrutzMail Zertifikat des Empfängers im lokalen Keyring der TrutzBox gesucht. Falls es sich dort nicht befindet, wird das Empfänger-Zertifikat vom Comidio-Server erfragt. Aus dem Empfänger-Zertifikat wird die .onion-Adresse (die Tor-Hidden-Service-Adresse) des TrutzMail Server-Zertifikats gelesen und mit der gefundenen Empfänger-TrutzBox eine verschlüsselte Verbindung aufgebaut. Danach wird die Mail auf der Sender-TrutzBox PGP-verschlüsselt und mit Hilfe von SMTP über das Tor-Netzwerk zur Empfänger-TrutzBox übertragen. Auf der Empfänger-TrutzBox wird die PGP-verschlüsselte Mail entschlüsselt und im lokalen Mail-Store abgelegt.
Damit wird nicht nur sichergestellt, dass die Datenübertragung zwischen den TrutzBoxen verschlüsselt ist, sondern dass auch der Empfänger und Absender authentifiziert werden.
Natürlich können TrutzMails, die zwischen TrutzBoxen ausgetauscht werden, vom Anwender selbst auch zusätzlich mit PGP verschlüsselt werden.

Mail-Austausch über die TrutzBox: Zusammenfassung

Obige Beschreibungen lassen erkennen, dass es aus technischer Sicht somit drei Möglichkeiten gibt, E-Mails mit der TrutzBox auszutauschen:

- A. TrutzMail – zwischen TrutzBoxen - immer verschlüsselt inkl. Metadaten
- B. Empfang unverschlüsselter E-Mail von Nicht-TrutzBox-Besitzern
- C. Senden und Empfangen von PGP-verschlüsselten E-Mails zu Nicht-TrutzBox-Besitzern

Aus Sicherheitsgründen können von der TrutzBox keine **un**verschlüsselten E-Mails gesendet werden.

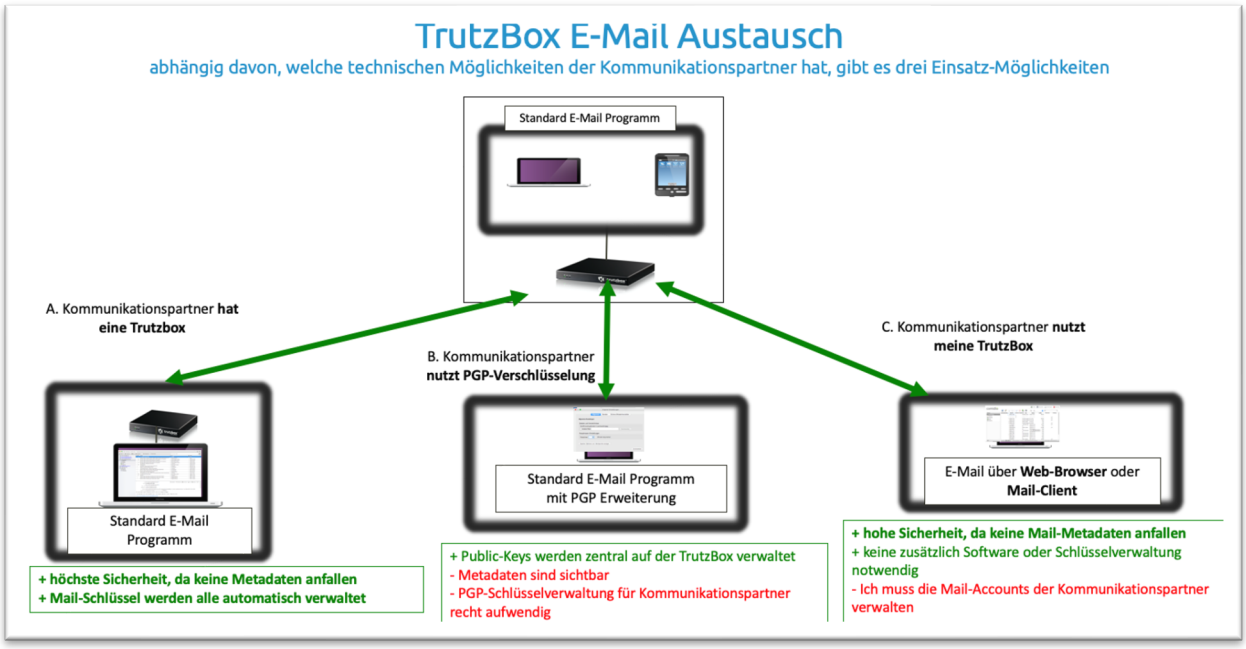


(© 2024 Comidio GmbH)

Drei alternative Einsatzmöglichkeiten um E-Mails auszutauschen

Abhängig davon, welche technischen Möglichkeiten der Kommunikationspartner hat, gibt es somit drei Möglichkeiten verschlüsselte Mails auszutauschen:

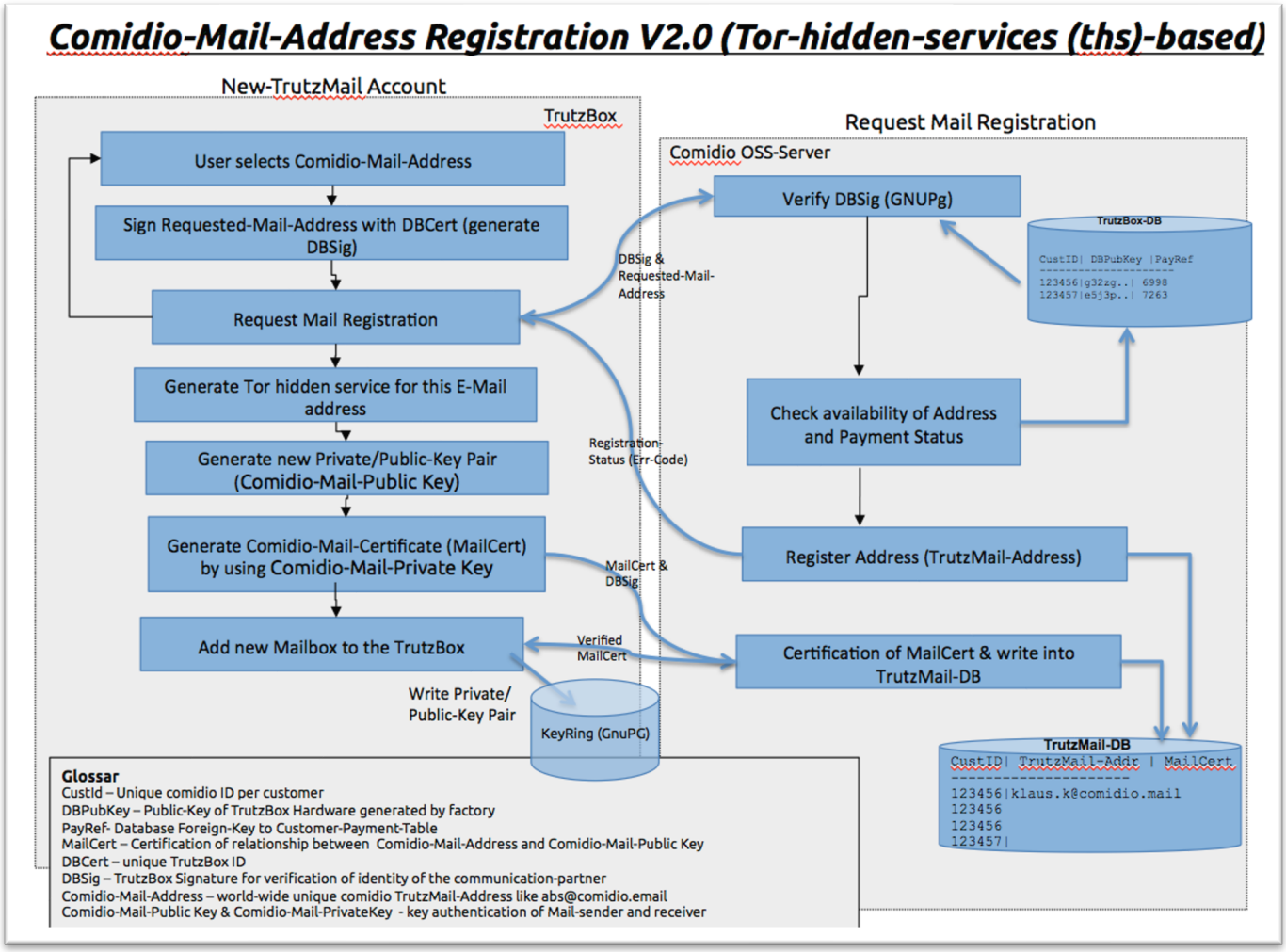
- A: Kommunikationspartner **hat eine TrutzBox.**
- B: Kommunikationspartner kann PGP-verschlüsselte Mails austauschen
- C: Kommunikationspartner hat keine TrutzBox und keine PGP-Verschlüsselung: Kommunikationspartner kann **meine TrutzBox mit benutzen.**



(© 2020 Comidio GmbH)

Neue TrutzMail Adresse registrieren

Wenn auf der TrutzBox ein neuer Benutzer angelegt wird, kann man diesem Benutzer auch eine Trutz-Mail-Adresse und somit einen TrutzMail-Account auf der TrutzBox zuweisen (siehe Kapitel Benutzer verwalten).
Die zentrale Comidio Kundendatenbank (OSS), die von der Comidio GmbH betrieben wird, verwaltet ein zentrales Adressbuch. Dieses Adressbuch kann nur von einer TrutzBox abgefragt werden. Wenn eine neue TrutzMail auf der TrutzBox registriert werden soll, wird zunächst automatisch auf der Comidio Kundendatenbank (OSS) geprüft, ob die gewünschte TrutzMail Adresse noch frei ist. Somit müssen TrutzMail Adressen über alle TrutzBoxen hinweg eindeutig sein und dürfen nur einmalig vergeben werden. Zusätzliche TrutzMail Adressen sind Teil des Vermarktungsmodells der Comidio GmbH. Deswegen wird beim Anlegen einer neuen TrutzMail Adresse auch geprüft, ob der Kunde einen laufenden Service-Vertrag hat und noch freie TrutzMail Adressen im Kontingent vorhanden sind.
Sind diese Kriterien erfüllt, wird auf der TrutzBox ein Schlüsselpaar (Private- und Public-Key) und ein Zertifikat (MailCert) generiert. Dieser private Schlüssel verlässt nie die TrutzBox und ist auch Comidio nicht bekannt. So kann Comidio weder bei einem Einbruch noch auf behördliche Anordnung TrutzMails entschlüsseln. Comidio kennt lediglich alle TrutzMail Adressen und deren Zertifikate (Public-Keys).
Die folgende Übersicht zeigt den Ablauf und die Kommunikation zwischen TrutzBox und dem OSS beim Anlegen einer neuen TrutzMail Adresse.



(© 2015 Comidio GmbH)

TrutzMail Zertifikat Updates

Es kann vorkommen, dass eine TrutzMail Adresse kompromittiert wird; z.B. weil eine TrutzBox inkl. den Passwörtern gestohlen wurde. Oder es kann vorkommen, dass der Inhalt des TrutzBox-Internen Speichermediums gelöscht wird, z.B. wenn eine TrutzBox neu aufgesetzt wurde (durch Hardware-Austausch oder Zurücksetzen der TrutzBox auf Werksauslieferung). In beiden Fällen wird das Zertifikat auf dem zentralen Comidio CA-Server als ungültig gekennzeichnet. Dazu gibt es auf dem zentralen Comidio Server eine „TrutzMail Address-Blacklist“. Aber es muss auch möglich sein, einzelne oder mehrere TrutzMail Zertifikate, die auf einer TrutzBox gespeichert sind und zuvor eine Mail an eine solche Mailadresse geschickt haben, als ungültig zu kennzeichnen.
Aber keine zentrale Stelle weiß, wer solche als ungültig zu kennzeichnenden Zertifikate im Laufe der Zeit auf irgend einer TrutzBox gespeichert hat (auch Comidio nicht). Es ist in dem Konzept auch durchaus beabsichtigt, dass keine zentrale Stelle weiß, wer an wen E-Mails geschrieben hat.

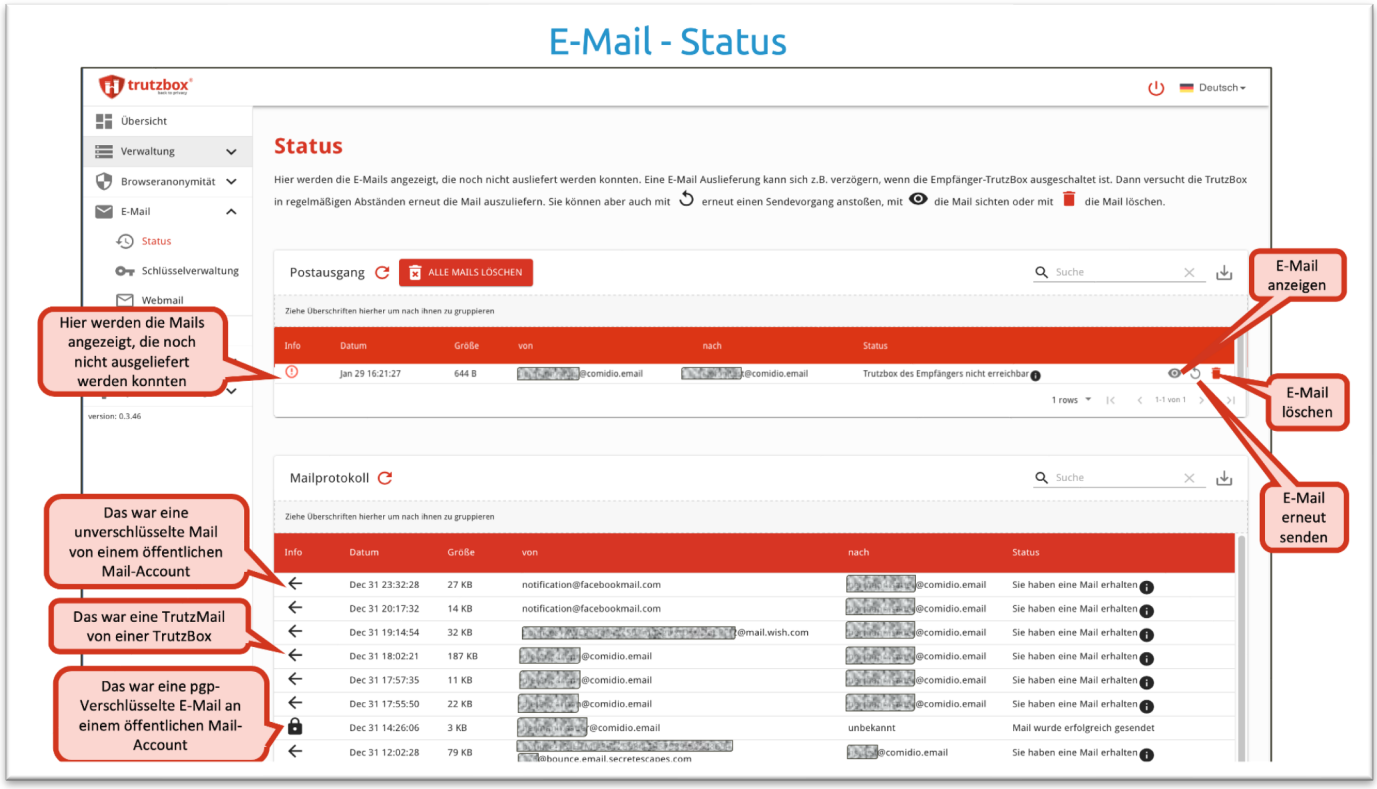
Aus diesem Grund gibt es einen automatischen Prozess, der jede TrutzBox einmal täglich die lokal gespeicherten Empfänger-Zertifikate mit denen der zentralen Comidio TrutzMail Zertifikat-Datenbank abgleicht. Falls eine der gespeicherten TrutzMail Zertifikate ungültig geworden ist, wird diese dann auf der TrutzBox gelöscht. Benötigt die TrutzBox danach das Zertifikat wieder, wird es erneut vom zentralen Comidio CA-Server angefragt.
Bei all diesen Abfragen wird immer nur der Hash einer TrutzMail Adresse abgefragt, so dass es nicht möglich ist, über den zentralen Comidio-Server an TrutzMail Adressen zu gelangen.
Zusätzlich können auch alle lokal auf der eigenen TrutzBox gespeicherten Empfänger-Zertifikate vom TrutzBox Administrator manuell gelöscht werden. Dazu gibt es auf der TrutzBox im Menüpunkt „E-Mail“ -> „Schlüsselverwaltung“ eine Funktion „Alle Empfänger-Zertifikate löschen“. Dabei werden die auf der TrutzBox gespeicherten TrutzMail Zertifikate gelöscht, so dass diese bei Bedarf erneut vom zentralen Comidio CA-Server angefragt werden.

TrutzMail Adressen löschen und wiederverwenden

Falls eine TrutzMail Adresse auf der TrutzBox gelöscht wird, sind zuvor ausgetauschte Zertifikate dieser E-Mail-Adresse evtl. noch auf anderen TrutzBoxen gespeichert. Da es nicht möglich ist, diese TrutzBoxen von der Löschung direkt zu informieren, bleiben diese Zertifikate weiterhin in Umlauf. Damit entsteht dasselbe Problem wie bei Zertifikaten, die in die Blacklist aufgenommen werden (vorheriger Punkt). Der Comidio Server wird allerdings über diese Art der Löschung informiert und markiert das gelöschte Zertifikat in seiner CA-Datenbank. Ein gelöschtes TrutzMail Konto führt allerdings nicht unverzüglich zu einer Aktualisierung der Zertifikate, da damit zu rechnen ist, dass das Konto erneut (auf derselben TrutzBox oder auf einer ausgetauschten TrutzBox Hardware, mit derselben TrutzLegitimation, eingerichtet wird. Falls nach ihrer Löschung die E-Mail Adresse erneut eingerichtet werden soll, lässt der Comidio Server dies nur zu, wenn die Anforderung von derselben, ursprünglichen TrutzLegitimation initiiert wird.
Dieselbe Situation kann auch entstehen, wenn die TrutzBox auf ihre Werkseinstellung zurückgesetzt wird. Weil dadurch alle Nutzer und deren TrutzMail Adressen auf der TrutzBox gelöscht werden, könnten danach die TrutzMail Adressen problemlos erneut registriert werden. Der Comidio Server lässt auch in diesem Fall eine solche Wiederverwendung der TrutzMail Adresse nur dann zu, wenn der Vorgang von einer TrutzBox initiiert wird, die mit derselben TrutzLegitimation wie bei der Erst-Registrierung der TrutzMail-Adresse eingerichtet wurde. Somit ist sowohl die TrutzLegitimation noch die TrutzMail-Adresse an eine Hardware gebunden und eine andere TrutzBox Hardware kann verwendet werden, sofern sie dieselbe TrutzLegitimation hat, wie die TrutzBox, mit der diese TrutzMail Adresse erstmalig registriert wurde.

TrutzMail Ein- Ausgang kontrollieren

Die Bedienoberfläche bietet dem Verwalter der TrutzBox unter „Mail“ -> „Status“ eine Übersicht über alle Mail-Ein- und Ausgänge. Damit können Probleme bei der Zustellung von E-Mails erkannt und gegebenenfalls behoben werden:



(© 2020 Comidio GmbH)

Im „Postausgang“ kann mit dem Symbol

- die Mail angezeigt werden, solange diese noch nicht verschickt wurde. Da die Mail allerdings schon PGP-verschlüsselt ist, ist der Mail-Inhalt nicht lesbar.
- Falls die TrutzBox die Mail nicht ausliefern kannte, versucht die TrutzBox in regelmäßigen Abständen das Versenden erneut. Mit kann man die Mail direkt noch einmal versuchen zu versenden.
- Mit kann die Mail gelöscht werden.

Im „Mailprotokoll“ werden alle abgeschlossenen Mail Ein- und Ausgänge angezeigt.
Falls der Postausgang oder das Mailprotokoll sehr viele Einträge zeigt, kann man durch Ziehen der Spalten-Überschrift in die darüber liegende graue Leiste die Anzeige nach dieser Spalte gruppieren.
Es kann vorkommen, dass eine E-Mail zur Zeit oder nie versendet werden kann. Um eine E-Mail versenden zu können, müssen vier Voraussetzungen erfüllt sein:

- Empfänger-Mail-Adresse muss existieren
- Empfänger TrutzMail Zertifikat muss gültig sein
- Empfänger TrutzBox muss eingeschaltet und online sein
- Absender TrutzMail Zertifikat muss gültig sein

Wenn eine der Voraussetzungen nicht erfüllt ist, werden je nachdem, welche dieser Voraussetzungen nicht erfüllt ist, entsprechende Informationen entweder direkt im MailClient, im TrutzBox-Mailprotokoll und/oder im TrutzBox-Mail-Logfile angezeigt.
Folgende Tabelle beschreibt alle TrutzMail versandt Fälle und deren Meldungen:

Fall: Mail an...				Kommentar: Mail an...	Meldung im Mail-Programm (Client)	Meldung im Mail-Log	Meldung in "TrutzMail Status"
Empfänger-Mail-Adresse existiert	Absender TrutzMail Zertifikat ist gültig	Empfänger TrutzMail Zertifikat ist gültig	Empfänger TrutzBox ist eingeschaltet und am Netz				
Y	Y	Y	Y	alle Bedingungen sind erfüllt, TrutzMail kann ausgeliefert werden	Mail erscheint im Verzeichnis "gesendet"	status=sent (250 2.0.0 Ok: queued as .....) removed disconnect from	Meldung wird zu kurz angezeigt um sie lesen zu können
N	n.a.	n.a.	n.a.	nicht existierende Empfänger-Mail-Adresse	Mail-Client zeigt: E-Mail kann nicht über den Server "trutzbox" gesendet werden Cannot encrypt mail for all recipients	Encryptor - ERROR - Cannot encrypt mail for	keine Meldung
Y	Y	N	n.a.	eine existierende Empfänger-TrutzMail-Adresse, mit ungültiger Signatur. Ob Empfänger TrutzBox eingeschaltet ist ist unrelevant.	Mail-Client zeigt: E-Mail kann nicht über den Server "trutzbox" gesendet werden Cannot encrypt mail for all recipients	Encryptor - ERROR - Cannot encrypt mail for	keine Meldung
n.a.	N	n.a.	n.a.	Eigene TrutzMail-Signatur ist ungültig oder abgelaufen. TrutzService Vertrag ist abgelaufen und wurde nicht verlängert.	Im Betreff der E-Mail wird beim Empfänger durch [UE] angezeigt, dass das Zertifikat des Absenders nicht geprüft werden konnte	keine spezielle Meldung	keine Meldung
Y	Y	Y	N	an eine existierende TrutzMail-Adresse, mit gültiger Signatur, aber ausgeschaltete TrutzBox	System Mail wird nach ca 2h und nach 7 Tagen an den Absender geschickt, mit der Information "Delayed Mail (still being retried)"	...No route to host	(connect to .....onion[?.?.?.?]:25: **No route to host**)

Falls die TrutzBox die Mail mit der Meldung „TrutzBox des Empfängers nicht erreichbar“ nicht versenden kann, versucht es die TrutzBox automatisch alle 2h eine Woche lang erneut. Der Absender bekommt dazu beim ersten Versuch und dann, wenn der letzte Versuch auch nicht funktionieren sollte, eine Mail, die darüber informiert.

TrutzRTC – Echtzeit Kommunikation (Real-Time-Communication)

Bitte beachten Sie, dass diese TrutzRTC-Funktion nur in der Business-Version der TrutzBox zur Verfügung steht.
Die TrutzBox wurde entwickelt, um dem Anwender einen zusätzlichen Schutz vor Angriffen und höchstmögliche Anonymität im Internet zu gewährleisten. Aber was nutzt es, wenn man anonym surft und E-Mails verschlüsselt, aber dann Skype, WhatsApp oder ähnliche Services für Audio- und Video-Konferenzen und Messaging (Chat) nutzt? Selbst teure und angeblich sichere Video-Konferenz-Systeme, die vor allem von Firmen genutzt werden, benötigen einen zentralen Kommunikations-Servern, der vom Anbieter betrieben wird und somit zumindest die Möglichkeit einer Überwachung bietet.
Firmen oder auch Privat-Anwender nutzen gerne kostenlose Dienste wie WhatsApp oder Skype, bei denen sie teilweise in den AGBs sogar zustimmen, dass die Kommunikationsdaten ausgewertet werden.
Somit war von Anfang an klar, dass die TrutzBox auch für Echtzeit Kommunikation eine sichere und anonyme Alternative anbieten muss.
Es gibt zwar eine Vielzahl von Realtime Messenger Software auf dem Markt, aber es gibt derzeit keine, die die Comidio Sicherheitsanforderungen erfüllt. Die EFF (Electronic Frontier Foundation) hat eine Übersicht über die Sicherheitsmerkmale der bekanntesten Tools erstellt[238]. Dabei wurden jedoch bei den Bewertungskriterien drei wichtige Eigenschaften nicht berücksichtigt:

- wie einfach ist das Tool zu installieren und zu bedienen,
- ob es auf allen gängigen Betriebssystemen/User-HW verfügbar ist und
- ob es auch Metadaten verschlüsselt.

Die TrutzMail Technologie bietet eine optimale Grundlage für die Entwicklung eines Realtime Messenger, der auch diese drei Eigenschaften unterstützt.
Comidio hat dazu auf der TrutzBox zwei Funktionen implementiert:

- **XMPP-Server**: für Messaging und je nach verwendetem Client auch weitere Funktionen wie Audio-, Video-Konferenzen, File-Transfer, Screen-Sharing...
- Und einen **Audio- und Video-Konferenz-Server**, auf dem man sich mit einem Browser, der den WebRTC-Standard unterstützt, verbinden kann und der in der Lage ist, sehr effizient mehrere Audio- bzw. Video-Konferenz-Teilnehmer zu verbinden.

Weiterführende Informationen zu XMPP sind https://de.wikibooks.org/wiki/XMPP-Kompendium und http://xmpp.org/ zu entnehmen.

TrutzRTC– Messaging/Chat Verbindungen (XMPP-Server)

Selbst bei sicheren, Ende-zu-Ende verschlüsselten Messanger-Diensten kann der Betreiber der Dienste immer die Metadaten von jeder Message sehen.
Eine Untersuchung von drei beliebten mobilen Messengern (WhatsApp, Signal und Telegram) haben

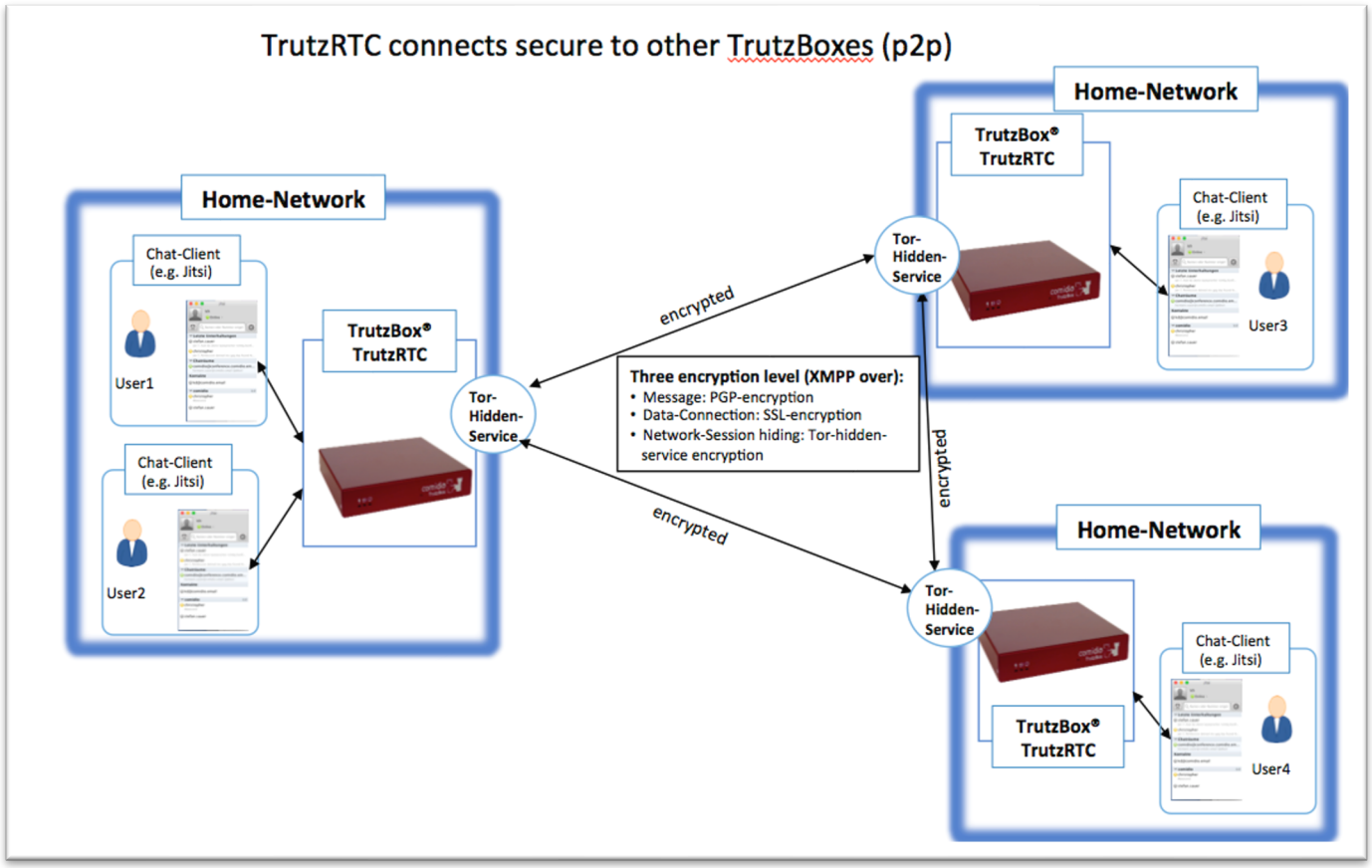
[238] https://www.eff.org/secure-messaging-scorecard

ausserdem gezeigt, dass entgegen den Erwartungen groß angelegte Crawling-Angriffe auch auf vermeintlich sicheren Messanger-Diensten möglich sind.[239]
Es liegt also nahe, selbst einen Messanger-Dienst zu betreiben. Damit ist kein Dritter Dienstleister eingebunden, der die Metadaten sehen könnte. Dieser sollte natürlich auf einem Standard basieren, also auf dem XMPP-Standard.
Das XMPP (Extensible Messaging and Presence Protocol), auf Deutsch „erweiterbares Nachrichten- und Anwesenheits-Protokoll“, ist ein Internet-Standard zum Austausch von Nachrichten (Chat). Es basiert auf der vor vielen Jahren entwickelten Jabber-Software und funktioniert ähnlich wie E-Mail. Ein XMPP-Server verwaltet Benutzer, den Online-Status der Benutzer und Nachrichten. Falls eine Nachricht an einen Teilnehmer verschickt werden soll, der sich nicht auf dem gleichen Server wie der Absender befindet, wird der Ziel-Server (TrutzBox des Kommunikationspartners) ermittelt, Kontakt aufgenommen und die Nachricht zu diesem XMPP-Server ausgeliefert. Das gleiche gilt nicht nur für Nachrichten sondern auch für andere Funktionen, wie z.B. Anwesenheitsstatus. Eine gute Deutsche Einführung in die Welt der XMPP-Kommunikation bietet http://www.einfachjabber.de/.
Es gibt viele öffentlich verfügbare XMPP(Jabber)-Server, die aber alle den Nachteil haben, dass bei jeder Chat-Kommunikation, die durch diese Server vermittelt wird, zumindest die Metadaten sichtbar sind. Somit ist es naheliegend, einen eigenen XMPP-Server zu betreiben...auf der TrutzBox.
Comidio hat den XMPP-Server auf der TrutzBox so erweitert, dass er in der Lage ist, die gleichen Sicherheitsfunktionen zu nutzen, die auch bei TrutzMail verwendet werden. Das bedeutet:

- Kommunikationspartner werden mit der TrutzMail Adresse adressiert.
- Der Verbindungsaufbau und die Nachrichtenübermittlung mit Nutzern auf einer anderen TrutzBox finden über Tor-Hidden-Services statt.
- Für die Verschlüsselung der Messages und Authentisierung der TrutzBox des Kommunikationspartners, werden die gleichen Zertifikate und Schlüssel wie bei TrutzMail verwendet.

Somit wird einfachste Bedienbarkeit und höchste Sicherheit, auch bei TrutzBox übergreifender Kommunikation sichergestellt. Einmal angelegte TrutzMail Adressen können direkt auch für Chat/Messaging verwendet werden. Dazu ist keinerlei Konfiguration auf der TrutzBox notwendig.

[239] https://encrypto.de/papers/HWSDS21.pdf



(© 2015 Comidio GmbH)

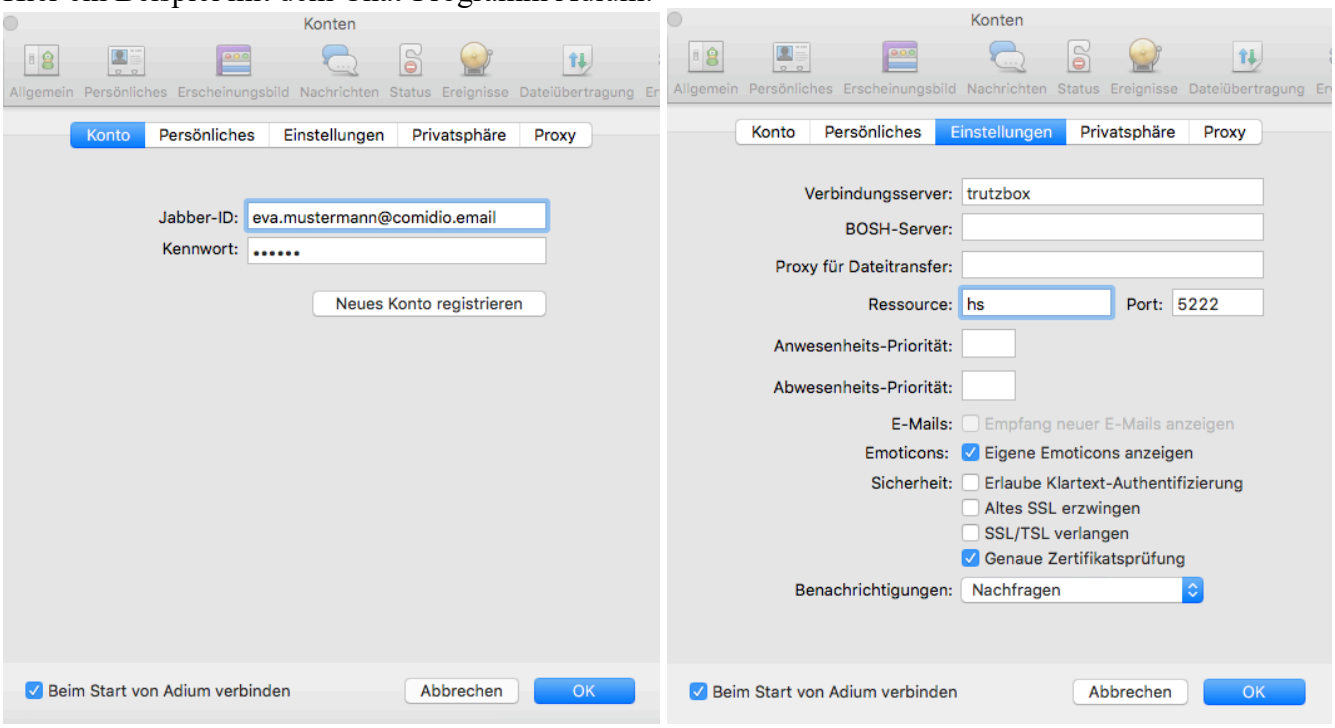
Um den XMPP-Server nutzen zu können, wird auf dem Endgerät ein XMPP-fähiges Programm benötigt. Chat-Programme, die das XMPP-Protokoll unterstützen, sind für alle gängigen Betriebssysteme mit unterschiedlichem Funktionsumfang verfügbar. Diese Links geben einen guten Überblick über verfügbare XMPP-Clients:

- https://de.wikipedia.org/wiki/Liste_von_XMPP-Clients
- https://de.wikibooks.org/wiki/XMPP-Kompendium:_Einrichtung
- http://xmpp.org/software/clients.html

Comidio empfiehlt folgende Chat-Programme für das jeweilige Betriebssystem:

Betriebssystem	XMPP-Software	Link
Apple Macintosh	Adium oder Swift	adium.im, swift.im
Microsoft Windows	PSI oder Swift	psi-im.org, swift.im
iOS (iPhone, iPad..)	ChatSecure	chatsecure.org
Android	Xabber	www.xabber.com

Nach der Installation eines solchen Messaging-Clients muss im Client der XMPP-Server konfiguriert werden. Dazu muss lediglich die entsprechende TrutzMail Adresse mit Passwort angegeben werden. Da viele XMPP-Clients den Server-Namen aus der E-Mail Adresse ermitteln, muss noch der falsch ermittelte Server-Name „comidio.email“ in „trutzbox“ geändert werden. Der XMPP-Standard-Port 5222 bleibt unverändert.
Es können in einem Client auch mehrere TrutzMail Adressen konfiguriert werden.
Hier ein Beispiel mit dem Chat-Programm Adium:



(© 2015 Comidio GmbH)

Danach können durch Eingabe der TrutzMail Adressen beliebig viele Kontakte zugefügt werden.
Je nach Funktionsumfang des Messaging-Clients unterstützt der XMPP-Server auf der TrutzBox diese XMPP-Standard Funktionen:

- Instant-Messaging: Text-Nachrichten inkl. Formatierung und Emoticons,
- Kommunikations-Gruppen anlegen und verwalten, Gruppen-Chats (Multi-User Chat - MUC[240]), auch TrutzBox übergreifend.
- Audio-/Video-Kommunikation: Telefongespräche (Jingle RTP Sessions, optional mit ZRTP Verschlüsselung[241]),
- Datei-Transfer: Dateien an den/die Kommunikationspartner schicken
- Screen Sharing: seinen eigenen Bildschirm für andere sichtbar machen
- Remote-Desktop: der Kommunikations-Partner kann meinen PC bedienen

[240] http://xmpp.org/extensions/xep-0045.html

[241] http://xmpp.org/extensions/xep-0167.html

- OTR (Off-the-Record Messaging)[242]: inoffizielle; vertrauliche, nicht für die Öffentlichkeit bestimmte Nachrichtenübermittlung. Im Gegensatz zur normalen PGP-Verschlüsselung, ist mit OTR später nicht mehr feststellbar, ob ein bestimmter Schlüssel von einer bestimmten Person genutzt wurde. Dadurch lässt sich nach Beenden der Unterhaltung von niemandem (auch keinem der beiden Kommunikationspartner) beweisen, dass einer der Kommunikationspartner eine bestimmte Aussage gemacht hat (glaubhafte Abstreitbarkeit).
- Online-Status, Last-Seen: ist der Kommunikationspartner online, gesprächsbereit... oder wann war er das letzte Mal online

Da die meisten dieser Sonderfunktionen nur dann unterstützt werden, wenn beide Kommunikationspartner den gleichen XMPP-Client benutzen, raten wir dazu, für erweiterte Funktionen besser den Video-Konferenz-Service der TrutzBox zu nutzen.

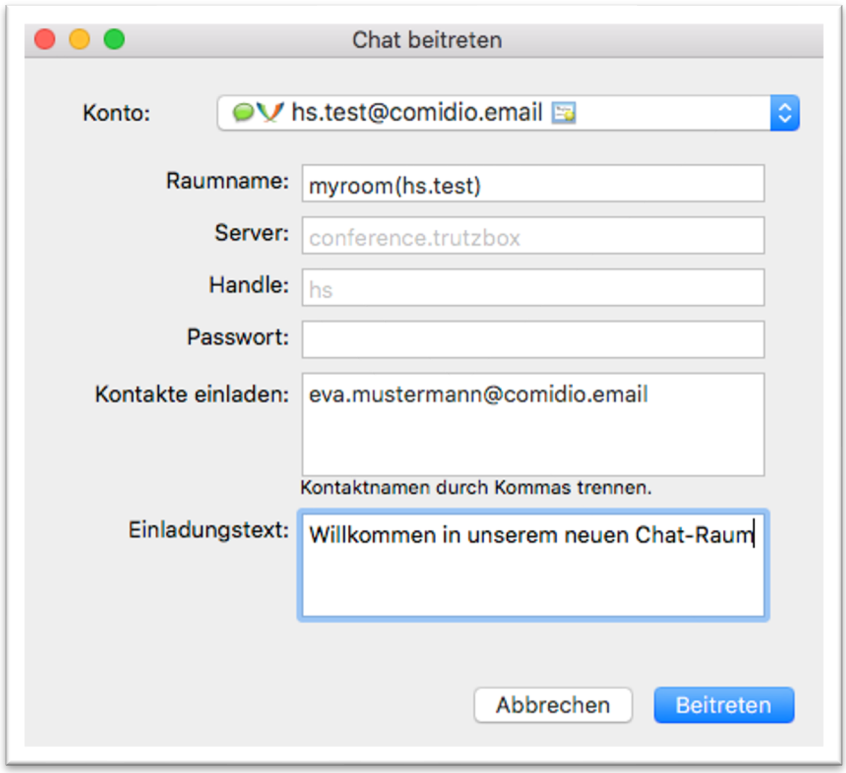
Externe Verbindungen zu TrutzRTC

Solange die TrutzBox mit dem Host-Namen „trutzbox“ erreichbar ist, kann sich der Messaging-Client direkt mit dem XMPP-Server auf der TrutzBox verbinden. Das funktioniert allerdings nur aus dem Heimnetzwerk, wenn der Client mit dem Internet-Router (Proxymode) oder dem sicheren Netzwerk der TrutzBox (Transparentmode) verbunden ist.
Um sich auch von unterwegs mit dem XMPP-Server auf der TrutzBox zu verbinden sollte die TrutzBox entweder über den „Fernzugriff“ oder über einen Domain-Namen erreichbar sein.
Wie der „Fernzugriff“ oder ein Domain-Name eingerichtet wird, entnehmen Sie bitte dem Kapitel „Fernzugriff einrichten“. Wenn dann der Fernzugriff auf dem Mobilen-Device eingerichtet und gestartet ist, kann das Messaging-Programm wie im Home-Netzwerk auf den TrutzRTC Server zugreifen. Dazu müssen keine zusätzlichen Ports auf dem Internet-Router zu Hause geöffnet werden.
Wenn das Messaging-Programm ohne Fernzugriff, also nur über den Domainnamen die TrutzBox erreichen soll, muss auf dem Internet-Router der XMPP-Port 5222 TCP zur TrutzBox weiter geleitet werden.

Einrichtung und Nutzung von Chat-Räumen

Die TrutzBox wird auch gerne von Vereinen, Freundes-Gruppen, Schulen, Industrie-Projekten usw. zur sicheren Kommunikation untereinander genutzt. Solche geschlossenen Nutzergruppen können mit mehreren Nutzern gleichzeitig nicht nur Video-Konferenzen abhalten und sichere E-Mails austauschen, sondern auch über einen (oder mehrere) Chat-Räume gemeinsam kommunizieren. Solche Chat Räume werden auch Multi User Chat (MUC) genannt.
Dazu ist es möglich, auf “meiner eigenen“ TrutzBox, also auf der TrutzBox auf der „ich“ eine TrutzMail-Adresse habe, einen Chat-Raum anzulegen und dann beliebig viele Teilnehmer mit ihrer jeweiligen TrutzMail-Adresse einzuladen.
Um z.B. im Chat-Programm Adium einen neuen Raum anzulegen, ruft man das Menü „Ablage“ -> „gehe zu Chat..“ auf:

[242] https://de.wikipedia.org/wiki/Off-the-Record_Messaging



Dabei haben die Felder folgende Bedeutung:

- **Konto**: hier das TrutzMail-Konto auswählen, unter dem der Chat-Raum angelegt werden soll
- **Raumname**: einen Raumnamen festlegen (hier myroom) und dahinter in Klammer den User-Account (ohne @comidio.email) anhängen. Der Raumname darf keine Sonderzeichen enthalten
- **Server**: nichts verändern
- **Handle**: nichts verändern
- **Passwort**: hier kann optional ein Zugangspasswort eingetragen werden
- **Kontakte einladen**: hier können mit Komma getrennt, Teilnehmer für den Raum eingeladen werden. Die Teilnehmer können aber auch später separat eingeladen oder auch wieder ausgeladen werden
- **Einladungstext**: hier kann man einen beliebigen Text angeben, der bei der Einladung angezeigt wird

Wenn so der Raum angelegt wurde, können weitere Kontakte (in der Kontaktliste mit der rechten Maus-Taste - Menü „zum Chat einladen“) in den Raum eingeladen werden.
Der Chat-Raum befindet sich dann auf der TrutzBox, auf welcher der Raum angelegt wurde. Teilnehmer einer anderen TrutzBox werden mit der Einladung automatisch benachrichtigt und verbinden sich mit diesem Raum.

Sicherheit und Anonymität bei der Nutzung des XMPP-Servers

Um maximale Sicherheit und Anonymität zu erreichen, verbinden sich die TrutzRTC Server bei TrutzBox übergreifender Kommunikation über das Tor-Netzwerk.
Dadurch wird die Kommunikation zwischen den TrutzBoxen dreifach geschützt und es werden sogar die Metadaten verschlüsselt:

- Die XMPP-Message ist PGP-verschlüsselt.
- Die Datenverbindung zwischen den TrutzBoxen ist SSL-verschlüsselt.
- Die Netzwerk-Verbindung wird durch Tor-Hidden-Service verschlüsselt und "versteckt".

Bei der XMPP-Kommunikation wird kein zentraler Server außerhalb der TrutzBox verwendet. Keiner, der den Internet-Verkehr abhört, ist in der Lage, Daten zu entschlüsseln. Ein möglicher Angreifer, der den Internetverkehr überwacht, ist nicht einmal in der Lage zu erkennen, dass es sich überhaupt um eine XMPP-Kommunikation handelt oder die IP-Adressen von Absender oder Empfänger zu scannen oder zu erkennen.
Die Sicherheit der Verbindung zwischen einem XMPP-Client und dem Server oder auch zwischen den XMPP-Clients bei Jingle-Verbindungen, hängt von den Sicherheits-Funktionalitäten des Clients ab und welche davon aktiviert sind. Somit können zusätzliche Client-Verschlüsselungen wie PGP (nur die eigentliche Message wird verschlüsselt), OTR (Off-the-Record Messaging) oder zrtp[243] (Voice-over-IP-Verschlüsselung) aktiviert werden, falls die genutzten Messaging Client diese Funktionen unterstützen.

TrutzRTC Video-Konferenz Server

Um effektiv mit einem Gesprächspartner oder einer ganzen Gruppe von Meeting-Teilnehmern kommunizieren zu können, bieten sich Telefon- oder Video-Konferenzen an. Die derzeit auf dem Markt befindlichen Konferenz-Lösungen haben den Nachteil, dass sie für viel Geld gemietet werden müssen. Es gibt zwar auch kostenlose Angebote, allerdings zahlt man bei denen mit seinen Kommunikations-Daten.
Aber auch bei den bezahlten Konferenz-Systemen ist immer ein zentraler Server, der den Verbindungsaufbau regelt und die Streaming-Daten bündelt, mit im Spiel. Somit ist hier zumindest immer die Möglichkeit gegeben, dass Neugierige die Metadaten oder sogar den gesamten Meeting-Inhalt belauschen können.
Die „Berliner Beauftragte für Datenschutz und Informationsfreiheit" beschreibt auf ihrer Webseite die Gefahren, die von Video-Konferenz-Systemen ausgehen, stellt Anforderungen an solche Systeme und bewertet die gängigsten Systeme [244],[245].

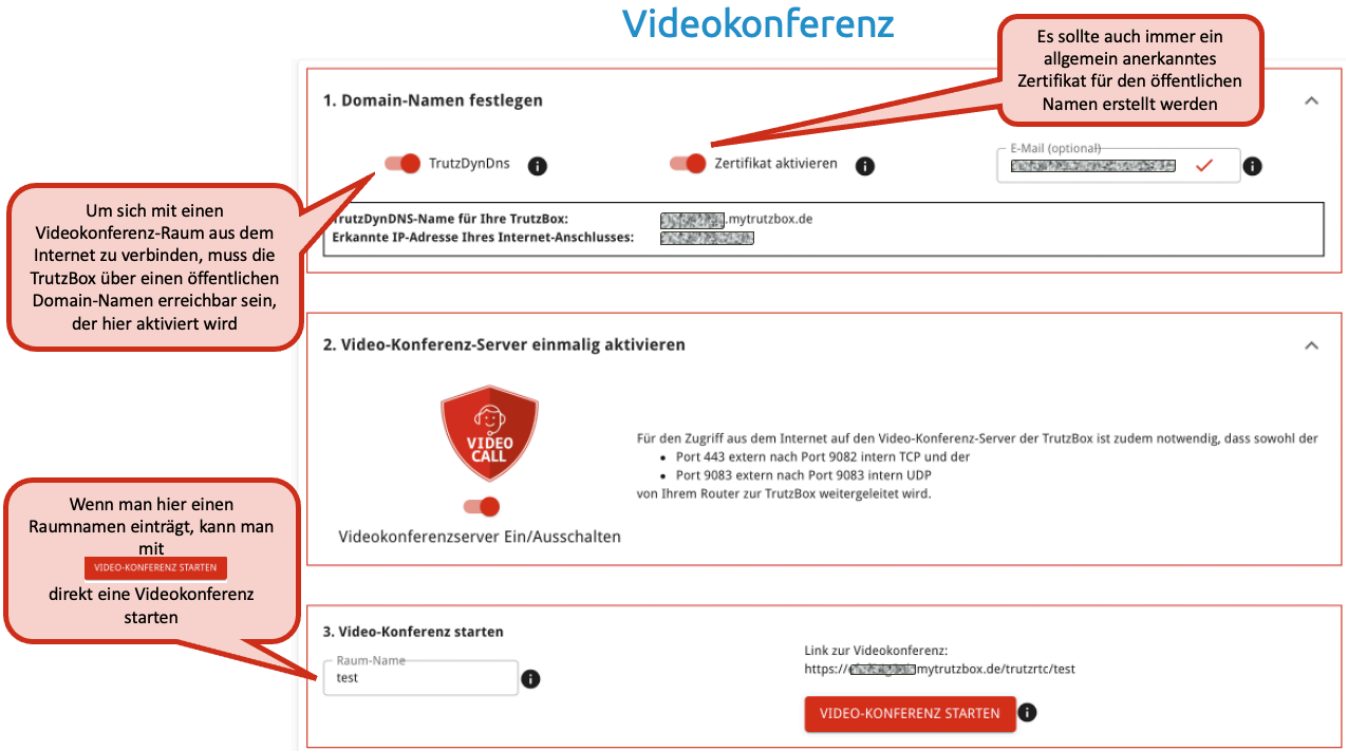
Mit Hilfe des XMPP-Servers und dem richtigen Messaging-Client ist es zwar möglich, eine Audio-/Video-Verbindung aufzubauen, allerdings nur mit einem weiteren Teilnehmer, und es ist notwendig, dass

[243] https://de.wikipedia.org/wiki/ZRTP

[244] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf

[245] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

alle Teilnehmer den gleichen XMPP-Client im Einsatz haben, der den gleichen Audio-/Video-Codex unterstützt. Somit sind Standard-XMPP Clients keine optimale Lösung für Telefon- oder Video-Konferenzen.
Um dem TrutzBox Anwender auch eine sichere Lösung für Telefon- oder Video-Konferenzen mit mehreren Teilnehmern zu ermöglichen, bietet die TrutzBox einen WebRTC-fähigen Konferenz-Server an (nur TrutzBox-Business). WebRTC[246] ist ein recht neuer Internet-Standard, der ursprünglich von Google entwickelt wurde und Audio-/Video-Konferenzen direkt mit einem Standard-Internet-Browser, also ohne zusätzliche Software, ermöglicht. Der Standard wurde zwar von Google entwickelt, allerdings ist bei der TrutzBox-Lösung weder Google, noch irgend eine anderes Unternehmen bei einer Video-Konferenz eingebunden.
Der TrutzBox-Administrator kann, falls noch nicht unter Netzwerk schon geschehen, unter „Videokonferenz“ einen öffentlich erreichbaren Domain-Namen über den Comidio-Dienst „TrutzDynDNS“ anfordern.
Wenn auf dem Internet-Router der entsprechende Port weitergeleitet wird, ist der Video-Konferenz-Server der TrutzBox aus dem Internet erreichbar.



(© 2021 Comidio GmbH)

Damit der Teilnehmer einer Video-Konferenz keine Zertifikats-Fehlermeldung bekommt, sollte immer auch „Zertifikat aktivieren“ aktiviert werden. Damit erhält der TrutzBox-Domain-Name ein offiziell signiertes LetsEncrypt-Zertifikat, das von allen Internet-Browsern anerkannt wird.
Falls die TrutzBox schon mit einer anderen öffentlich nutzbaren Domain erreichbar ist (z.B. mit einer vorhandenen Firmendomain), kann auch diese für die Verbindung zu einem Video-Konferenz-Server

[246] http://webrtc.org/

genutzt werden. In diesem Fall würde der Video-Konferenz-Teilnehmer aber eine Zertifikats-Sicherheits-Warnung bekommen, da der Video-Konferenz-Server lediglich das LetsEncrypt-Zertifikat der TrutzDynDNS-Adresse an den Browser übermittelt. Ein evtl. vorhandenes Zertifikat einer anderen vorhandenen Domain kennt der Video-Konferenz-Server auf der TrutzBox nicht.

Um eine Video-Konferenz zu starten, muss lediglich aus dem internen Netzwerk oder aus dem Internet- mit einem WebRTC fähigen Browser die TrutzBox mit

*https://**xxxxxx**.mytrutzbox.de/trutzrtc/**raumname***

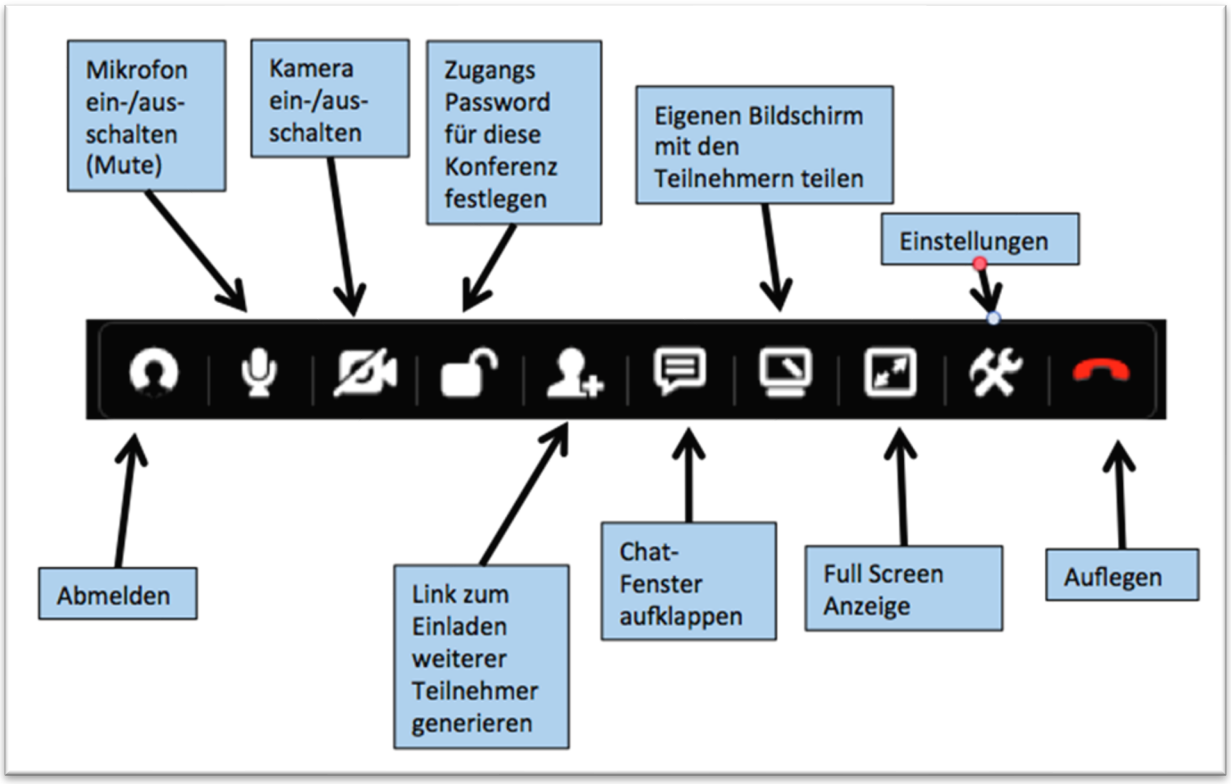
aufgerufen werden. Wobei

- xxxxxx.mytrutzbox.de der TrutzDynDNS-name ist und
- raumname einfach ein selbst vergebener Raum-Name ist. Beim gewählten Raumnamen dürfen keine Sonderzeichen verwendet werden!

Dabei sind zwei Fälle zu unterscheiden:

- Der Raum existiert noch nicht:
  somit ist man jetzt der Erste, der diesen Raum anlegen möchte, und man ist somit der „Raum-Administrator" für diesen Raum. Dann ist es notwendig, sich zunächst mit seiner TrutzMail Adresse und dem TrutzMail Password an dem Konferenz-Server anzumelden. Somit können nur TrutzBox Benutzer, die ein TrutzMail Konto auf dieser TrutzBox haben, einen neuen Raum eröffnen. Nach Anlegen und Verbinden mit dem Raum, kann der Raum-Administrator wahlweise noch ein Password für diesen Raum festlegen und weitere Raum-Optionen festlegen.
- Der Raum existiert schon:
  dann verbindet sich der Browser mit dem Raum. Falls der Raum- Administrator ein Password auf den Raum gelegt hat, muss dieses jetzt eingegeben werden. Falls der Raum schon angelegt ist, kann sich jeder zu dem Raum verbinden. Dazu muss er weder eine eigene TrutzBox besitzen, nicht als Benutzer auf der TrutzBox eingetragen sein, noch eine TrutzMail Adresse besitzen.

Sobald der Browser mit dem Raum verbunden ist, sollte man durch Anklicken des eigenen Verbindungs-Fensters unten seinen „Anzeigenamen" angeben.
Durch Positionierung der Maus am oberen Bildschirmrand wird ein Bedien-Menü geöffnet.
In diesem Menü werden folgende Funktionen angeboten:



(© 2015 Comidio GmbH)

Ein SIP-Gateway von und zum Video-Konferenz-Server wird von Comidio offiziell nicht unterstützt. Wer entsprechendes Know-how besitzt, kann jedoch unter https://github.com/jitsi/jigasi nähere Informationen zur Konfiguration eines SIP-Gateways nachlesen.

Sicherheit und Anonymität bei der Nutzung des Video-Konferenz-Servers

Der Video-Konferenz-Server befindet sich auf der TrutzBox und nimmt keinerlei Verbindung zu einem anderen Server im Internet auf. Per Browser verbindet man sich mit dem Konferenz-Server und benötigt auch keine andere Verbindung außer zur TrutzBox. Da die Browser-Verbindung zur TrutzBox DTLS-verschlüsselt ist (TLS für UDP), wird somit maximale Anonymität und Abhörsicherheit im Internet gewährleistet.

Leistungsgrenzen des Konferenz-Servers

Der TrutzRTC Konferenz-Server basiert auf der Open-Source Software Jitsi-Video-Bridge[247],[248]. Obwohl dieser Konferenz-Server sehr leistungsfähig und auch die TrutzBox Hardware sehr leistungsstark ist, sind nicht unbegrenzt viele Teilnehmer möglich. Die Anzahl der Teilnehmer ist in erster Linie abhängig von der Geschwindigkeit der Internet-Anbindung jedes einzelnen Teilnehmers und des TrutzBox Besitzers. Für die Sprachübertragung genügt ca 40KBit/s up- und down-load Geschwindigkeit pro Teilnehmer. Für Kamera oder Bildschirm-Sharing werden ca 800 KBit/s jeweils benötigt (abhängig von der Bildschirmauflösung und wie oft sich das Bild ändert). Somit werden wahrscheinlich bei normalen

[247] https://de.wikipedia.org/wiki/Jitsi

[248] https://jitsi.org/Projects/JitsiVideobridge

DSL/VDSL Internet-Anbindungen zunächst Engpässe bei der Internet-Anbindung entstehen, bevor die TrutzBox Hardware zum Engpass wird. Solche Internet-Engpässe lassen sich am besten auf dem Internet-Router analysieren.
Test der Video-Konferenz auf der TrutzBox haben ergeben, dass die Leistungsgrenze bei ca. 15 Teilnehmern erreicht wird, wenn nur ein Teilnehmer seinen Bildschirm teilt oder eine Kamera an ist.
Die Jitsi.Meet Software selbst skaliert ziemlich gut, was dieser Benchmark auf einem großen Server mit sehr schneller Internet-Anbindung zeigt: https://jitsi.org/Projects/JitsiVideobridgePerformance.

Externe Verbindungen zum TrutzRTC-Konferenz-Server

Um sich extern, also über Internet mit dem Konferenz-Server der TrutzBox zu verbinden, wird bei den Teilnehmern keine TrutzBox benötigt. Wer den Link kennt (und das evtl. vergebene Passwort), kann an der Konferenz teilnehmen. Das erleichtert vor allem die Nutzung von Webinaren oder spontanen Konferenzen.
Damit der Video-Konferenzserver über das Internet erreichbar ist, müssen allerdings auf dem Internet-Router, an dem die TrutzBox angeschlossen ist, diese zwei Ports an die TrutzBox weitergeleitet werden (TrutzRTC Portfreigabe)

- TCP: von extern 443 auf intern 9082
- UDP: von extern 9083 auf intern 9083

*Mit dem Link „https://**xxxxxx**.mytrutzbox.de/trutzrtc/**raumname** “ kann dann über das Internet dem Raum beigetreten werden.*

Falls im Netzwerk in dem die TrutzBox hängt der externe Port 443 schon für andere Anwendungen belegt ist und diese Anwendung auch aus dem Internet erreichbar sein soll, kann auch ein beliebiger anderer externer Port genutzt werden. Dann müssen die Teilnehmer der Video-Konferenz jedoch im Aufruf nach dem Domain-Namen dieser Port mit angegeben werden.

Z.B. bei Weiterleitung des Ports 4443 anstatt 443:
*„https://**xxxxxx**.mytrutzbox.de:4443/trutzrtc/**raumname** “*

Telefonverbindung von und zum Video-Konferenzserver

Da TrutzRTC auf dem Jitsi-Meet-Server basiert, wäre es technisch zwar möglich, sich auch per Telefon in eine Video-Konferenz ein zu wählen. Es wäre auch möglich, von einer Video-Konferenz aus einen Teilnehmer aus dem Telefonnetz anzurufen. Das dafür notwendige Telefonmodul „Jigasi - Jitsi Gateway to SIP“ ist jedoch derzeit auf der TrutzBox nicht installiert: https://github.com/jitsi/jigasi.

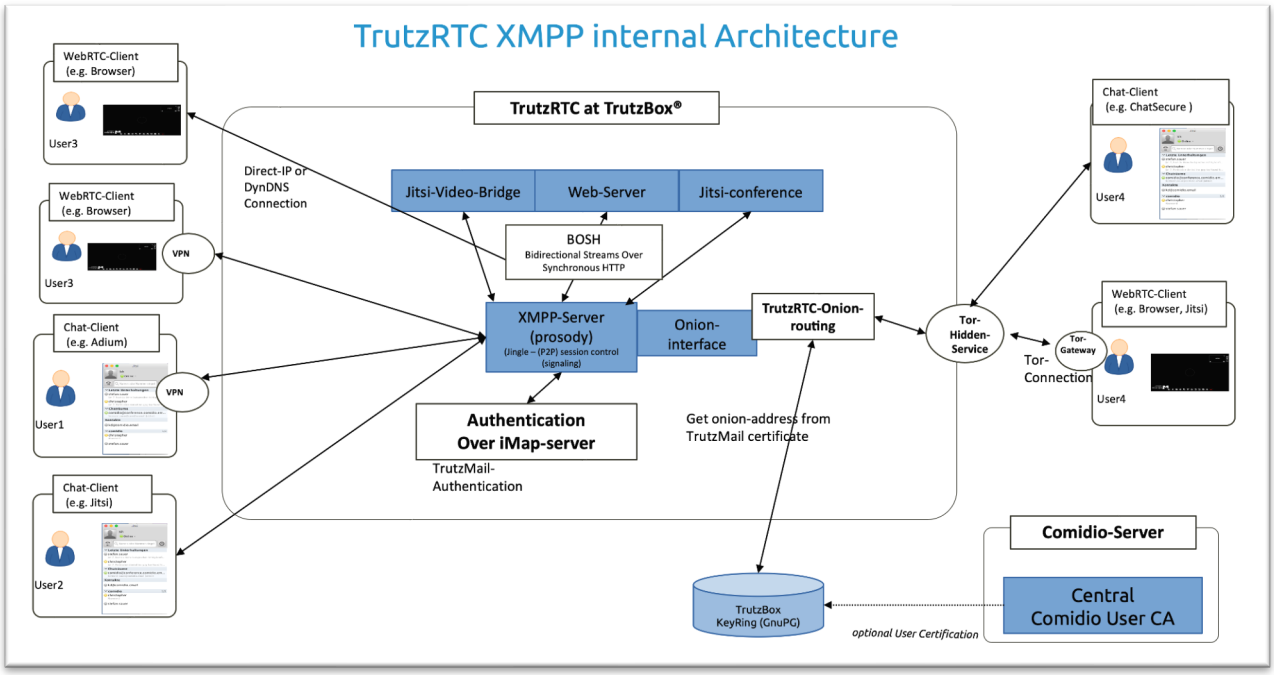
Interne TrutzRTC Architektur

Zum tieferen Verständnis hier eine Beschreibung der internen TrutzRTC Architektur.
Das web-Interface der Video-Konferenz wird über einen Apache2 Server bedient. Dessen Konfiguration liegt hier (sollte nicht verändert werden): /usr/share/comidio/trutzrtc/comidio/trutzrtc.apache2.conf

Abweichent vom original-Jitsi wird von der TrutzBox das jitsi-Konfigurationsfile dynamisch bei jedem neuen Konferenz-Teilnehmer für den Teilnehmer neu generiert.
Das cgi-Script */usr/share/comidio/trutzrtc/comidio/cgi/rtc-config.cgi*

generiert bei jedem neuen Konferenz-Teilnehmer dynamisch das Config-File trutzbox-config.js (das config-File geht an jeden Teilnehmer-Browser). Bei der Generierung des conf-Files wird unter anderem auch dynamisch der TrutzDynDNS-Name eingesetzt. Welche Konfiguration ein Teilnehmer genau bekommt, kann man mit diesem Link abrufen:
https://**xxxxxx**.mytrutzbox.de/trutzrtc/config.js
Die Parameter des Configurations-Files sind hier beschrieben: https://community.jitsi.org/t/how-to-how-to-customize-meeting-options/.

Für den Verbindungsaufbau einer Video-Konferenz und für die Chat-Funktion von TrutzRTC wird der XMPP-Server „prosody“[249],[250] genutzt. Prosody ist ein weit verbreiteter Open-Source XMPP-Server, der sich vor allem durch Ressourcen schonenden Betrieb und umfangreiche Erweiterbarkeit auszeichnet.
Um beim Catten über die TrutzMail Adresse den XMPP-Server (also die TrutzBox) des Kommunikationspartners zu finden, wurde dieser von Comidio um ein spezielles TrutzRTC Onion-Routing erweitert. Somit ist die TrutzRTC Implementierung in der Lage, sich über Tor-Hidden-Services mit anderen TrutzRTC Servern verschlüsselt und anonym zu verbinden. Beim Verbindungsaufbau mit der TrutzBox des Kommunikationspartners wird die entsprechende Signatur der TrutzMail-Adresse überprüft. Dadurch wird verhindert, dass es einem Angreifer gelingen könnte, mit Hilfe einer „gefakten“ TrutzMail-Adresse, die Identität eines anderen zu übernehmen.
Damit sich ein TrutzRTC Raum-Administrator mit Hilfe seiner TrutzMail Adresse authentisieren kann, wird für die XMPP-User-Authentisierung die IMAP-Server-Authentifikation genutzt.



(© 2015 Comidio GmbH)

[249] https://prosody.im/

[250] https://de.wikipedia.org/wiki/Prosody

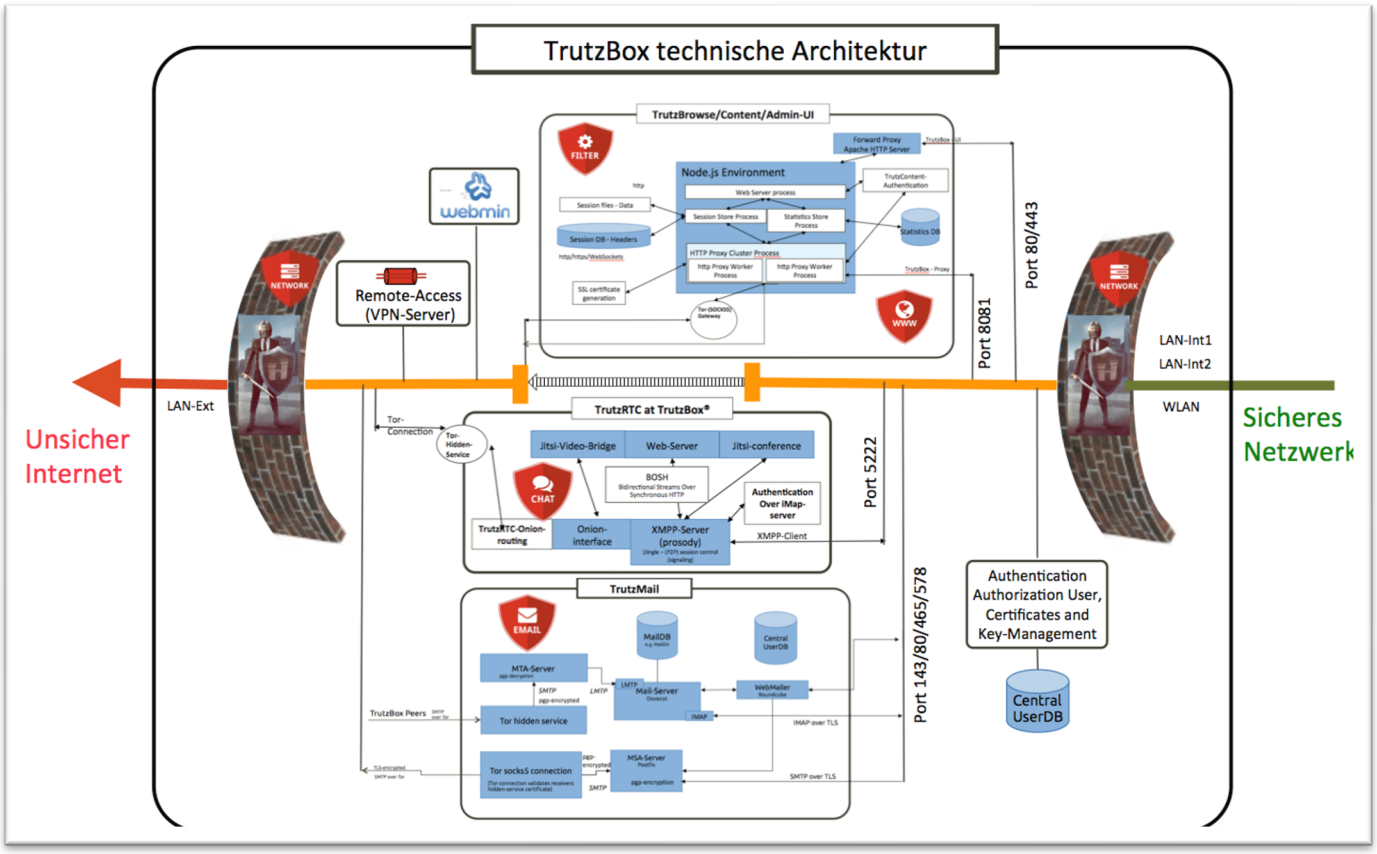
TrutzBox Basis Schutz (TrutzBase)

Es ist notwendig alles dafür zu tun, dass die TrutzBox selbst nicht Opfer eines Hackerangriffs werden kann. Falls ein Hacker in der Lage wäre die TrutzBox für seine Zwecke zu missbrauchen, könnte das großen Schaden anrichten. Darin unterscheidet sich die TrutzBox wenig von einem Internet-Router. Allerdings befindet sich die TrutzBox im internen Netzwerk, nicht wie der Internet Router im öffentlichen Netzwerk. Somit ist sie auch zusätzlich durch die Firewall des Internet-Routers geschützt.
Außerdem gilt es auch, die an die TrutzBox angeschlossenen Netzwerkgeräte auf unterer Netzwerkebene, so gut es technisch möglich, ist zu schützen. Solche angeschlossenen Netzwerkgeräte sind nicht nur PCs, MACs oder mobile Devices, sondern auch Fernseher, mobile Geräte wie iPhone, iPad, Android-Devices usw.; ebenso schon vorhandene oder zukünftige „Smart Home“ Devices, wie Heizung, Zahnbürste oder Fitness-Armband.
Der TrutzBox Basis Schutz besteht aus folgenden Komponenten:

- TrutzBox Netzwerk
- Firewall
- Host Intrusion Detection System
- Abgesichertes Betriebssystem
- VPN–Zugriff auf die TrutzBox über das Internet (Fernzugriff)

TrutzBox Netzwerk

Die TrutzBox funktioniert auf Netzwerk-Ebene wie ein Router. Sie trennt das Netzwerk zwischen dem externen (unsicheren) und dem internen (sicheren) Netzwerk auf. Für Geräte, die über die TrutzBox kommunizieren, werden für alle Ports, für die eine Anwendung auf der TrutzBox bereit steht (Mail, www-Proxy, Chat, Video-Konferenz...), die Zugriffe über den jeweiligen TCP-Port auf die TrutzBox-Anwendung umgeleitet. Somit ist die TrutzBox in der Lage, für diese Anwendungen den Datentransfer in beiden Richtungen zu kontrollieren und unerwünschte Daten zu blockieren oder zu pseudonymisieren.



(© 2017 Comidio GmbH)

Das TrutzBox externe (unsichere) Netzwerk

Die TrutzBox wird mit dem LAN-Ext-Anschluss per LAN-Kabel am Internet-Router angeschlossen. Beim Hochfahren (Booten) der TrutzBox bezieht sie eine (aus TrutzBox-Sicht) externe IP-Adresse vom DHCP-Server des Routers. Diese kann ein IPv4- oder auch IPv6-Adresse sein. Dabei teilt sie dem DHCP-Server ihren Host-Namen „trutzbox“ mit.
Beim Setup der TrutzBox kann der TrutzBox auch eine feste IP-Adresse zugewiesen werden. Diese Einstellung (DHCP oder feste IP-Adresse) kann auch nachträglich unter „Netzwerk -> „Status“ geändert werden.

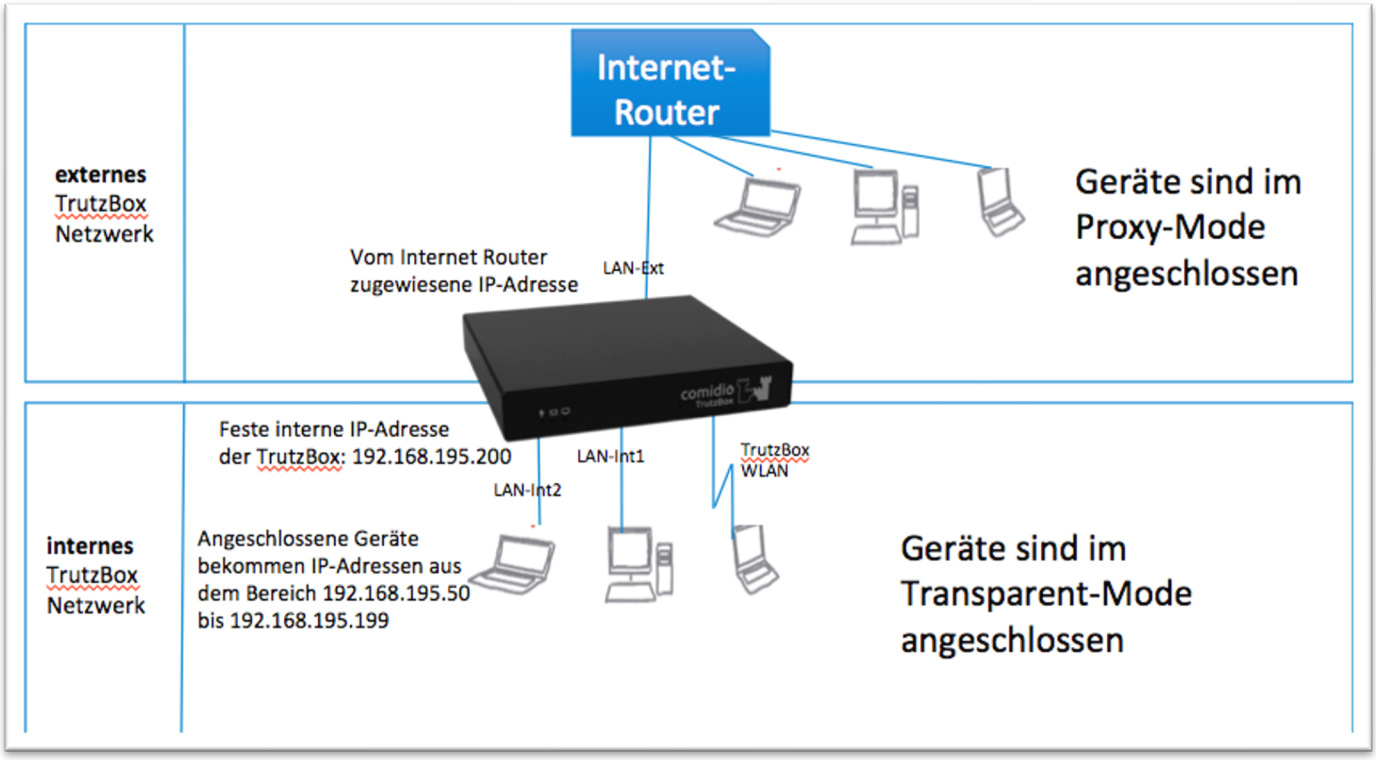
Das TrutzBox interne (sichere) Netzwerk

Um höchstmögliche Sicherheit für die an der TrutzBox angeschlossenen Geräte zu gewährleisten, baut die TrutzBox ein eigenes, vom Internet-Router getrenntes internes (sicheres) Netzwerk auf. Die TrutzBox stellt drei Netzwerk-Interfaces zur Verfügung, über die Geräte an das interne Netzwerk angeschlossen werden können: (optional), LAN-Int1 und LAN-Int2. Diese drei Netzwerk-Anschlüsse sind in einer Netzwerk-Bridge zusammen geschaltet. Sie bilden somit zusammen ein einzelnes Netzwerk. Alle daran angeschlossenen Geräte können ungehindert untereinander kommunizieren.
Falls mehr LAN-Anschlüsse benötigt werden, können diese Netzwerk-Anschlüsse auch durch Router, Hubs, Switchs oder WLAN-Router erweitert werden. Durch einen DHCP-Server bekommen die angeschlossenen Geräte (die Geräte, die im Transparent-Mode angeschlossen sind) eine neue IP-Adresse aus dem Bereich 192.168.195.50 bis 192.168.195.199. Ein eigener DNS-Server (dnsmask) leitet dabei die

Namensauflösung für die angeschlossenen Geräte an den DNS-Server des Internet-Routers weiter. Die TrutzBox vergibt im internen Netzwerk nur IPv4-Adressen, keine IPv6-Adressen.

Die TrutzBox übernimmt das Routing zwischen dem TrutzBox internen Netzwerk (WLAN, LAN-Int1 und LAN-Int2) und dem TrutzBox externen Netzwerk (LAN-Anschluss “LAN-Ext”).

Die TrutzBox selbst hat im internen Netzwerk immer die IP-Adresse 192.168.195.200.



(© 2017 Comidio GmbH)

Einem angeschlossenen Gerät kann auch eine fest zugeordnete (statische) IP-Adresse aus dem Bereich 192.168.195.50 bis 192.168.195.199. vergeben werden. Subnet mask ist dann 255.255.255.0, die Router- und DNS-Server-IP-Adresse ist 192.168.195.200

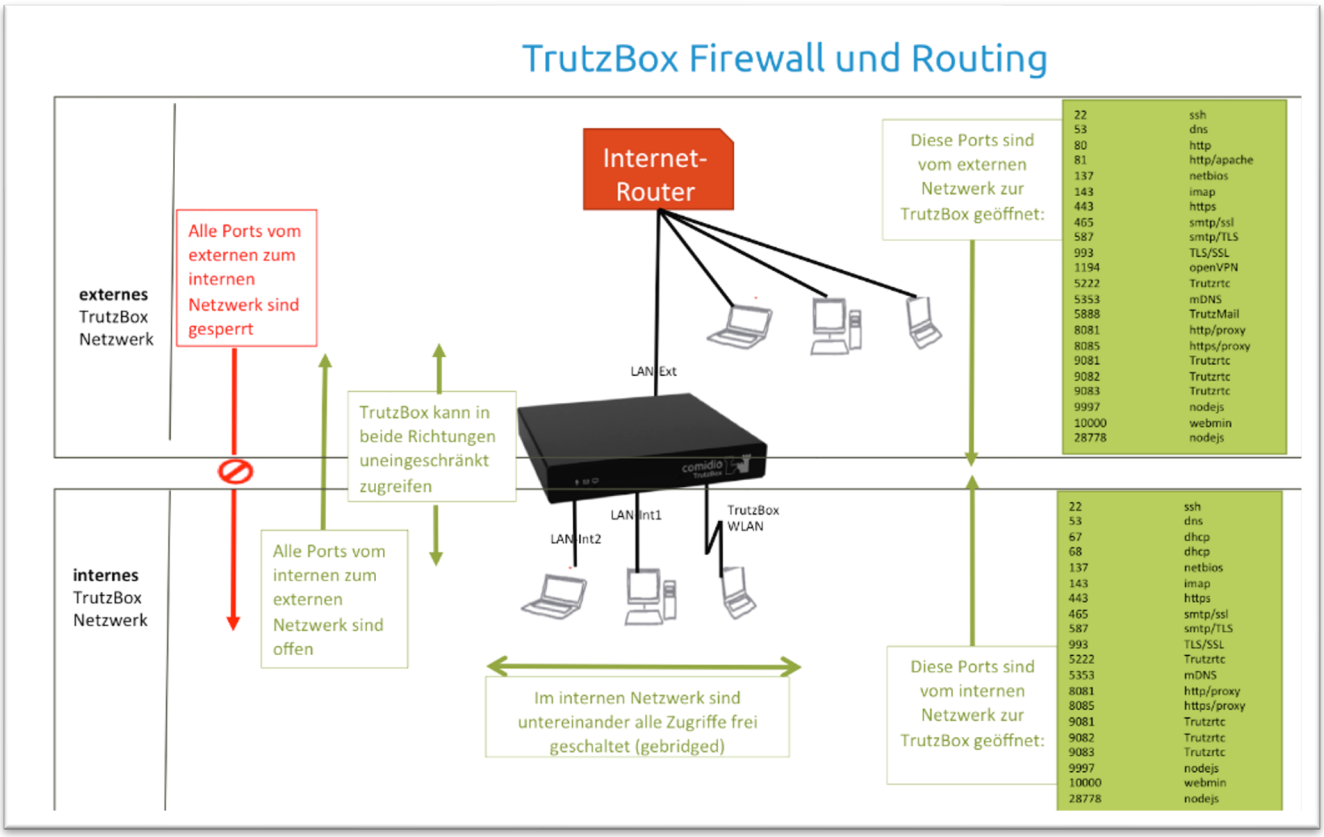
Firewall

Um sowohl die TrutzBox als auch das daran angeschlossene interne Netzwerk zusätzlich zu schützen, wurde eine Statefull-Inspection Firewall installiert. Diese schützt nicht nur die TrutzBox selbst vor unbefugten Zugriff auf Netzwerkseite, sondern blockiert auch Angreifer von außen. Zusätzlich schützt die Firewall alle angeschlossenen Netzwerkgeräte über entsprechende Portfreigaben vor unkontrolliertem Netzwerkzugriff.

Die verwendete Firewall ist eine Stateful Packet Inspection Firewall (SPI), d.h. jedes Datenpaket wird einer bestimmten aktiven Verbindung (Session) zugeordnet:

- Alle am internen Netzwerk angeschlossenen Geräte sind untereinander gebridged, sodass diese uneingeschränkt miteinander kommunizieren können.
- Alle angeschlossenen Geräte können auf allen Ports Verbindungen nach „extern“ (LAN-Ext) aufbauen. Wenn ein Gerät am internen Netzwerk auf ein Gerät am Internet-Router (externes Netzwerk) zugreifen möchte, dann muss ein voll qualifizierter Hostnamen verwendet werden (also z.B. fritz.box angehängt werden). Alle Verbindungen über Port 80/443 werden dabei automatisch über den TrutzBox Proxy (Filter) geleitet, der dann die ein- und ausgehenden Daten kontrolliert.
- Ein Verbindungsaufbau von extern zur TrutzBox ist nur für spezielle Ports freigeschaltet.
- Ein Verbindungsaufbau vom externen Netzwerk nach intern ist nicht freigeschaltet und somit nicht erlaubt.

Für IPv6 Verbindungen läuft auf der TrutzBox eine zweite Firewall, die den gleichen Regelsatz wie die IPv4-Firewall enthält. Somit kann die TrutzBox am Ext-Anschluss sowohl eine IPv4 als auch eine IPv6 Adresse beziehen, die von zwei Firewalls überwacht werden.

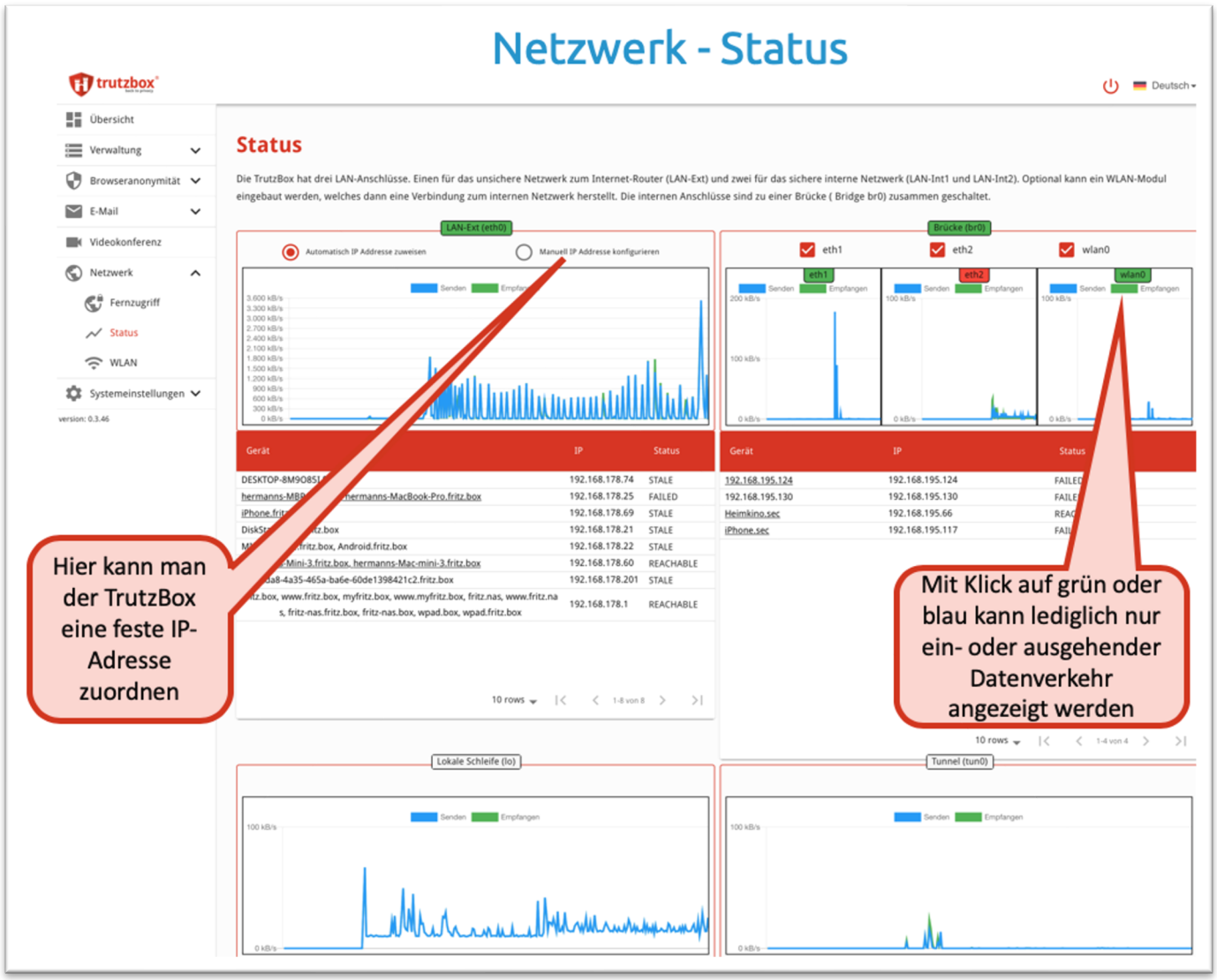


(© 2017 Comidio GmbH)

Als Basis für die Firewall wird die Open-Source Firewall „iptables“ verwendet. Zusätzlich wird als Add-On das Package Shorewall Firewall zur Verfügung gestellt, um für Experten weitere Funktionen wie z.B. die vereinfachte Benutzerführung oder Einrichtung von Zonen zu erreichen.

Netzwerk - Status

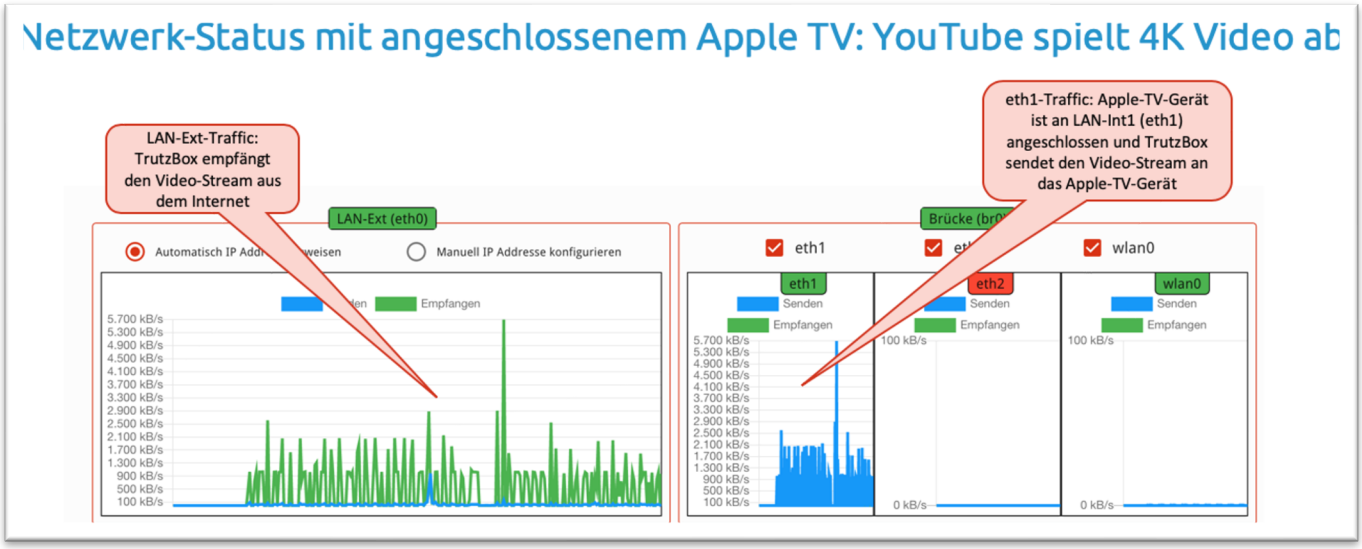
Die Netzwerk-Übersicht der TrutzBox gibt eine gute Übersicht über den aktuellen Netzwerk-Verkehr. Somit kann damit auch ungewöhnlicher oder nicht erwarteter Netzwerk-Verkehr entdeckt werden



(© 2020 Comidio GmbH)

Die bei den jeweiligen Netzwerk-Interfaces angezeigten Geräte ermittelt die TrutzBox durch einen Network-Scan. In der Regel werden hier mehr Geräte als bei der Geräte-Liste des Proxies angezeigt, da hier auch Geräte gefunden werden, die zwar im gleichen Netz der TrutzBox hängen, aber keinen Kontakt mit der TrutzBox hatten. Der Netzwerkverkehr in den jeweiligen Grafiken, ist jedoch der Netzwerkverkehr, der durch das entsprechende TrutzBox-Netzwerk-interface geflossen ist.

In folgendem Beispiel wird per YouTube auf einem AppleTV-Gerät, das an den internen LAN-Int1-Anschluss angeschlossen ist, ein 4K Video über die TrutzBox abgespielt.



(© 2020 Comidio GmbH)

Network Intrusion Detection System (N-IDS)

Ein Netzwerk basiertes Intrusion Detection System (N-IDS) besitzt die Fähigkeit, in Echtzeit den Netzwerk-Traffic zu analysieren und entsprechend zu protokollieren. Der Inhalt der Pakete des Datenstroms wird mit charakteristischen Mustern von bekannten Angriffen verglichen. Diese Muster werden allgemein Signaturen genannt, die bei einem IDS in „Rules“ (Regeln) festgehalten werden. Zur Mustererkennung wird das Werkzeug Snort eingesetzt. Dieses verwendet den Aho-Corasick-Algorithmus. Inzwischen gibt es für Snort einige tausend Signaturen. Da international sehr häufig neue Angriffsmethoden auf Computer und Netzwerke bekannt werden, sollte die Sammlung der Signaturen (ähnlich wie bei Virenscannern) regelmäßig aktualisiert werden. Snort wird allgemein genutzt, um aktiv Netzwerkverkehr zu blockieren. oder passiv verschiedene Formen eines Angriffs zu erkennen.
Ein IDS kann eingesetzt werden, um bekannte Angriffe auf die Schwachstellen von Netzwerksoftware zu entdecken. So führt z.B. Snort Protokollanalysen durch, sucht und vergleicht Inhalte, um passiv verschiedene Formen eines Angriffs, wie zum Beispiel einen Pufferüberlauf, Portscans, Angriffe auf Web-Anwendungen oder SMB-Probes zu erkennen. Möglichkeiten für Angriffe sind gegeben durch so genannte Exploits, oder eigens dafür bestimmte Programme, wie etwa Internet-Würmer (z. B. Sasser oder W32.Blaster) die ihrerseits wiederum ein Backdoor-Programm (ursprünglich Administrator Hintertüre bzw. der Wartungszugang) beinhalten können (bzw. selbst eines sind), durch das der eigentliche Angriff schlussendlich erfolgt. Bei einem erkannten Angriff kann zum Beispiel ein Alarm ausgelöst und die Netzwerkpakete zur späteren Analyse oder Beweissicherung mitgeschrieben werden.

Host Intrusion Detection System (H-IDS)

Ein Host-IDS funktioniert ähnlich wie das bereits erwähnte N-IDS, nur bezieht es sich hier auf das System selbst. Das H-IDS läuft damit im Hintergrund zur Vorbeugung gegen Einbrüche und erkennt ein mögliches Eindringen auf die TrutzBox selbst und wehrt diesen Eindringling ab.
Das H-IDS erhält seine Informationen aus Log-Dateien, Kernel-Daten und anderen Systemdaten, wie etwa der Registrierungsdatenbank. Es schlägt Alarm, sobald es in den überwachten Daten einen vermeintlichen Angriff erkennt.

Intrusion Prevention System (IPS) oder Deep-Packed-Inspection (DPI)

DPI ist eine Kombination von Netzwerk-Sicherheitstools, die nicht nur die Kommunikation kontrollieren, sondern Datenpakete auch analysieren und verstehen können.
Dazu dient zum einen ein Intrusion Detection System, wie oben beschrieben, welches die Datenpakete überwacht und zum anderen ein Intrusion Prevention System, welches geeignete Gegenmaßnahmen ergreift. DPI wird in einer späteren TrutzBox Version zur Verfügung stehen.
Durch all diese Maßnahmen bietet die TrutzBox einen zusätzlichen Schutz vor Netzwerkangriffen.

Schutz der TrutzBox selbst:

Die TrutzBox ist von Hause aus bereits durch den richtigen Einsatz des Betriebssystems Linux gut vor Viren geschützt. Zusätzlich ist das Betriebssystem noch abgesichert, siehe Beschreibung unten.

Fernzugriff - VPN - Virtual Private Network

Die TrutzBox steht typischer Weise zu Hause oder in einer Firma. Um die TrutzBox Funktionen auch unterwegs nutzen zu können sollte man die TrutzBox nicht mitnehmen, sondern den Fernzugriff auf der TrutzBox aktivieren. Der Fernzugriff auf die TrutzBox wird durch ein VPN realisiert.
VPN bedeutet „virtual private network“. Ein VPN verbindet ein Gerät über ein unsicheres Netzwerk (das Internet) mit einem privaten Netzwerk (z.B. Firmen- oder Heimnetzwerk). Es ermöglicht einem Computer über ein öffentliches Netzwerk Daten auszutauschen, als wäre der Computer direkt mit dem Firmen- oder Heimnetzwerk verbunden. Über einen solchen VPN Zugang können TrutzBox Nutzer die gesamte TrutzBox Funktionalität auch von außerhalb des Heimnetzwerks nutzen, z.B. von unterwegs mit dem Smartphone.
Dadurch bietet dieser Zugang die gleiche Funktionalität, Sicherheit und Kontrollmechanismen wie aus dem privaten Netzwerk zu Hause oder in der Firma. Eine VPN-Verbindung wird erreicht, indem eine virtuelle Punkt-zu-Punkt Verbindung vom Endgerät, über das Internet, zu der TrutzBox, mit entsprechender Authentisierung und Verschlüsselung aufgebaut wird. Eine VPN-Verbindung kann auch aus dem lokalen Netzwerk heraus aufgebaut werden.
Mit VPN ist es dem TrutzBox Besitzer auch möglich, anderen (z.B. Freunden, Verwandten oder Mitarbeitern) Zugriff auf eine TrutzBox zu geben und diese mitzubenutzen. Die TrutzBox ermöglicht diese

Mitbenutzung zwar, aber Comidio empfiehlt das Mitbenutzen der TrutzBox nur dann, wenn die Mitbenutzer Vertrauen in den TrutzBox-Administrator haben. Der Administrator der TrutzBox wäre zumindest technisch in der Lage, diese Nutzer zu überwachen und auf vertrauliche Informationen zuzugreifen.
Des Weiteren sollte man bei Nutzung von VPN darauf achten, dass die eigene Internet-Verbindung (vor allem die Upload Geschwindigkeit) genügend Durchsatz bietet.
Um den Fernzugriff nutzen zu können, muss der eigene Internet-Anschluss vom Internet aus erreichbar sein. Leider ist das nicht immer der Fall. Meist sind z.B. Mobilfunkverbindungen vom Internet aus nicht erreichbar. Auch kommt es immer öffter vor, dass der private Internet-Provider keine echte, eindeutige IPv4 Adresse dem eigenen Internet-Anschluss zuordnet, sondern lediglich nur einen „Dual-Stack Lite“ Anschluss zur verfügung stellt. In diesem Fall wird die lokale externe IPv4-Adresse dürch ein IPv6-Netzwerk geroutet und die IPv4-Adresse ist nicht eindeutig und nicht von außen erreichbar.

Wenn die TrutzBox z.B. über über eine Mobilfunkverbindung am Internet hängt, oder nur über „Dual-Stack“ am Internet angebunden ist, kann es sein, dass die TrutzBox nicht über VPN erreichbar ist.

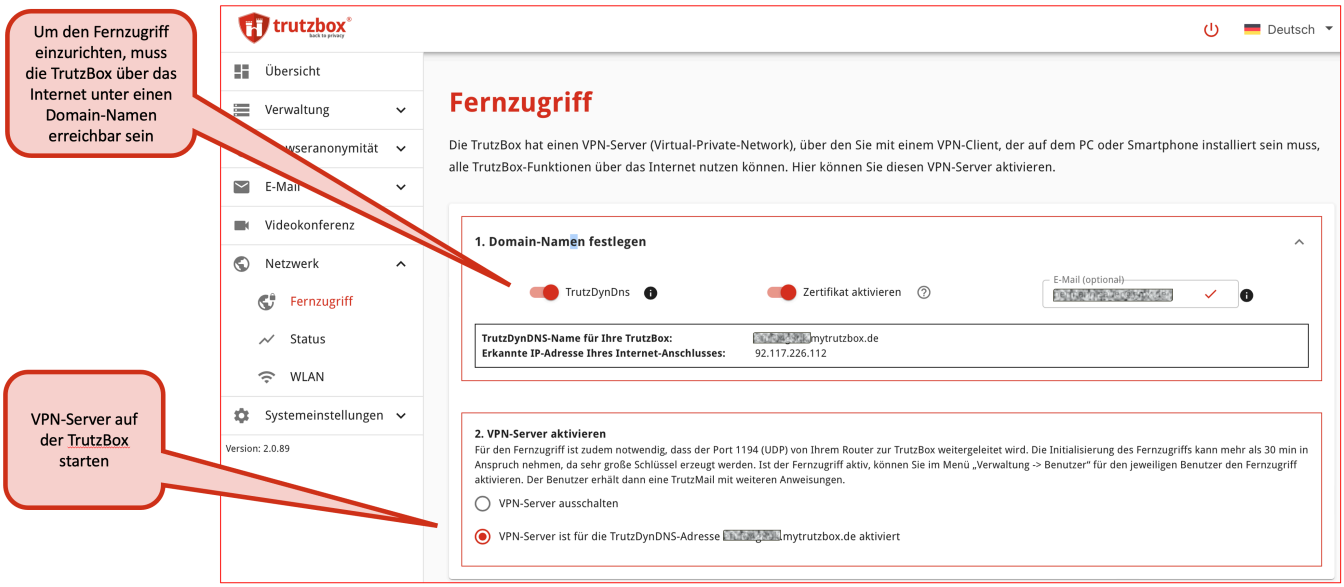
TrutzBox auf Fernzugriff vorbereiten, Let´s Encrypt Zertifikat aktivieren und Internet-Router frei schalten

Um von unterwegs, z.B. Hotel, auf die TrutzBox zugreifen zu können, muss das Heimnetzwerk, an dem die TrutzBox angeschlossen ist, über einen Domain-Namen erreichbar sein.
Da das VPN-Zertifikat auf den Domain-Namen ausgestellt wird, kann man erst nachdem ein Domain-Name angegeben wurde, den Fernzugriff auf die TrutzBox aktivieren.

Die eingesetzte VPN Lösung auf der TrutzBox (VPN-Server) basiert auf OpenVPN. Um VPN (Fernzugriff) nutzen zu können, müssen auf der TrutzBox unter „Netzwerk“ -> Fernzugriff“ zunächst zwei Schritte durchgeführt werden:
1. „TrutzDynDNS“ und „Zertifikat aktivieren“
2. „VPN-Server aktivieren und warten, bis die VPN-Server-Schlüssel generiert wurden

Die Generierung des SSL-Zertifikats für den TrutzDynDNS-Namen wird automatisch über letsencrypt.org eingerichtet. Da Letsencrypt nur 5 Zertifikate pro Woche erlaubt, sollte man dieses Flag nicht mehr als 5 mal pro Woche einschalten (https://letsencrypt.org/docs/rate-limits/).

Fernzugriff

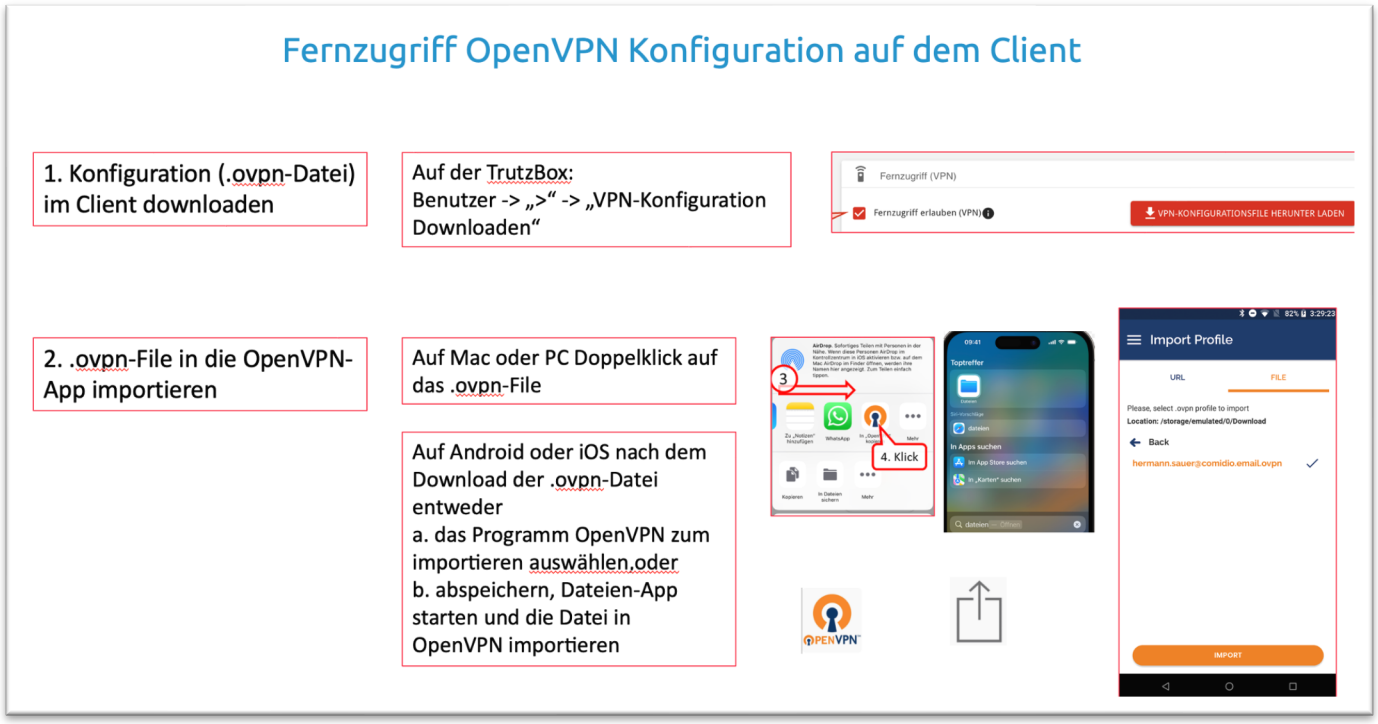


(© 2020 Comidio GmbH)

Bei der Aktivierung des Fernzugriffs wird der VPN-Server auf der TrutzBox eingerichtet. Dabei wird auch ein sicherer OpenVPN-Server-Schlüssel auf der TrutzBox generiert, was sehr lange dauern kann (bis zu 30 min).
Um auf die TrutzBox von außen über das VPN-Protokoll zugreifen zu können, muss auf dem Internet-Router der UDP-Port 1194 (TrutzBox-VPN Portfreigabe) zur TrutzBox weiter geleitet werden.

Mobiles Gerät für den Fernzugriff vorbereiten

Nachdem der Fernzugriff auf der TrutzBox aktiviert wurde, steht für jeden eingerichteten TrutzBox Benutzer, der eine TrutzMail Adresse hat, unter dem Menüpunkt „Benutzer Verwalten" eine neue Option „Fernzugriff" zur Verfügung. Wenn diese Option für einen Benutzer aktiviert wird, bekommt der Benutzer ein OpenVPN-Client-Zertifikat generiert, das ihm per OpenVPN-Konfigurationsfile über TrutzMail automatisch zugeschickt wird. Dieses OpenVPN-Konfigurationfile (.ovpn) kann dieser dann auf allen seinen mobilen Geräten im OpenVPN-Programm importieren.
In der Benutzerverwaltung kann dieses OpenVPN-Konfigurationsfile auch nachträglich herunter geladen werden.
Als VPN-Client-Programm für iPhone, Android und Windows hat sich dazu „openvpn" (openvpn.net) und für MAC Tunnelblick (tunnelblick.net) bewährt. Eine Liste von VPN-Clients ist hier zu finden: https://de.wikipedia.org/wiki/OpenVPN#Frontends.
Danach kann unterwegs von einem beliebigen Internet-Anschluss auf die TrutzBox im Unternehmen oder zu Hause zugegriffen und alle Funktionen der TrutzBox genutzt werden.

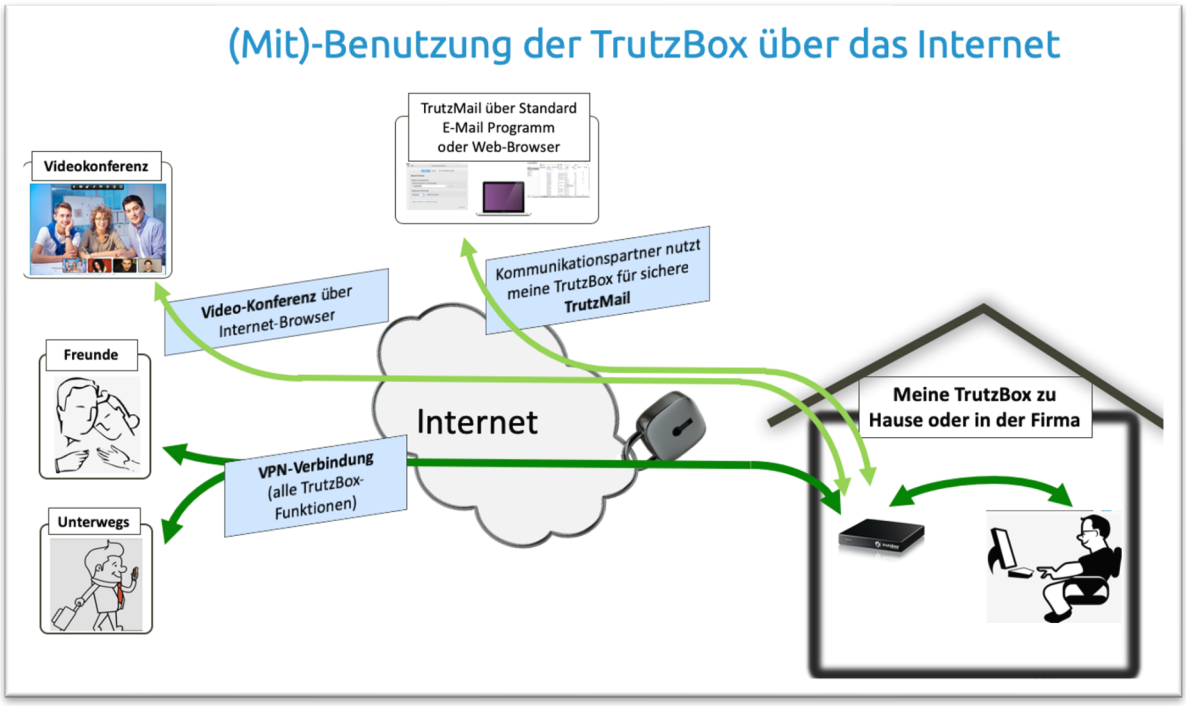


(© 2024 Comidio GmbH)

TrutzBox-Funktionen über das Internet nutzen, ohne zuvor eine VPN-Verbindung auf zu bauen, also ohne die Fernzugriffsfunktion

Mit dem oben beschriebenen Fernzugriff bekommt man per VPN-Verbindung über das Internet vollen Zugriff auf alle Funktionen der TrutzBox. Somit ist VPN auch für den Administrator geeignet.
Es gibt auch die Möglichkeit, den Zugriff auf einzelne Anwendungen ohne VPN-Verbindung zu ermöglichen. Das macht Sinn, z.B. bei der Nutzung von

- TrutzRTC (Video-Konferenz), bei dem ein Teilnehmer lediglich im Browser den Domain-Namen eingeben muss. Z.B: https://efuf99g8iz.mytrutzbox.de/trutzrtc/raumname
- Nutzung von TrutzMail (also des TrutzBox-Mail-Servers). Dort beim konfigurieren des Mail-Accounts im Mail-Client unter „Server“ den Domain-Namen eintragen oder den Web-Mailer der TrutzBox z.B. mit https:// efuf99g8iz.mytrutzbox.de/mail aufrufen
- oder auch bei Nutzung des XMPP-Servers. Dort beim konfigurieren des XMPP-Accounts im XMPP-Client unter „XMPP-Server“ den Domain-Namen eintragen



(© 2020 Comidio GmbH)

Für den Zugriff auf einzelne TrutzBox-Anwendungen über das Internet wird ein SSL-Zertifikat für die TrutzBox-DynDNS-Domain benötigt. Dieses SSL-Zertifikat kann durch Aktivierung der Option „Zertifikat aktivieren“ im Menü „Netzwerk“ -> „Fernzugriff“ aktiviert werden.
Hier noch einmal der Hinweis, dass für die Nutzung von TrutzBox-Funktionen über das Internet, ohne dass zuvor eine VPN-Verbindung aufgebaut wurde, auf dem Internet-Router an dem die TrutzBox angeschlossen ist, die entsprechenden Ports für die Anwendung geöffnet werden müssen.

IPv6 Unterstützung

Grundsätzlich unterstützt die TrutzBox auch IPv6 auf dem externen Netzwerk. Aufgrund der Eigenarten von IPv6, gerade in Kombination mit IPv4, ist jedoch einiges zu beachten.
Dabei muss man drei Netzwerke unterscheiden:

1. Die IP-Adresse des Internet-Anschlusses am Internet-Router (z.B. FritzBox): hier ist IPv6 zunächst problemlos in Verbindung mit der TrutzBox zu nutzen, wobei die IPv6-Adresse der Internet-Service-Provider liefert. Es kann lediglich Probleme mit VPN-Zugriffen über das Internet zum eigenen Internet-Anschluss kommen, wenn das externe Gerät eine IPv6 Adresse hat. Stichwort "DS-Lite-Tunnel“. Das hat jedoch nichts mit der TrutzBox zu tun.
2. Internes Netzwerk, also ihre Geräte, die mit dem Internet-Router verbunden sind. Dazu gehört dann auch die TrutzBox, die per LAN-Kabel an den Internet-Router angeschlossen wird. Hier kann die TrutzBox vom Internet-Router eine IPv6-Adresse bekommen, was uneingeschränkt funktioniert. Geräte, die die TrutzBox nutzen sollen, können am internen Netzwerk verbleiben (also am Internet-Router - "Proxy-Mode",). Diese Geräte können auch eine IPv6-Adresse bekommen. Da es unter IPv6 allerdings nicht möglich ist, den Hostnamen eines angeschlossenen Geräts

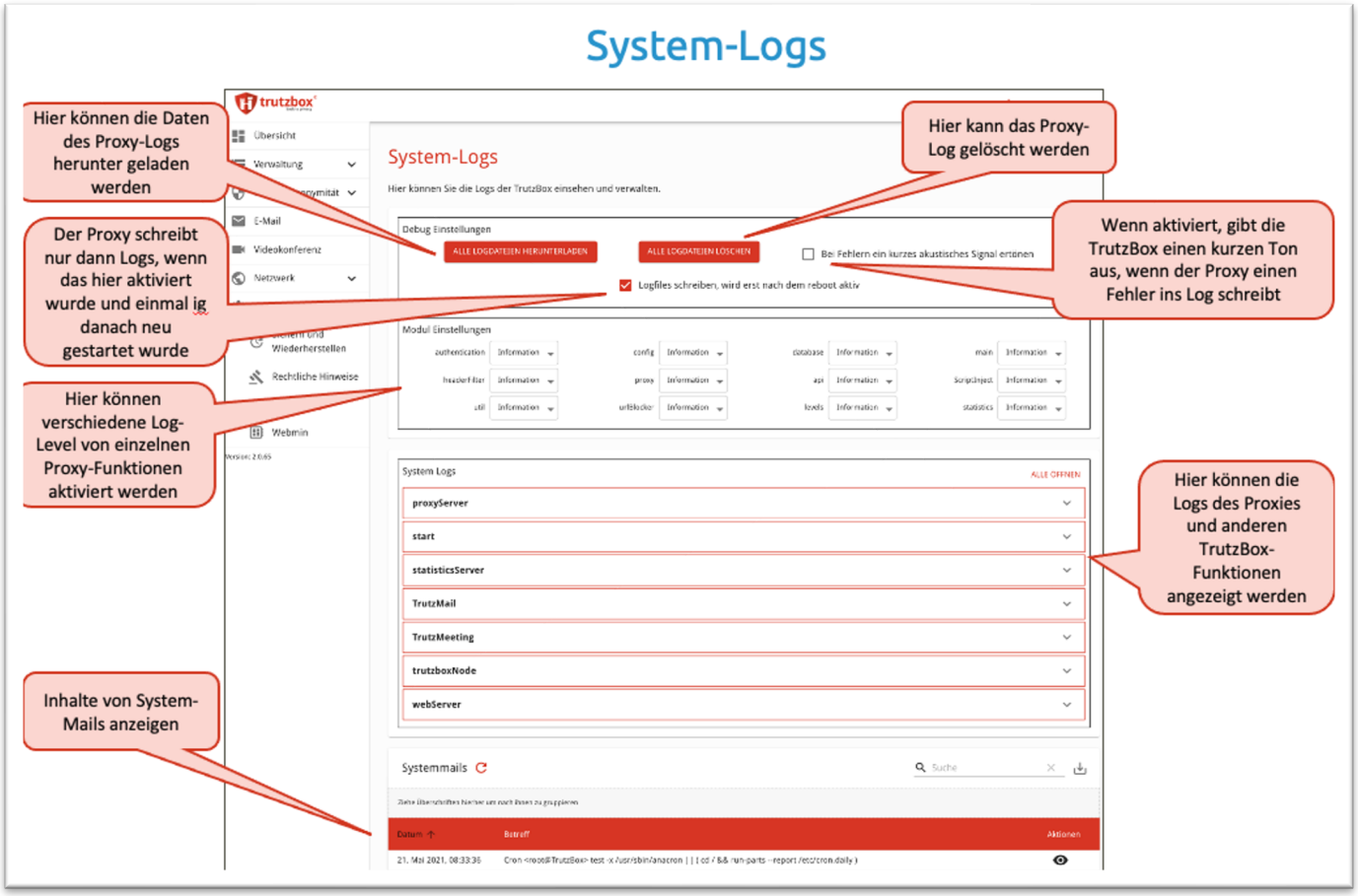
zu ermitteln, raten wir grundsätzlich davon ab, im internen Netz solche Geräte unter IPv6 zu betreiben (kann i.d.R. im angeschlossenen Gerät eingestellt werden).

3. Da die TrutzBox wie ein Router funktioniert, können auch Geräte an das interne TrutzBox-Netzwerk angeschlossen werden (Transparent-Mode). In diesem Fall muss in dem angeschlossenen Gerät kein Proxy konfiguriert werden. Geräte die am TrutzBox internen Netzwerk angeschlossen sind, werden im „Transparent-Mode“ betrieben. Da die TrutzBox lediglich IPv4 Adressen auf ihrem internen Netzwerk vergibt, können solche Geräte nur mit IPv4 betrieben werden.

Um das Thema IPv6-Unterstützung etwas einfacher zusammen zu fassen gilt Folgendes: die IP-Adresse des Internet-Service-Providers kann eine IPv6-Adresse sein. Im internen Netzwerk raten wir in Home-Netzwerken grundsätzlich (also auch ohne TrutzBox) von der Nutzung von IPv6 ab, da es eigentlich auch keine Vorteile bringt.

System-Logs

Unter System-Logs werden Information aus zwei verschiedenen Quellen angezeigt. Hier ist es zum einen möglich, den Proxy im Detail zu debuggen und zum anderen, werden hier Inhalte von Mails angezeigt, die das Betriebssystem selbständig sendet.



(© 2021 Comidio GmbH)

Proxy debuggen

In dem Menü „Modul Einstellungen“ ist es möglich, den Proxy im Detail zu debuggen. Damit der Proxy Debug Informationen ins Log-File schreibt, muss diese Funktion zunächst mit aktvieren von "Logfiles schreiben, wird erst nach dem reboot aktiv“ frei geschaltet werden. In den Modul-Einstellungen können verschiedene Log-Level von einzelnen Proxy-Funktionen aktiviert werden. Auf Level „Information“ werden nur sehr elementare Informationen geschrieben. Das ist die Default Einstellung. Auf Level „Debug“ gibt es meist genügend Informationen, um den Proxy zu analysieren.
Da die TrutzBox mit diesen Funktionen evtl. sehr viele Daten ins Log-File schreibt, sollte diese Debug-Funktion nur mit Bedacht und nur für kurze Zeit aktiviert werden, um ein Überlauf der SSD-Platte zu vermeiden.
Alle Log-Files werden nach voreingestellten Zeiten komprimiert und später dann gelöscht.

Systemmails

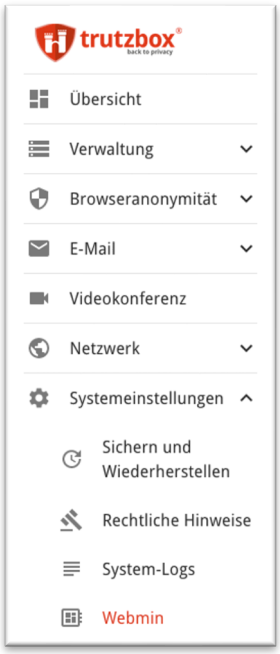
Das TrutzBox Betriebssystem sendet regelmäßig interne E-Mails um bestimmte Vorgänge mitzuteilen. Diese internen E-Mails können hier abgerufen werden. Diese E-Mails werden nur kurze Zeit gehalten und danach automatisch gelöscht.

Systemeinstellungen (Webmin)

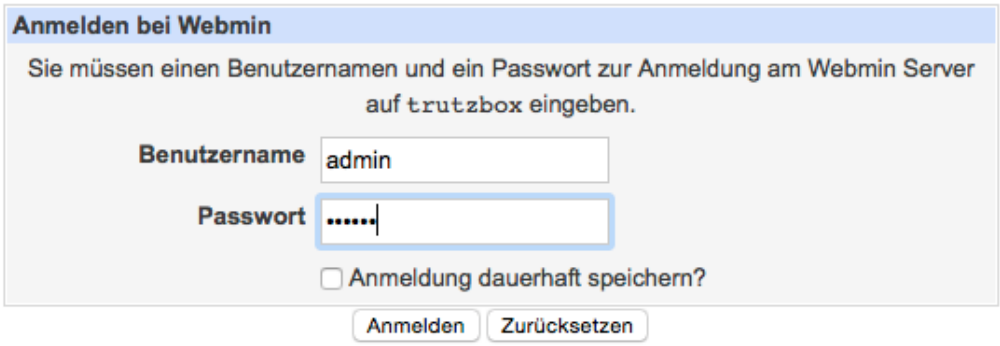
Einige sehr betriebsystemnahe Funktionen, können mit dem Werkzeug „Webmin“ bedient werden. Webmin wird standardmäßig auf der TrutzBox ausgeliefert und mit dem Menüpunkt „Systemeinstellungen“ ->“Webmin“ aufgerufen.

Wichtig: Webmin sollte nur von erfahrenen Linux Administratoren benutzt werden, da es mit diesem Werkzeug möglich ist, die Konfiguration der TrutzBox derart zu verstellen, dass diese nicht mehr nutzbar ist!

In einem solchen Fall kann es passieren, dass die TrutzBox nur noch durch Zurücksetzen auf Werkseinstellung wieder funktionsbereit gemacht werden kann. Dadurch gehen allerdings alle TrutzBox Daten (z.B. E-Mails) und Einstellungen verloren!

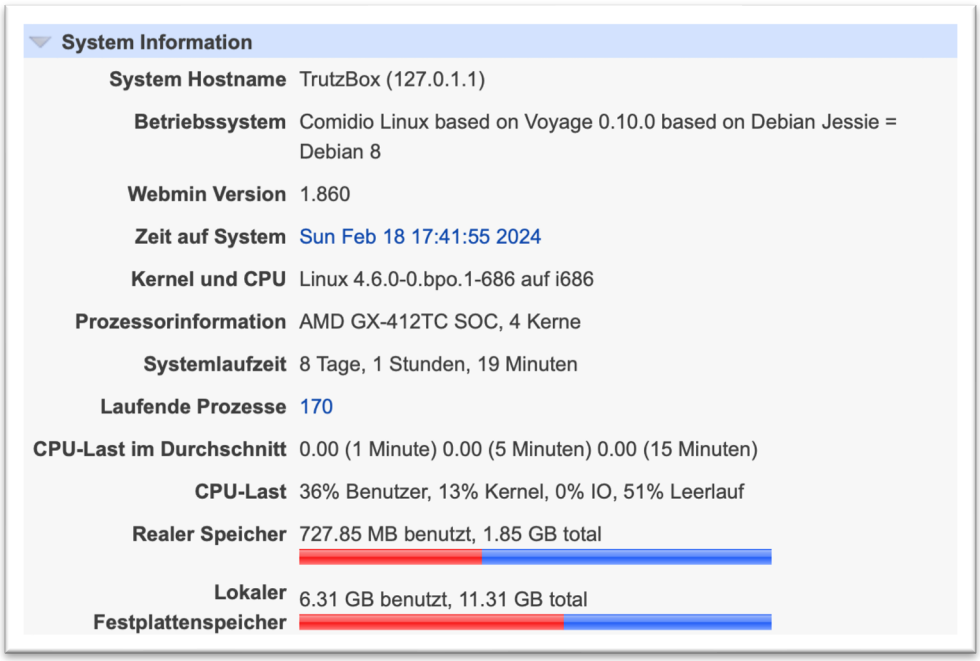


Da es sich bei Webmin[251] um ein eigenständiges Programm handelt, ist es notwendig, sich zunächst neu einzuloggen. Dazu bitte als Benutzernamen „admin“ und das TrutzBox Administrator Passwort eingeben.

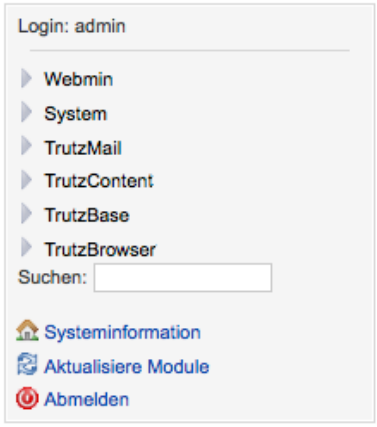


Nach dem Anmelden zeigt Webmin eine zusammengefasste Übersicht der Systeminformationen an:

[251] http://doxfer.webmin.com/Webmin/Main_Page



Evtl. ausstehende Updates der TrutzBox können direkt mit dem Link nach „Paket-Updates“ verwaltet werden. Das manuelle Einspielen von Updates sollte nur nach Rücksprache mit dem TrutzBox-Support durchgeführt werden, da Updates normalerweise immer automatisch eingespielt werden.
Über das Webmin Menü



können dann weitere systemnahe Einstellungen vorgenommen werden. Die wichtigsten sind:

- „Webmin“ selbst konfigurieren, z.B. weitere Webmin Funktionen aus dem Internet laden und installieren
- „System“ Betriebssystem-nahe Funktionen ausführen, z.B. neue Software Pakete zuladen und installieren
- „TrutzMail“ Mail-Eingangs- und Mail-Ausgangs-Server verwalten, TrutzMail Spam-Filter verwalten

- „TrutzBase“ Firewall, Antivirus und Netzwerk-Konfiguration. Hier werden zukünftig weitere Netzwerk Tools zur Verfügung stehen. Hier ist es auch möglich, bei Netzwerk Problemen im Menüpunkt „Shoreline Firewall“, die Firewall temporär auszuschalten:

  1. Konfiguration anwenden - Startet die Firewall neu mit der eingegebenen Konfiguration
  2. Konfiguration aktualisieren - Unbenutzt, keine Änderung
  3. Lösche Firewall - Ausschalten der Firewall
  4. Stoppe Firewall - Firewall wird gestoppt und verhindert den Zugang ins Internet, Zugriffe auf die TrutzBox bleiben erhalten
  5. Zeige Status - Zeigt den Status der Firewall an, z.B. dass die Firewall aktiv ist und seit wann
  6. Prüfe Firewall - Überprüft die Regeln der Firewall und zeigt mögliche Fehler an
  7. Zeige Dump - Führt einen Dump aus und zeigt die Ergebnisse in einer Tabelle an
  8. „TrutzBrowse“ - Web-Server Einstellungen

Über Webmin den Systemstatus der TrutzBox auf den eigenen PC geladen

9. Solange man in Webmin eingeloggt ist, wird durch Eingabe des Links: *https://trutzbox:10000/sysinfo.cgi* eine Datei, die den Systemstatus der TrutzBox enthält auf den eigenen PC geladen. Dieser kann dann, evtl. zusammen mit Log-Files, zur Analyse an Comidio geschickt werden.

TrutzBox mit Hilfe von Webmin auf Werkseinstellung zurücksetzen

Da Webmin unabhängig von der restlichen TrutzBox Software läuft und einen eigenen Web-Server hat, ist die Wahrscheinlichkeit groß, dass im Fall einer Störung der TrutzBox, Webmin noch funktioniert. Somit ist Webmin ein nützliches Werkzeug, das im Fall einer Fehlfunktion des TrutzBox Admin-Userinterfaces zur Analyse und Reparatur der TrutzBox verwendet werden kann.
Dazu zunächst in Webmin mit dem Link https://trutzbox:10000 aufrufen und einloggen. Unter dem Menüpunkt „System“ -> „Kommandozeile“ ist es möglich, ein Systemkommando auf der TrutzBox (Shell) abzusetzen.
Dort bitte rechts neben dem Knopf „Führe Befehl aus:“ das Kommando

/usr/lib/comidio/trutzbox/prepareFactoryReset.sh

eintragen und dann den Knopf „Führe Befehl aus:“ drücken. Damit wird das Zurücksetzen der TrutzBox, wie im Handbuch beschrieben, angestoßen.

TrutzBox Betriebssystem

Comidio hält sich, soweit möglich, an die sieben Prinzipien des „Privacy by Design“ (PbD)[252]. Da Comidio ein kommerzielles Unternehmen ist, kann allerdings nicht garantiert werden, dass alle sieben Prinzipien vollständig eingehalten werden können.
Um bestmögliche Sicherheit zu bieten, muss es dem Markt möglich sein, die TrutzBox Software von neutralen Dritten zu verifizieren. Quelloffenheit ist ein wichtiges PbD Prinzip. Das TrutzBox Betriebssystem basiert auf dem Debian-Derivat Voyage[253] (Linux), das von Comidio besonders abgesichert wurde. Sämtliche TrutzBox-Software ist Quelloffen.
Auf dem Betriebssystem wurde eine webbasierende Management Konsole implementiert (TrutzBox User-Interface), die es einem TrutzBox Administrator unter anderem erlaubt, die Benutzer und die TrutzBox Funktionalitäten zu verwalten.
Um die TrutzBox Software und TrutzBrowse/TrutzContent Blacklists aktuell halten zu können, wurde das Standard „Debian Package Manager“ (dpkg) verwendet.

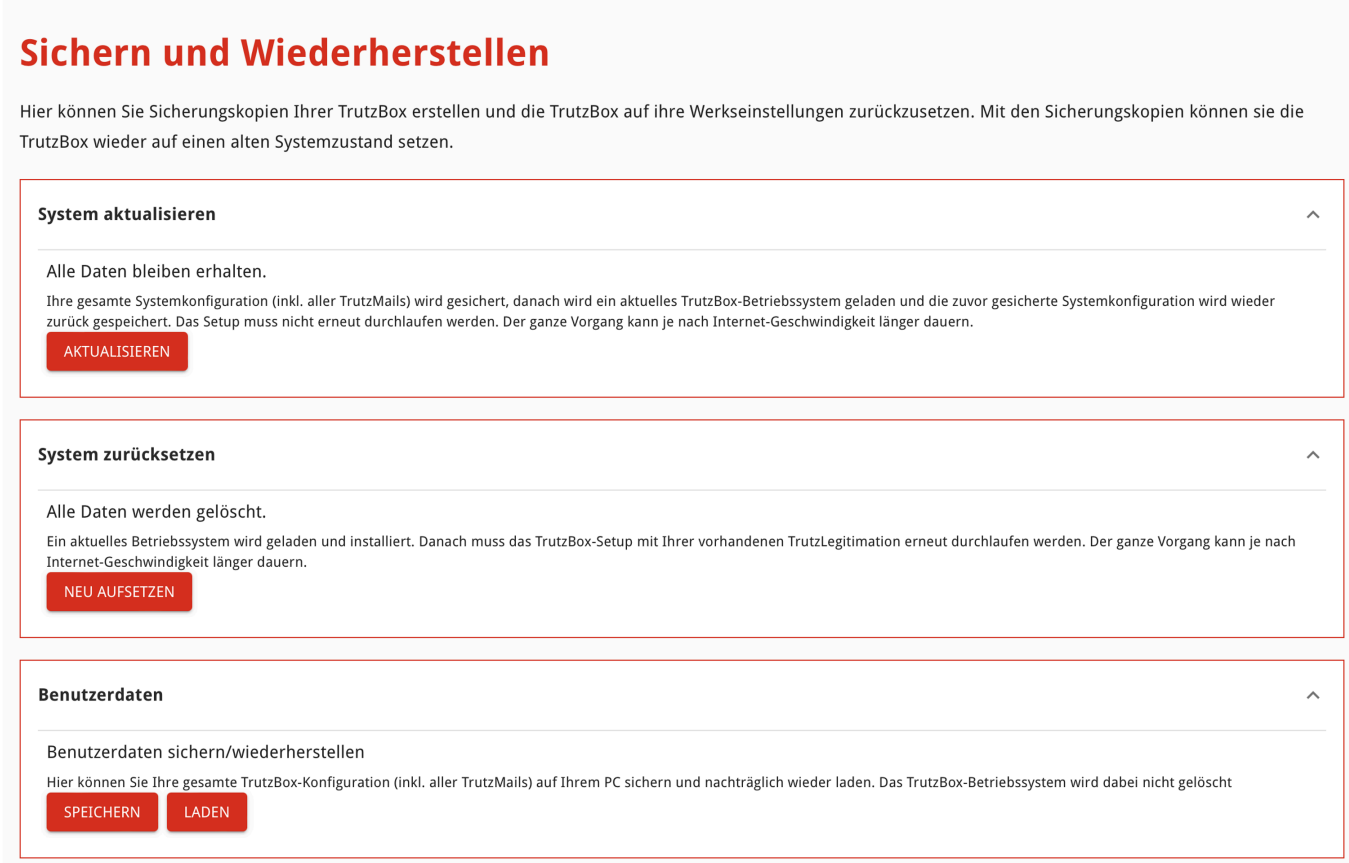
252 http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

253 http://linux.voyage.hk

TrutzBox zurücksetzen

Um bei Betriebsstörungen, die nicht mehr behebbar sind, die TrutzBox dennoch wieder in einen betriebsbereiten Zustand zu versetzen, hat der Administrator unter dem Menüpunkt „Systemeinstellungen“ -> „Sichern und Wiederherstellen“ die Möglichkeit, die TrutzBox in einen definierten Zustand zu versetzen. Hier ist es auch möglich, alle Einstellungen der TrutzBox zu speichern (Sicherung aller Einstellungen) und eine vorherige Sicherung aufzuspielen.

Dazu gib es drei Möglichkeiten.



(© 2024 Comidio GmbH)

System aktualisieren - Alle Daten bleiben erhalten.

Die gesamte Systemkonfiguration (inkl. aller Schlüssel und TrutzMails) werden gesichert, danach wird ein aktuelles TrutzBox-Betriebssystem von Comidio geladen (falls ein neueres Betriebssystem dort vorliegt) und die zuvor gesicherte Systemkonfiguration wird wieder zurück gespeichert. Das Setup muss nicht erneut durchlaufen werden. Der ganze Vorgang kann je nach Internet-Geschwindigkeit länger dauern.

System zurücksetzen - Alle Daten werden gelöscht.

Alle Daten auf der TrutzBox werden gelöscht. Ein aktuelles Betriebssystem wird geladen und installiert. Danach muss das TrutzBox-Setup mit Ihrer vorhandenen TrutzLegitimation erneut durchlaufen werden. Der ganze Vorgang kann je nach Internet-Geschwindigkeit länger dauern.

Die TrutzBox sollte vor einem Besitzerwechsel mit diesem Menüpunkt auf die Werkseinstellung zurück gesetzt werden.

Bitte beachten Sie, dass dabei alle Einstellungen und Daten auf der TrutzBox gelöscht werden. Also auch evtl. noch gespeicherte E-Mails werden dabei gelöscht. Danach wird eine komplette Sicherheitskopie der TrutzBox Software bei Auslieferungsstand, über die aktive Partition kopiert. Das kann längere Zeit dauern.
Dann kann die TrutzBox erneut mit der ursprünglich ausgelieferten TrutzLegitimation in Betrieb genommen werden. Da dabei auch neue Zertifikate auf der TrutzBox generiert werden, ist es notwendig, alle zuvor auf den Client-Geräten bzw. Browsern importierten Zertifikate der TrutzBox zu löschen, und neu zu importieren.

Benutzerdaten sichern/wiederherstellen
Hier können Sie Ihre gesamte TrutzBox-Konfiguration (inkl. aller TrutzMails) auf Ihrem PC sichern und nachträglich wieder laden. Das TrutzBox-Betriebssystem wird dabei nicht gelöscht und auch nicht erneuert.

TrutzMail Adressen bleiben reserviert nach Zurücksetzen der TrutzBox

Beim Reset auf Werkseinstellungen, werden auch alle Mail-Accounts auf der TrutzBox gelöscht. Comidios zentrale Verwaltung der E-Mail Adressen stellt allerdings sicher, dass die zuvor angelegten E-Mail Adressen nur mit der gleichen TrutzLegitimation "reaktiviert" werden dürfen, mit der sie ursprünglich eingerichtet wurden. Diese E-Mail-Adressen sind somit für den TrutzBox Besitzer (genauer gesagt für die TrutzLegitimation) reserviert. Damit wird sichergestellt, dass niemand eine E-Mail Adresse "kapert" und sich dann als jemand anderes ausgeben kann.
Diese "reservierten" E-Mail Adressen werden auf der TrutzBox unter "Benutzer verwalten" farblich gekennzeichnet. Durch den Knopf "reaktivieren" ist es möglich, diese E-Mail Adresse dann wieder auf der TrutzBox anlegen.

TrutzBox Hardware

Schon bei der Erstellung der TrutzBox Software-Architektur war klar, dass ein Gerät, das im Grunde genommen fast die gleiche Funktionalität wie professionelle Firewalls zur Verfügung stellen soll, auch relativ hohe Anforderungen an die Hardware stellt. Vor allem TrutzBase und viele gleichzeitige TrutzMail und TrutzBrowse Nutzer benötigen hohe CPU-Leistung und viel Hauptspeicher; zumal speziell beim

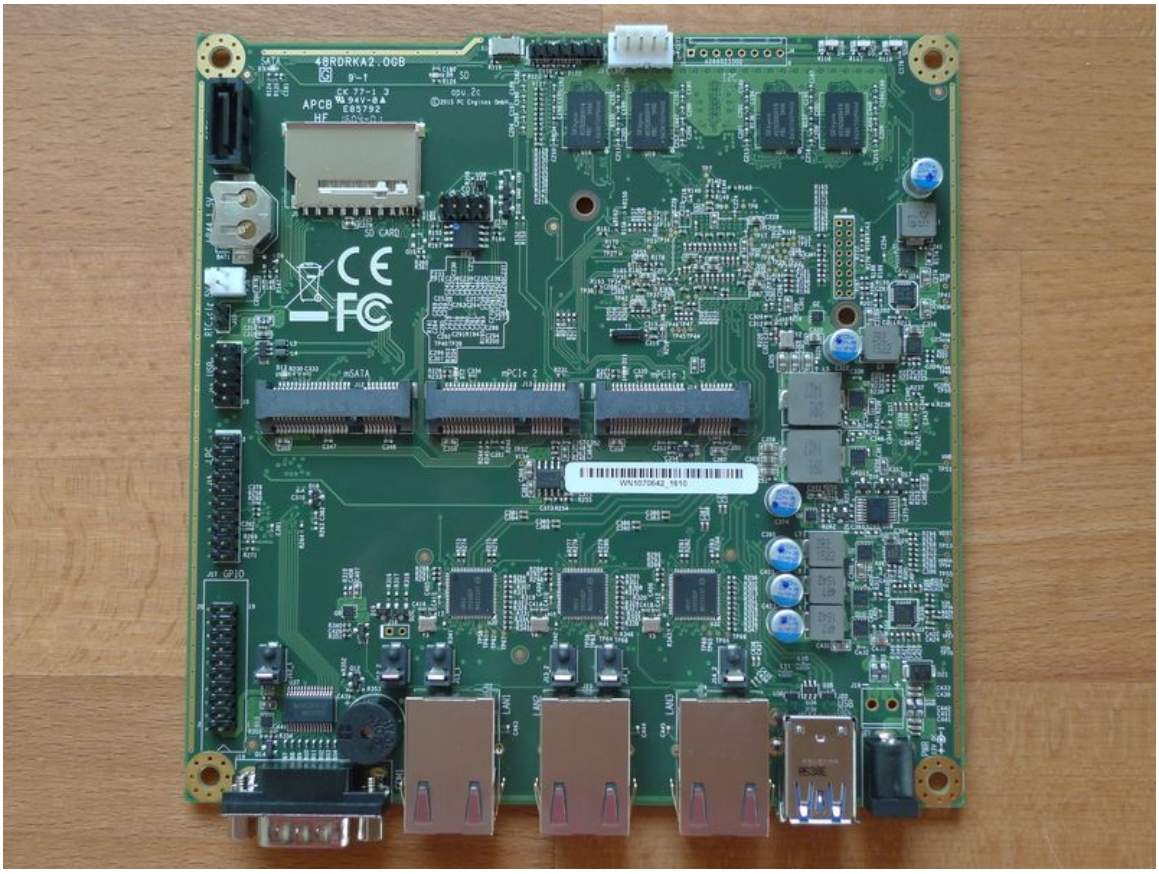
Surfen im Internet eine spürbare Verzögerung nicht akzeptierbar wäre. Bei einer E-Mail stört es in der Regel wenig, wenn diese 2 Minuten später ankommt. Wenn aber gerade viele E-Mails gesendet werden, sollte das Surfen im Internet trotzdem immer noch flüssig sein.
Die benötigte Hardware-Leistung für Real-Time Kommunikation hält sich in Grenzen. Dort wird i.d.R. zuvor der Zugang zum Internet zuerst zum Engpass, bevor die Leistungsgrenze der TrutzBox erreicht wird.
Folgende Hardware-Anforderungen waren für Comidio entscheidend:

- für den Dauerbetrieb ausgelegter Server,
- keine mechanischen Bauteile (keine drehende Festplatte sondern eine schnelle SSD),
- geringer Stromverbrauch,
- neben WLAN auch noch mindesten 2 LAN-Anschlüsse mit schnellen 1Gbit/s,
- geringer Kühl- und Platzbedarf, mechanisch stabil, sodass weitere Geräte darauf gestapelt werden können und
- eine Home-Version, die für Privatpersonen bezahlbar ist.

Aus diesen Gründen hat sich Comidio, als Hardware Basis für die TrutzBox, für Hardware der Firma PC-Engines entschieden.

- Bis 8/2016 wurde die TrutzBox auf Basis des APU.1 System-Boards in der 2GB Version, ausgeliefert.
- Ab 9/2016 kommt das APU2 System-Board des gleichen Herstellers zum Einsatz. Des weiteren wird mit dieser Version als Speichermedium eine SSD, anstatt der zuvor eingesetzten SD-Karte verwendet.
- Ab 2020 wird die TrutzBox-Business mit 4GB Hauptspeicher und größerer SSD alternativ angeboten.

Die Hauptplatine (Board) ermöglicht vier verschiedene Speichermedien: SD-Karte, USB-Stick, SATA HD/SSD und mSATA-SSD. Von allen vier Medien kann das System hochgefahren (gebootet) werden.



Das Board wird mit LAN-Kabel und Netzteil ausgeliefert. Optional kann ein WLAN-Adapter dazu oder nachträglich bestellt werden. Die TrutzBox erkennt, welches WLAN-Modul angeschlossen ist und, falls es ein von Comidio unterstütztes WLAN-Modul ist, lädt die entsprechende WLAN-Konfiguration automatisch.

Aufspielen von Updates oder eines kompletten TrutzBox Images (Betriebssystem)

Die TrutzBox kümmert sich automatisch um anstehende Updates, indem sie jede Nacht nachschaut, ob ein Update für sie bereit steht. Falls ja, wird dieses automatisch heruntergeladen und eingespielt. Dazu ist keine Benutzer-Interaktion notwendig.
Es kann jedoch vorkommen, dass es notwendig wird, ein komplett neues Image auf die TrutzBox aufzuspielen. Dazu dient zwar der Menüpunkt „Sichern und Wiederherstellen“, wenn jedoch das komplette Speichermedium defekt ist, kann man ein neues TrutzBox-Image per USB-Schnittstelle aufspielen. Das kann der Nutzer selbst vornehmen. Dazu benötigt der Nutzer einen mindestens 32GB großen USB-Speicherstick. Im TrutzBox Handbuch ist detailliert beschrieben, wie man mit Hilfe des USB-Sticks ein neues TrutzBox-Image aufspielt.

Austausch der Hardware

Im Falle einer defekten Hardware, kann diese recht einfach ausgetauscht werden. Da alle Authentisierungsschlüssel nur in Form von Software auf dem Boot-Medium gespeichert sind, ist es möglich, das Boot-Medium in eine andere TrutzBox Hardware zu stecken und diese unverändert in Betrieb zu nehmen. Da die Authentizität eines E-Mail-Nutzers an die TrutzLegitimierung gebunden ist, kann auch das interne Speichermedium (SSD) bei defekt ausgetauscht werden und der Nutzer kann ohne seine Anonymität gegenüber Comidio aufgeben zu müssen, seine alte Authentizität gegenüber seinen E-Mail Partnern wieder herstellen.

Ausblick

Seit Q2 2016 hat die TrutzBox Marktreife erlangt und ist im Comidio Online-Shop erhältlich. Ihre derzeitige Funktionalität ist in einem Zustand, der dem Nutzer ein großes Maß an Sicherheit und Anonymität beim Surfen und Mailen bringt. Allerdings stehen noch einige zu implementierende Funktionen auf dem langfristigen Comidio Entwicklungsplan. Nach dem aktuellen Stand sind dies:

- Weitere Verbesserungen bzgl. TrutzBrowse. Der TrutzBrowse Proxy verfälscht z.Z. zwar HTTP Header und berücksichtige Blacklists, um schädliche oder Tracking-Webseiten zu filtern; allerdings sind findige Programmierer in der Lage, mit eingebetteten Java-Script Code, Nutzerdaten zu ermitteln und Schäden auf des Nutzers Rechner zu verursachen. In einer zukünftigen TrutzBrowse Version könnte auch Java-Script-Code nach Schädlingen und Daten-Trackern abgescannt werden. Des Weiteren ist es in der aktuellen Version der TrutzBox einem Web-Server möglich, persönliche Daten als Parameter (http-post payload Daten) an den Server zu übermitteln. Auch das sollte in Zukunft von der TrutzBox besser unterbunden werden können.

- Weitere Proxies (z.B. Mediatomb oder Twonkymedia) für andere Web-Protokolle wie Medien-Server Proxys für YouTube, Flicker oder auch Flash (falls Flash überlebt).

- Die TrutzBox funktionell so zu erweitern, dass sie das interne Netzwerk nach Geräten durchsucht, die eine potentielle Gefährdung darstellen. Vor allem IoT-Geräte sind mittlerweile bei Hackern sehr begehrt und werden mit unerwünschter Software infiziert. Mit diesen von Hackern kontrollierten Geräten, z.B. ein Drucker oder ein Fernseher, werden dann Angriffe im Internet gefahren. Die TrutzBox könnte auch auf anstehende Updates für solche Geräte hinweisen. Comidio hat mit mehreren deutschen Universitäten 2023 begonnen, ein Projekt zu starten, das diese Funktionalität abdecken wird. Dieses Projekt hat eine Laufzeit von drei Jahren.

- Comidio könnte zukünftig Teile der TrutzBox Funktionalität (z.B. nur TrutzMail) auf einer preisgünstigeren Hardware anbieten. Mit relativ geringem Aufwand ist es möglich, Teile der Funktionalität auf günstiger ARM-Hardware wie z.B. Raspberry-PI, Beaglebone, Banana-Pi, Cubieboard, Wandboard oder sogar Arduino zu portieren.

- Um auch Social-Media Funktionen auf Basis von Eigenhosting betreiben zu können, könnte zukünftig eine Portierung und Integration einer Open-Source Social-Media Software sinnvoll sein. Derzeit ist jedoch noch nicht abzusehen, welche Open-Source Social-Media Plattform sich im Markt durchsetzen könnte. Comidio beobachtet dazu derzeit Hubzilla, Friendica, Diaspora, Mastodon oder GNU Social.

- Trackingschutz erweitern, indem Anfragen an Netzwerke wie "Google Hosted Libraries" nicht erreicht werden, aber diese imitiert. Somit werden Anfragen an CDNs von der TrutzBox dann selbst ausgeliefert (ähnlich wie das Plugin „decentraleyes“: https://addons.mozilla.org/de/firefox/addon/decentraleyes/ https://github.com/Synzvato/decentraleyes).

