TrutzBox® Kompendium

Version 4.91

Hermann Sauer
Comidio GmbH

Januar 2018

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

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 alle im Internet ausspioniert 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 oder geschätzte weitere 81.000 Firmen, die vom Erfassen und Handeln von Daten leben.
- Geheimdienste und andere staatliche Einrichtungen, die illegaler Weise 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.

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 Anhalts los überwacht werden. Viele, die sich dieses Problems bewusst sind, meiden kostenlose Internet-Dienste wie Facebook, Google, 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.

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

Die Auswertung hat gezeigt, dass es sehr viele technische Möglichkeiten gibt, sich im Internet zu schützen.

Allerdings sind die verfügbaren Werkzeuge einzeln nicht ausreichend:

- 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 Tools bekannt.

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. 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.

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

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.

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 Cryptoparty-Handbook[5].

Dieses vorliegende TrutzBox® Kompendium beschreibt ausführlich die aktuelle Bedrohungslage, vor welchen Angriffen die Comidio TrutzBox® schützt und wie sie im Detail funktioniert.

[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

Kommerzielle Daten-Tracker und Daten-Händler

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

Der Satz ist zwei Jahre alt 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. Zum Zeitpunkt der Comidio Recherche hatte allein focus.de 16 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 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 "Man in the Middle Attack" zum Fernseher durchzuführen und den kompletten Empfangs- und Sende-Stream zu manipulieren[11].

---

[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

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

Diese Übersicht der Datenhändler-Marktführer im deutschen Datenhandel zeigt, welche Unternehmen sich zu welchen Zwecken positioniert haben (ohne Internetplattformen)[12]:

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,
- eventuelle Haustiere und
- eventuelle sportliche Tätigkeiten.

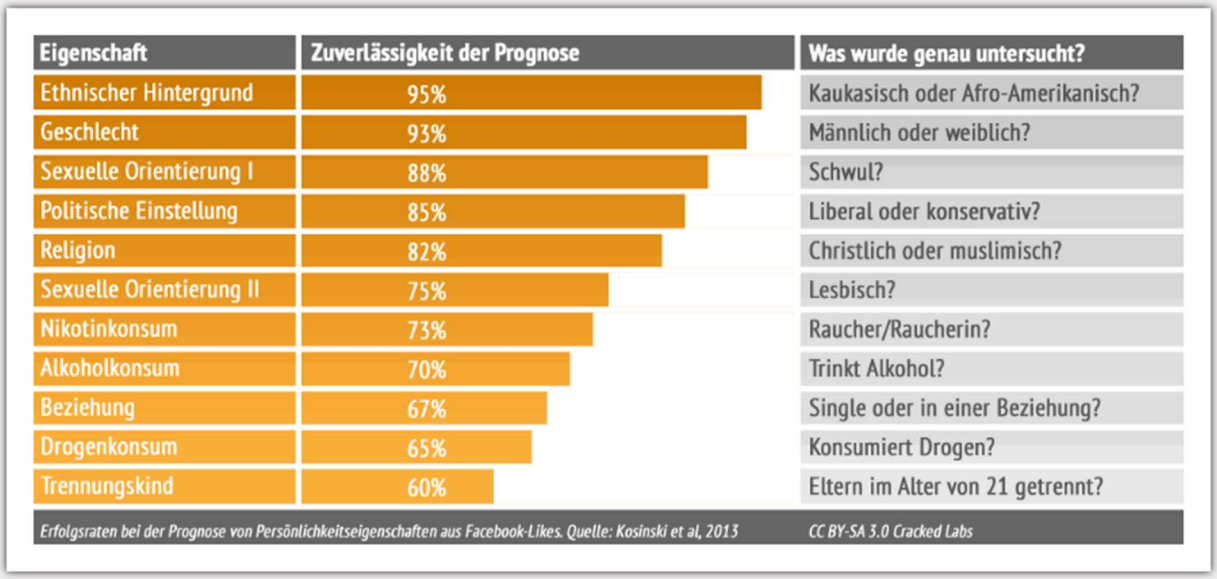
[12] https://safeaddress.de/blog/adress-und-datenhandel-ueberblick/

Facebook

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

- 274 neue Nutzer pro Minute
- 8,81 Milliarden Dollar Umsatz
- 16 Dollar pro Nutzer im Jahr
- Aktueller Firmenwert: 385 Milliarden Dollar.
- Durch WhatsApp und Instagram 1,6 Milliarden Nutzer

Viele Webseiten haben mittlerweile den Facebook-Like-Knopf auf ihren Seiten einprogrammiert. Dieser wird pro Minute von über 3 Millionen Internetnutzern gedrückt (das sind 50.000 Likes pro Sekunde!), um der Seite anzuzeigen, dass man sie mag[14]. Unabhängig davon, ob man überhaupt ein Konto bei Facebook hat, können unter andere folgende persönliche Eigenschaften allein auf Basis dieser Facebook-Likes berechnet werden[15]:



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

[13] http://www.apfelpage.de/news/facebook-verdient-16-dollar-pro-nutzer-im-jahr/

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

[15] http://crackedlabs.org/studie-kommerzielle-ueberwachung
http://www.pnas.org/content/suppl/2013/03/07/1218772110.DCSupplemental/pnas.201218772SI.pdf

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.

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[16]: Mehr Details zu den Daten, die Facebook sammelt sind unter dem Blog „What should you think about when using Facebook?“ aufgeführt[17].

- ✓ 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[18],[19]

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

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

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

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

Facebook bietet allerdings online einige Funktionen an, mit denen man seine bei Facebook gespeicherten Daten einsehen kann[20]. Diese Daten beinhalten auch, welche Firmen seine Daten von Facebook durch einen Werbeabruf erhalten haben.

Einen sehr interessanten Einblick, in die internars des Unternehmens Facebook haben die Studien von „Facebook Algorithmic Factory“ ergeben[21]

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“22. 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 über 44 Millionen Deutsche".“[23].

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

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

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

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

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)

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/

Aber 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[24].
- „Personalentscheidungen auf Basis Big Data Auswertungen“ werden gerne von Personalabteilungen genutzt. Das Unternehmen Cornerstone hält dafür Ihre Daten bereit[25], und ConnectCubed[26] kann sogar die Leistungsfähigkeit der zukünftigen Mitarbeiter voraus-sagen[27]
- „Preisdiskriminierung“ ist heute schon Realität[28]. 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[29].

[24] http://www.zestfinance.com

[25] http://www.cornerstoneondemand.com

[26] http://connectcubed.com/

[27] http://connectcubed.com

- „Krankheitsprognosen aus Konsumverhalten“ werden von Versicherungen getestet[30].

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 wird, 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[31]. 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”[32] 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.

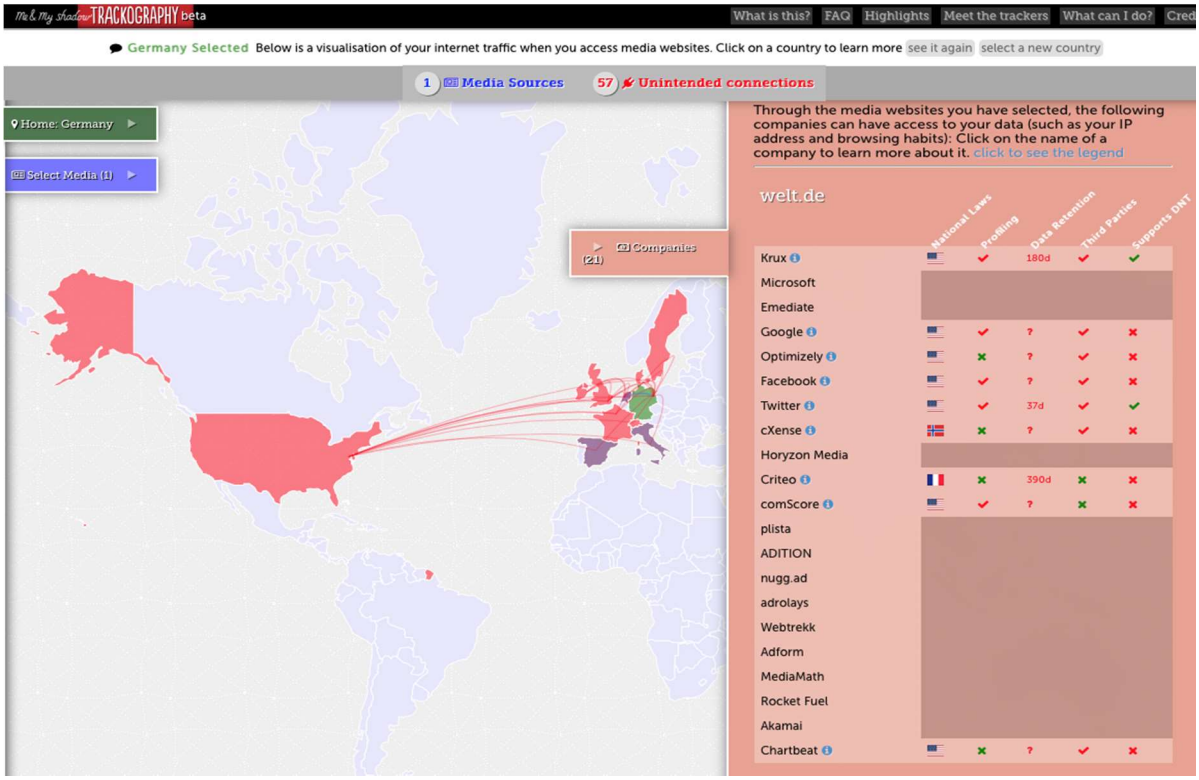
[28] http://www.zeit.de/wirtschaft/2014-10/absolute-preisdiskriminierung

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

[30] http://www.wsj.com/articles/SB10001424052748704648604575620750998072986

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

[32] 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.

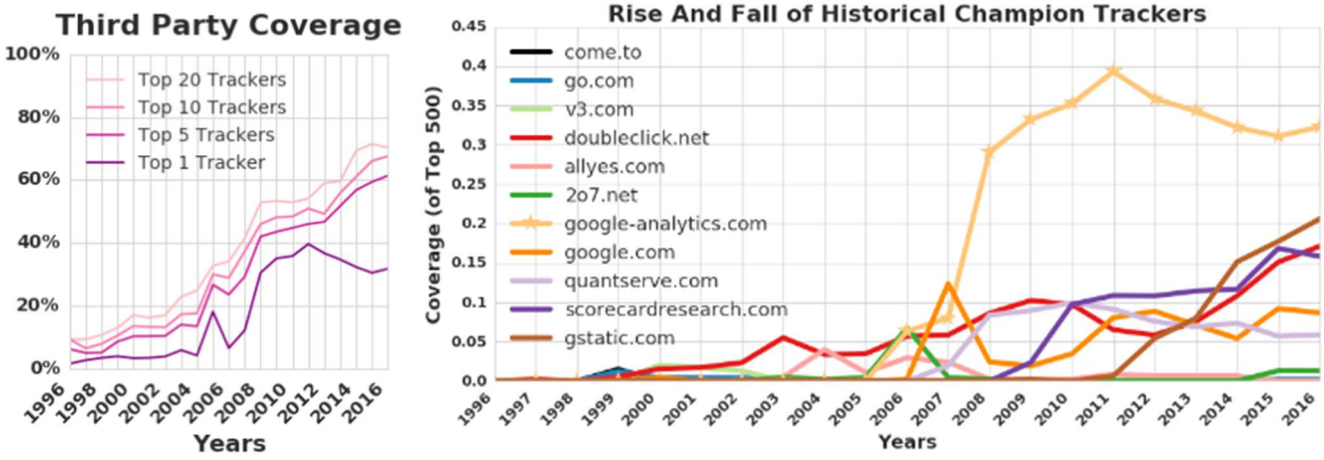
Des Weiteren sollte man auch nie vergessen, dass alle diese von Daten-Trackern gesammelten Daten auch gerne auch von Kriminellen und Geheimdiensten in diesen Ländern abgefischt werden.

Aber nicht nur beim Browsen im Internet sammeln kommerzielle Firmen Daten über uns. Gerade erst hat Microsoft die Datensammelwut von Windows 10 erläutert[33].

Wie sich das Tracking im Internet über die letzten 20 Jahre entwickelt hat, haben Forscher der University of Washington analysiert[34]:

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

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



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

Werbung im Internet

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 ersten Quartal 2016 hat alleine Facebook 5,2 Milliarden Dollar 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 Apps 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 3.874 Marketing Technology-Lösungen zeigt, wie komplex und unübersichtlich der Markt mittlerweile geworden ist:

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

Eine Studie ergab, dass es 81.000 Online Tracking Dienste gibt! Aber nur 123 dieser Dienste den Markt dominieren [35]. Alle diese Dienste haben sich erst über die letzten Jahre etabliert und werden unter anderem über Werbung bezahlt. Der „Chief Marketing Technologist Blog“[36][37] 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

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

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

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

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[38],[39]. Dieses Vorgehen wird Malvertising[40] 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[41]). 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[42] einkaufen. Ein weiterer Vorteil für Angreifer bietet Malvertising dadurch, dass der Angreifer keine eigene Infrastruktur für 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[43]. 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.

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

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

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

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

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

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

Echtzeit-Versteigerung von Werbung

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“[44] 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[45] wird das Werbemittel des jeweils Höchstbietenden ausgeliefert[46].

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.

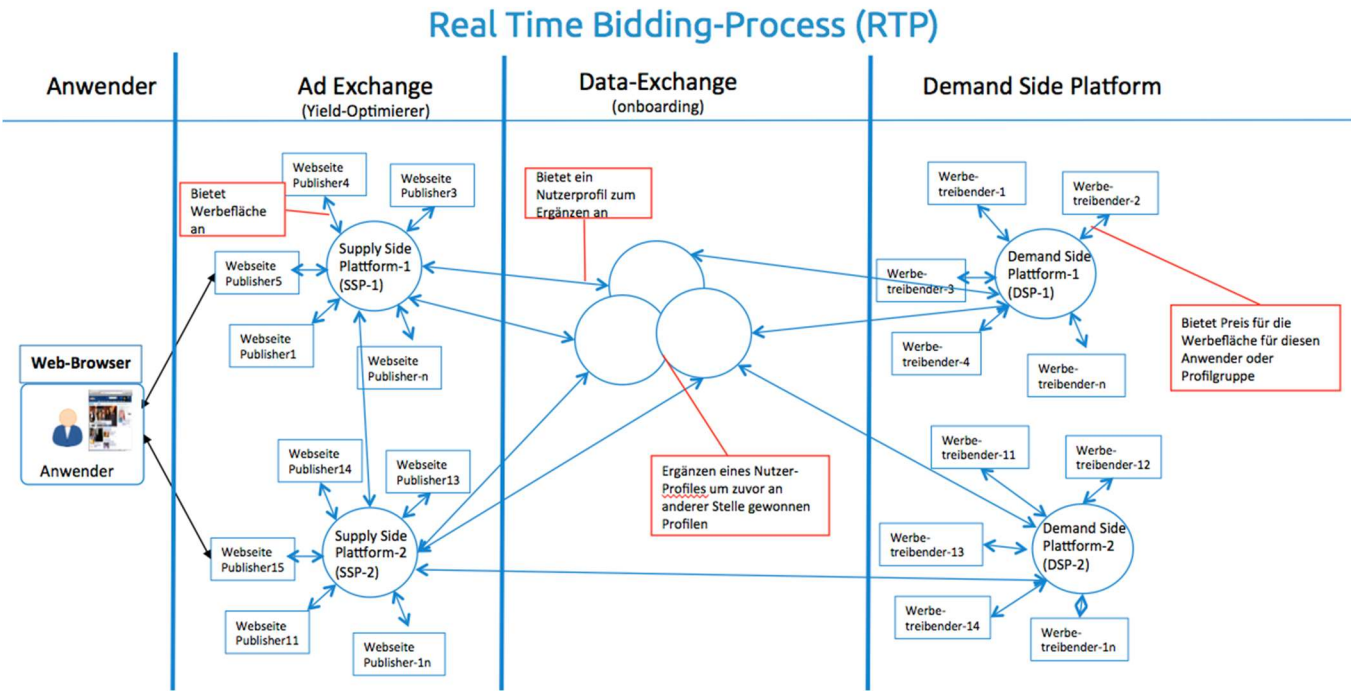
Die Werbefläche und das Profil des Besuchers wird zunächst einer „Sell Side Platform“ (SSP) höchstbietend zur Versteigerung angeboten. Sell Side Platform (SSP) oder auch Supply Side Plattform ist ein Begriff aus dem automatisierten Handel im Onlinemarketing. Es bezeichnet eine Technologie, die es einem Publisher erlaubt, sein Inventar für ihn möglichst gewinnbringend Ad-Exchanges und Werbetreibenden anzubieten[47].

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[48]. 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. Onboarding bezeichnet den Prozess, ein bestehendes Nutzerprofil um weitere Profile aus anderen

[44] https://de.wikipedia.org/wiki/Programmatic_Advertising
[45] https://de.wikipedia.org/wiki/Ad_Impression
[46] https://de.wikipedia.org/wiki/Real_Time_Bidding
[47] http://www.digitalwiki.de/ssp-sell-side-platform/
[48] http://www.digitalwiki.de/dsp-demand-side-platform/

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.

Eine recht gute Marktübersicht über DSP-, SSP-Anbieter, die auch in Deutschland vertreten sind und Publisher welche SSP nutzen, gibt „programmatic beef“[49]

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

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

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/

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[50].

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 wir in der Zusammenarbeit mit der Tracking-Industrie erst am Anfang stehen, 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

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

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.

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“[51].

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.[52]

Ein Artikel von Netzpolitik.org bringt es auf den Punkt[53]:

„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.”

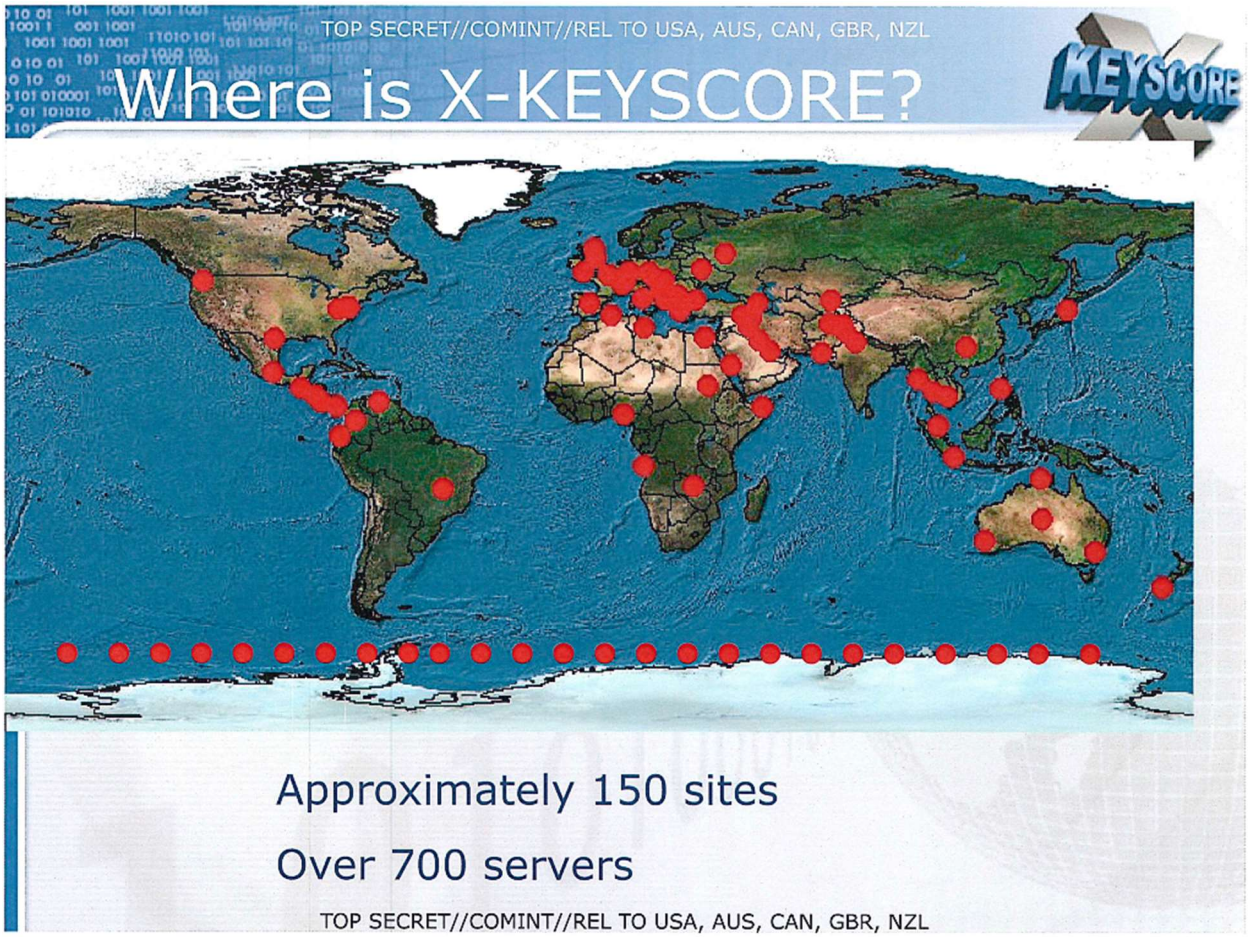
[51] https://blog.emvolution.me/2016/07/warum-werbeprofile-der-kuhhandel-des-21-jahrhunderts-sind/

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

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

Aus einem geheimen Gutachten der Bundesdatenschutzbeauftragten Andrea Voßhoff geht hervor, dass der deutsche Bundesnachrichtendienst (BND) im Verdacht steht, bei Abhöraktionen systematisch gegen Bestimmungen des Datenschutzes verstoßen zu haben[5455].

Geheimdienste zapfen das Internet an zentralen Internet-Daten-Austauschpunkten an 56 . Allein der amerikanische Geheimdienst NSA betreibt Datenaustauschpunkte, die weltweit an ca. 150 Standorten positioniert sind[57].



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

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

[56] http://www.golem.de/news/de-cix-wie-sich-der-internetknoten-frankfurt-abhoeren-laesst-1411-110344.html
http://www.golem.de/news/operation-eikonal-bnd-zapft-telekom-in-frankfurt-an-1412-110965.html
http://electrospaces.blogspot.de/2014/11/incenser-or-how-nsa-and-gchq-are.html

[57] 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[58][59] 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[60].

„The Guardian“ berichtete, dass 10/2014 sagenhafte 1,2 Millionen Menschen auf dieser NSA Beobachtungsliste standen[61]. 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[62],[63].

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[64].

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[65].

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

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

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

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

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

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

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

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

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

herauszufiltern, um bei Bedarf eine konkrete Person im Detail zu beobachten[66]. 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)[67]. Kurz danach stellte auch der VPN Anbieter Cryptoseal aus den gleichen Gründen sein Angebot ein[68]. Amerikanische IT-Dienstleister, die vom amerikanischen Geheimdienst zur „Zusammenarbeit“ gezwungen werden, sind zusätzlich verpflichtet, diesen Sachverhalt geheim zu halten.

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[69].

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 wären 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 Omars[70] Dieser wurde von der CIA, mit Unterstützung der italienischen Polizei, entführt und gefoltert. Da es eines 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:

---

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

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

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

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

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

- **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)[71]. Wem genau hatte Facebook diesen Hinweis angezeigt?[72]
- 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“[73].

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“[74].

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

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

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

[73] http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/
https://www.youtube.com/watch?v=UdQiz0Vavmc

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

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[75]. funktioniert von einem anderen Land aus oder sogar von jedem beliebigen Punkt auf der Erde. Das besonders Perfide hieran ist, dass es damit 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."[76]

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[77].

Es gibt einen sehr empfehlenswerten interaktiven Film mit dem Namen „Netwars / out of CTRL", der im Detail über diesen digitalen Krieg aufklärt[78].

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[79].

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

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

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

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

[78] http://netwars-project.com/de/webdoc

[79] http://www.heise.de/extras/timeline

dieser Informationen können Internet-Kriminelle z.B. auf Kosten anderer einkaufen oder Geld von Bankkonten abheben.

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[80]. 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[81].

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 nur für große Firmen entwickelt worden und somit für Privatanwender nicht nur zu teuer, sondern für Laien auch nicht zu bedienen. 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 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[82].[83]

[80] https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html
[81] http://www.bitkom.org/de/presse/8477_82074.aspx
[82] http://www.grundrechteschutz.de/gg/recht-auf-informationelle-selbstbestimmung-272
[83]https://de.wikipedia.org/wiki/Grundrecht_auf_Gew%C3%A4hrleistung_der_Vertraulichkeit_und_Integrit%C3%A4t_informationstechnischer_Systeme

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[84]. 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[85].

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 hilflosen Internet-Laien, die sich zwar oft des Problems bewusst sind, aber keine Möglichkeit sehen, diese Angriffe auf Ihre Persönlichkeit abzuwehren.

Diesen Internet-Laien, also private Anwender und kleine 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)

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

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

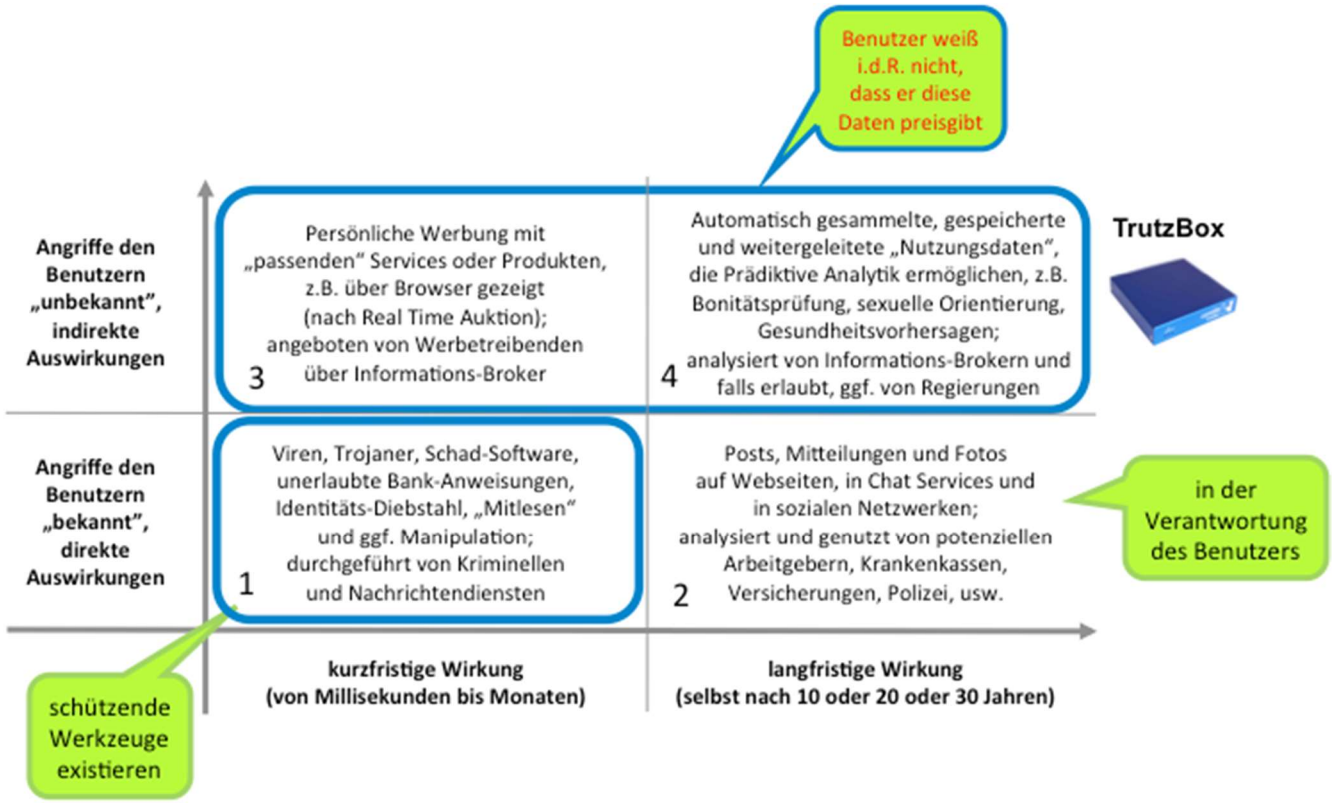
Die Angreifer in diese drei Gruppen einzuteilen ist sinnvoll, da sie einerseits unterschiedliche Bedrohungen darstellen und andererseits mit jeweils eigenen technischen Mitteln und juristischen Möglichkeiten arbeiten.

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, Google+ und anderen sozialen Netzwerken.

Er kann aber auch auf seiner eigenen Homepage persönliche Daten veröffentlicht haben. Natürlich freuen sich alle drei Gruppen auch über diese Daten. Aber, 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 er persönliche Daten in sozialen Netzwerken löscht, entzieht er sie 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:



(© 2015 Comidio GmbH)

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, Google+, 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[86], 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!

[86] 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“[87],[88]:

- Google Plus
- Benutzerdefinierte Suche
- Enterprise Search
- Google Earth Enterprise
- Website-Übersetzer
- AdWords
- DoubleClick
- AdMob
- Google Analytics
- Google Fonts
- Google hosted libraries
- Google Public DNS

[87] http://www.heise.de/ct/14/11/links/134.shtml
[88] https://developers.google.com/apis-explorer/#p/

- Blogger.com
- Blogspot.com
- 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[89]. Für die vielen anderen Mechanismen, mit denen Google den Nutzer ausspioniert, gibt es das nicht.

Tim Libert (https://timlibert.me) hat eine Studie[90] veröffentlicht, in der er nicht nur eine Million Webseiten auf Datentracker hin analysiert hat, sondern auch, in wieweit diese von der NSA genutzt werden:

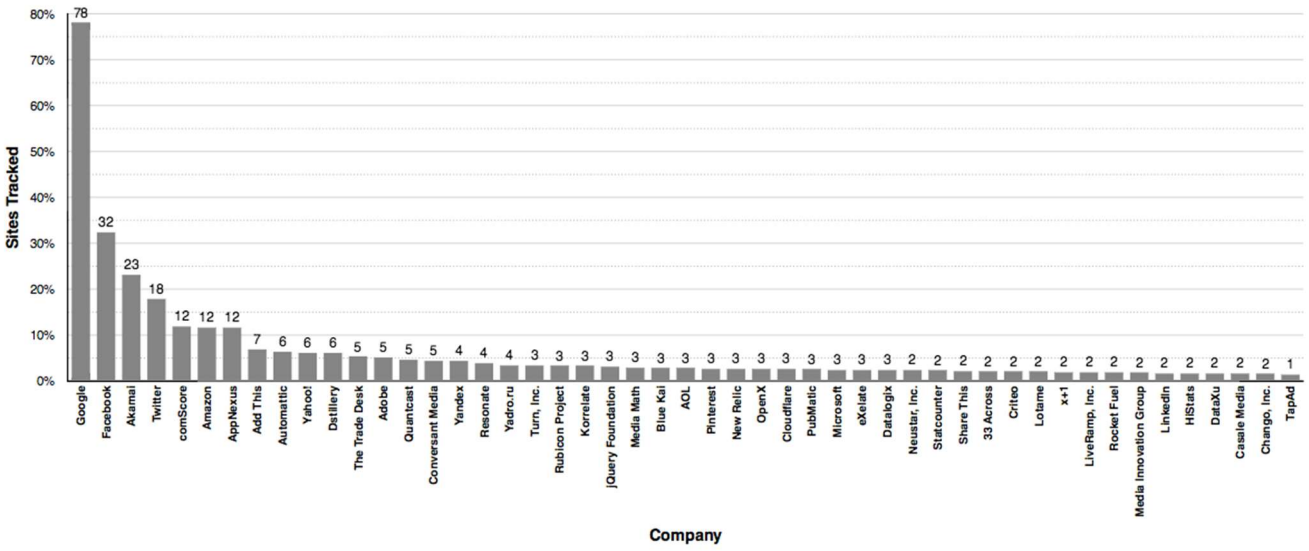


Figure 1: *Percentage of Sites Tracked by Top 50 Corporations*

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.

[89] https://tools.google.com/dlpage/gaoptout?hl=de
[90] https://timlibert.me/pdf/Libert-2015-Exposing_Hidden_Web_on_Million_Sites.pdf

Eine weitere Seite, dasfilter.com hat ebenfalls eine Statistik über die Web-Sites mit den meisten Trackern erstellt[91]:

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[92].

Hier ein Beispiel:

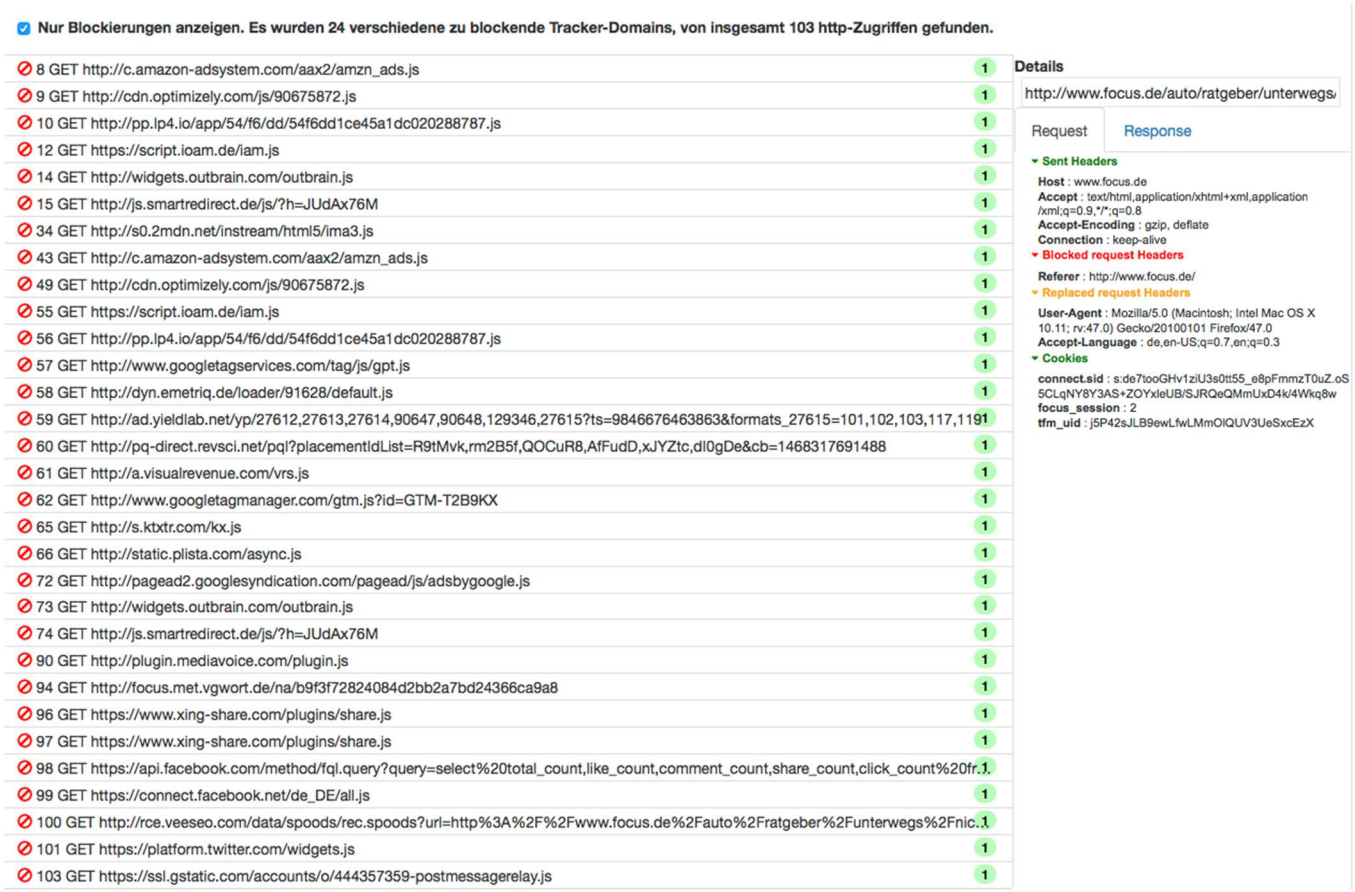
Wenn der Nutzer die Webseite der Zeitschrift Focus aufruft (focus.de), weiß Google bereits, dass jemand auf dem Rechner des betroffenen Nutzers gerade Focus liest (doubleclick und google-analytics). Wenn er dann auf focus.de einen konkreten Artikel anklickt, sieht er einen Facebook „Teilen“ Knopf oder LikeMe-Knopf. Abhängig davon, wie dieser Knopf auf der Webseite programmiert wurde, weiß jetzt auch Facebook, dass sein Rechner die

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

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

Seite von focus.de aufgerufen hat. Und das ohne, dass er diesen Knopf betätigt, und ohne dass er überhaupt Mitglied bei Facebook sein muss.

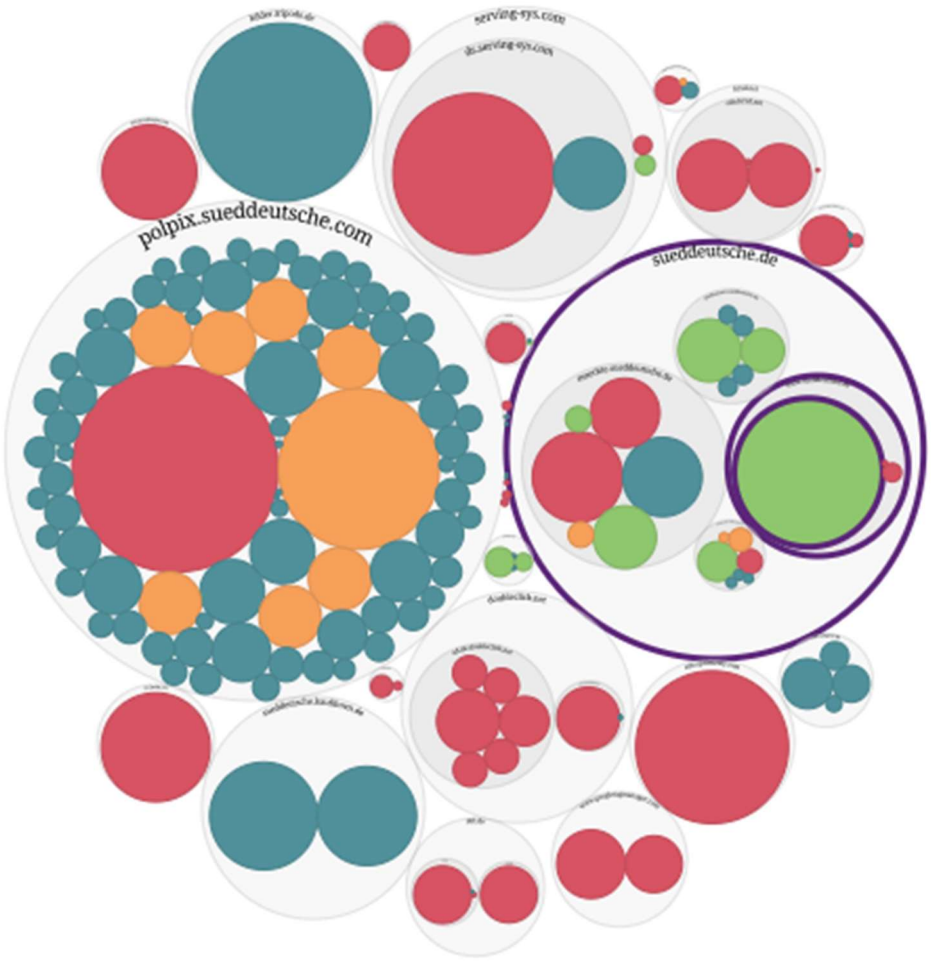
Das Blocking-Protokoll des Comidio TrutzBox® TrutzBrowse Services zeigt die Details der Tracker, hier am Beispiel eines Artikels von focus.de (abgerufen am 11.07.2016):



(© 2016 Comidio GmbH)

Jetzt wissen neben Google und Facebook auch die Firmen Amazon 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 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

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[93].

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

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 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 automatisch 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 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/
- http://noc.to/
- https://fingerprint.pet-portal.eu

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

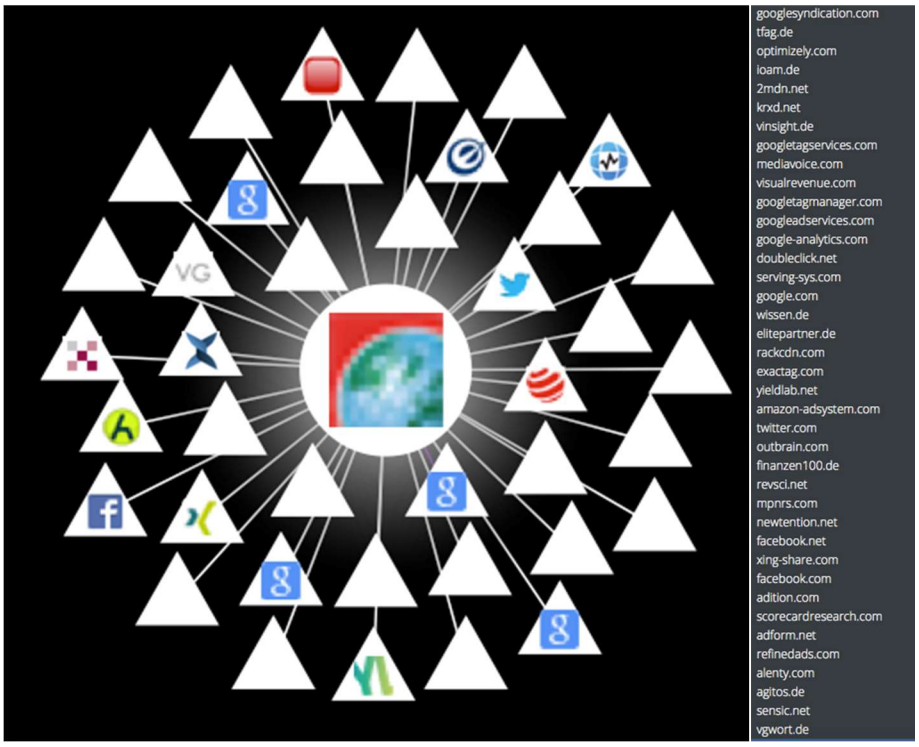
Mit Hilfe der Webseite https://privacyscore.org (Compare Websites with PrivacyScore) kann man Webseite prüfen, wie sicher diese sind. Die Entwickler dieser Seite haben auch eine Funktion eingebaut, über die man eine ganze Liste von Links prüfen lassen kann. Einige interessante Gruppen von Web-Seiten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

https://privacyscore.org/list/47/?categories=privacy,ssl,security,mx

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)[94] und „lightbeam“[95] sehr anschaulich

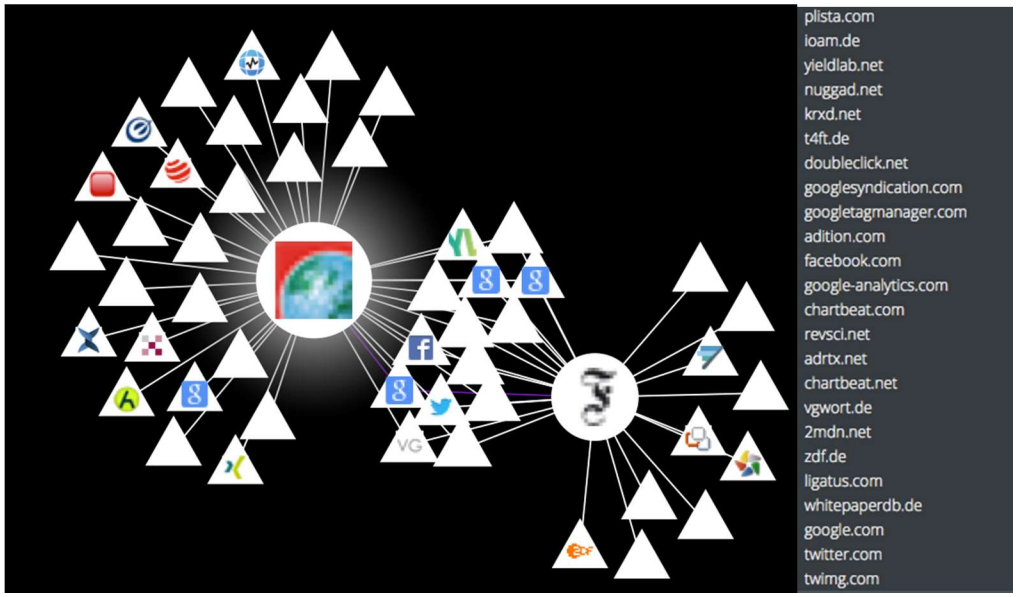
Bei Aufruf eines Artikels von der Seite „focus.de“ werden weitere 39 Daten-Tracker mitgeladen (hier mit „lightbeam“ visualisiert:



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

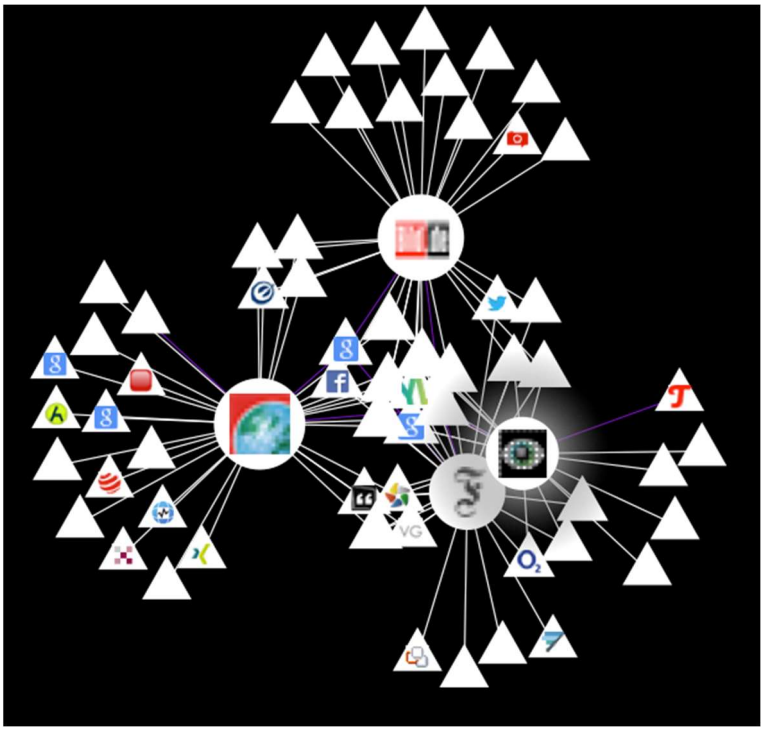
[94] https://disconnect.me

[95] https://addons.mozilla.org/en-us/firefox/addon/lightbeam/



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

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[9697]:

- 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[98]
- WebRTC Local IP Discovery
-

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

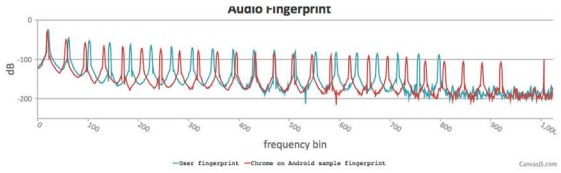
[97] http://www.heise.de/security/meldung/Das-Zombie-Cookie-1094770.html

[98] AudioContext Fingerprint

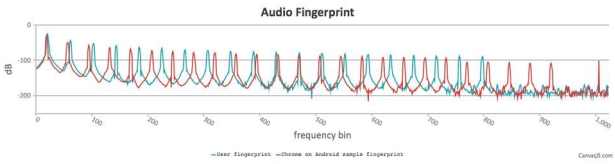
Durch die Kombination mehrerer dieser Techniken entstehen Cookies, die nahezu unlöschbar sind und „Evercookies“ genannt werden[99].

Seit einiger Zeit werden verstärkt auch Browser-Profile mit Hilfe des Canvas-Fingerprinting erkannt [100]. 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[101].

Ghostery hat eine Auflistung der 50 Sachverhalte verfügbar gemacht[102], die ein Server erfährt, wenn der Nutzer eine Webseite besucht“, und ein Tool (BrowserSpy) [103] gebaut, mit dessen Hilfe jede einzelne Information abgefragt werden kann.

Hier werden die Techniken der Daten-Sammler sehr gut beschrieben: https://www.anonym-surfen.de/help/wwwprivacy_technik.html. http://newsreadsus.okfn.de hat diese „Trittbrettfahrer“ sehr schön animiert.

[99] http://samy.pl/evercookie/
[100] http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block
[101] https://www.tracks-summit.de/news/2016-03-08-mobile-tui-group-testet-cookieloses-tracking/
[102] https://purplebox.ghostery.com/post/1016024218
[103] http://browserspy.dk

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.

Wie wir gesehen haben, ist jeder mit 5-6 Daten eindeutig wieder erkennbar. 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[104], 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[105]. 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 [106].

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

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

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

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“ [107]. 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[108].

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" [109] 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.

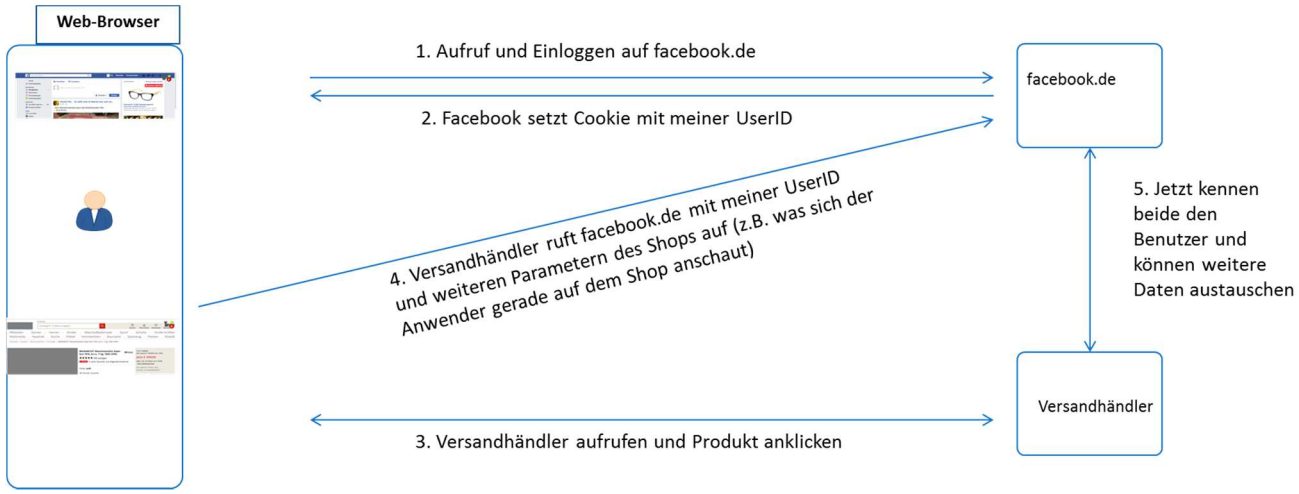
Irgendwann einmal ruft der Anwender anonym die Seite eines Internet-Shops (Versandhändler) auf und schaut sich einige Produkte an. Ein Tracker oder die Seite des Versandhändlers selbst ruft nun Tracker-A (facebook.de) auf und übergibt dabei sowohl den facebook-cookie mit meiner eindeutigen Facebook-Id 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

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

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

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

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[110].

Die TrutzBox verhindert schon in ihrer Standard-Einstellung diese Art der De-Anonymisierung.

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 sowohl für facebook als auch für diesen „Online-Versandhändler“ der Security-Slider auf L9 gestellt werden.

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

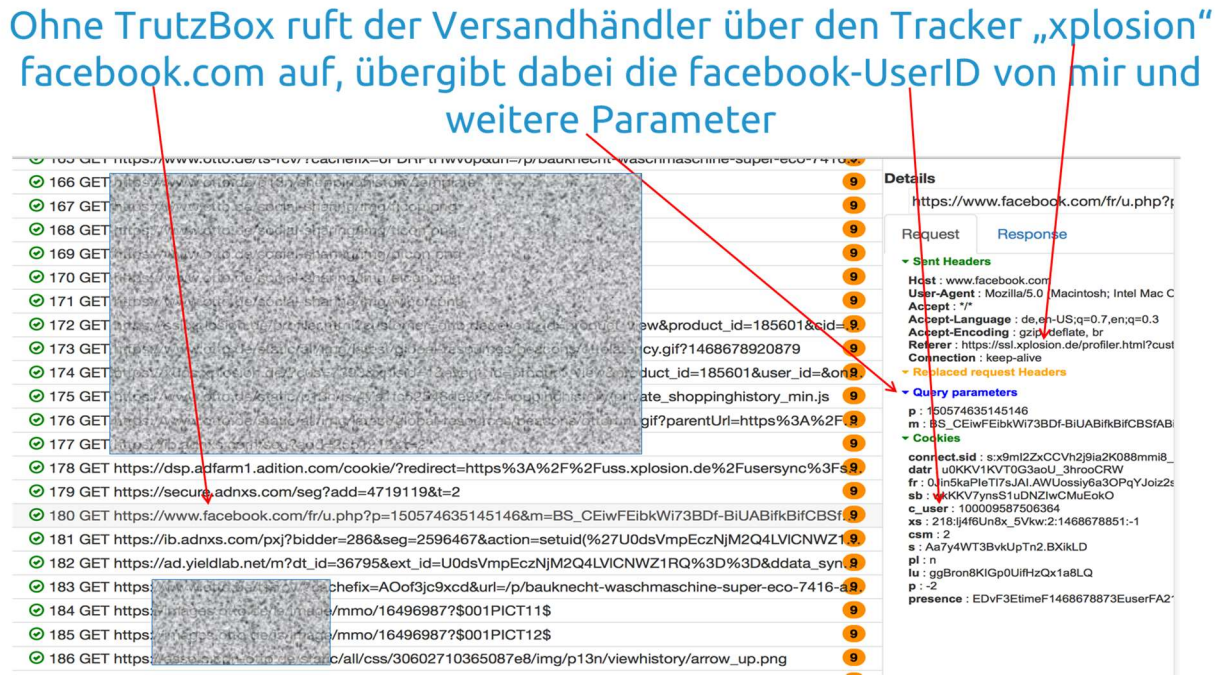
Zuerst in Facebook einloggen. In Facebook kann man sehen, dass ein Cookie geschrieben wird:

(©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 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**[111]**.** 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*

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

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 TOMORROW FOCUS Media – mit denen von InteractiveMedia zu bündeln und diese für die Vermarktung zugänglich zu machen*"[112]. 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 sichergestellt. Durch das Unternehmen „***InteractiveMedia"*** werden auch sowohl SmartTV als auch IPTV (Internet-Fernsehen) mit eingebunden.

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

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“ 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:

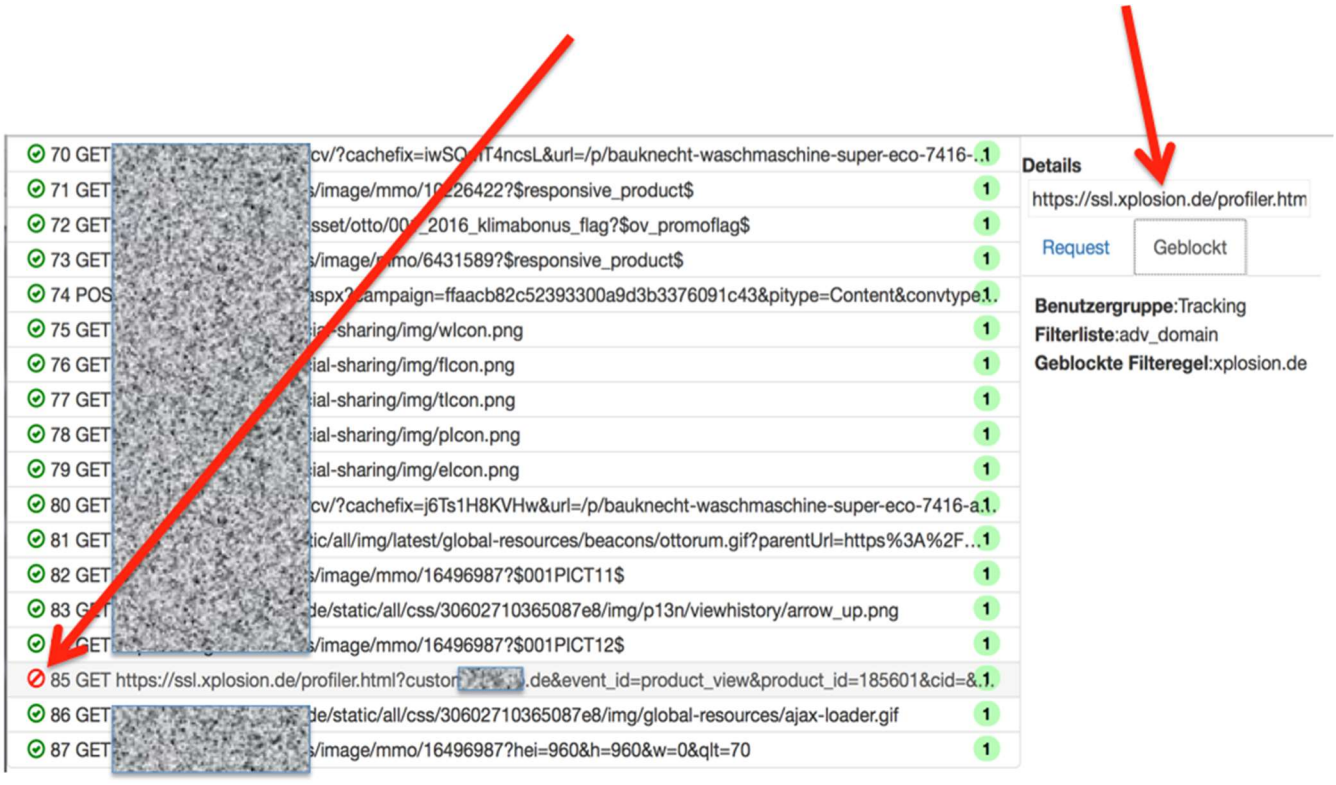
„pid_signature=Wd5lwqWbBiwkWC_FHSjlWScDWq5jWqBFWQwFwD5jwCWbwSU8Wsf0E_rr“

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:



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 das 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. Diese kann derzeit jedoch nur die TrutzBox blockieren.

Tracking trotz abgeschalteten JavaScript und Cookies

Dass es auch möglich ist, bei abgeschalteten JavaScript und Cookies trotzdem einen User wiederzuerkennen, zeigt Mechanismus, der das http-header Feld „Etag“ nutzt.

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

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.

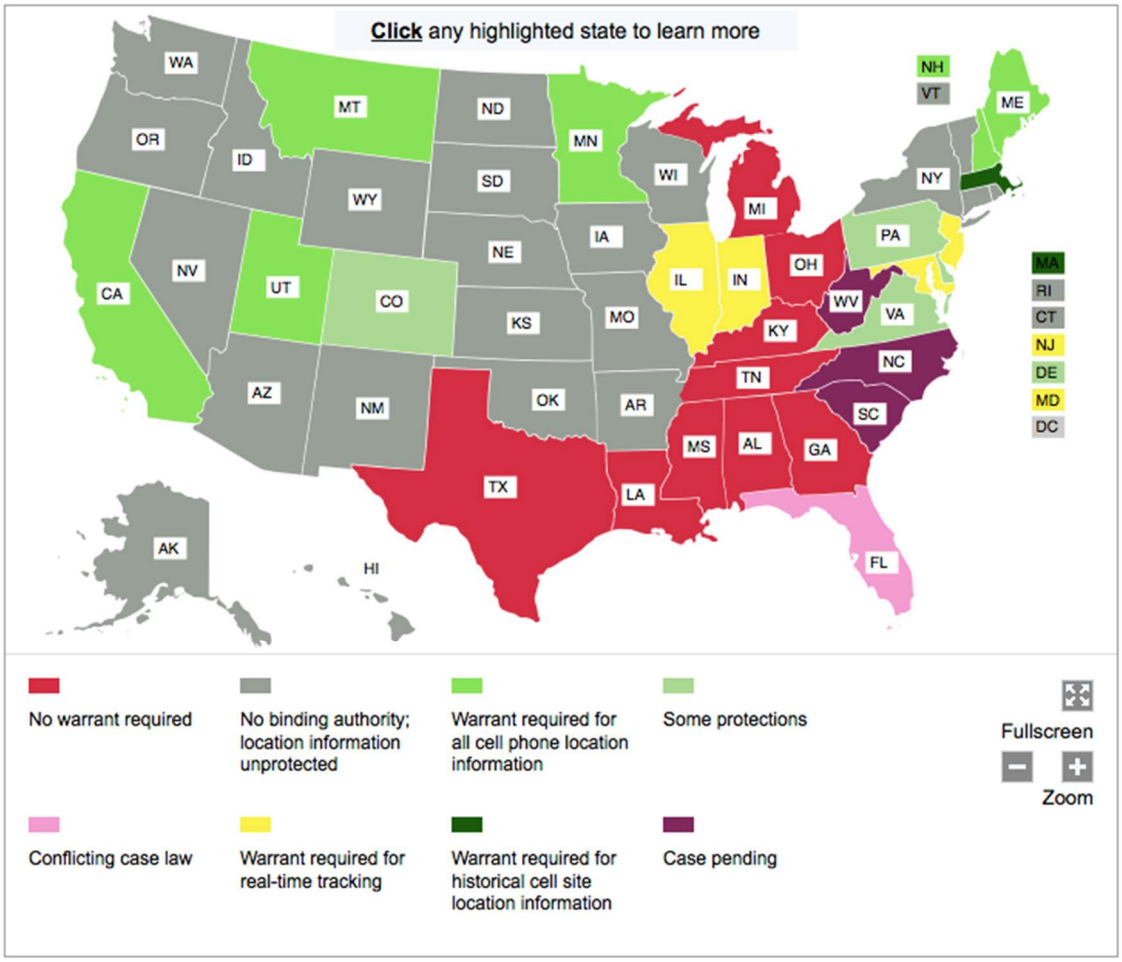
Dieses Beispiel zeigt, wie wichtig es für die Anonymisierung ist, dass der http-header kontrolliert wird. Und genau das macht die TrutzBox.

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 mit proprietären Protokollen 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. 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[113].

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



Screenshot vom 20.6.2016 aus https://www.aclu.org/map/cell-phone-location-tracking-laws-state

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 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.[114]

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 Kontextinformationen 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. [115].

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.

„The Wall Street Journal“ stellt eine gute Übersicht zur Verfügung die zeigt, welche der verbreitetsten Apps welche Daten sammelt[116].

Die Firma NSO Group entwickelt und verkauft Werkzeuge, mit denen sogar die neuesten Generationen von IPhones ausspioniert werden können[117].

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 „Klar“ auf den Markt gebracht, die „Schutz Ihrer Privatsphäre“ verspricht[118]:

„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.“

---

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

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

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

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

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

Allerdings hat diese App selbst einen Tracker eingebaut, der jeden aufgerufenen Link, direkt an die Tracking-Firma Adjust übermittelt:

11:05 1 https://app.adjust.com/sdk_click
11:05 1 https://app.adjust.com/sdk_click
11:05 1 https://app.adjust.com/sdk_click
11:05 1 https://app.adjust.com/sdk_click
11:05 1 https://app.adjust.com/sdk_click
11:05 1 https://app.adjust.com/sdk_click
11:04 1 https://app.adjust.com/sdk_click
11:04 1 https://app.adjust.com/session

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. „[119]

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

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, bei denen der Nutzer seine Daten speichert, 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[120],[121]), weltweit und in Echtzeit auf E-Mails, Chat und Browser-Transaktionen des Nutzers zugreifen[122].

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 Schlüsselwörtern Kommunikationsteilnehmer auf eine Verdächtigen-Liste setzen. Diese Suchmerkmale werden „Selektoren" genannt [123] [124]. 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[125].

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[126].

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.

---

[120] 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

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

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

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

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

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

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

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 von Firmen, die Überwachungslösungen liefern[127]. Wo in Deutschland Geheimdienste stationiert sind zeigt Eagle-Eye auf[128]. 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 [129]. 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[130]:

"*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.

---

[127] http://buggedplanet.info/index.php?title=DE
http://buggedplanet.info/index.php?title=Main_Page

[128] http://www.photocontest-eagle-eye.org/research.html

[129] https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

[130] http://fm4.orf.at/stories/1754728/

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“[131]. 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[132].

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:

- 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.)

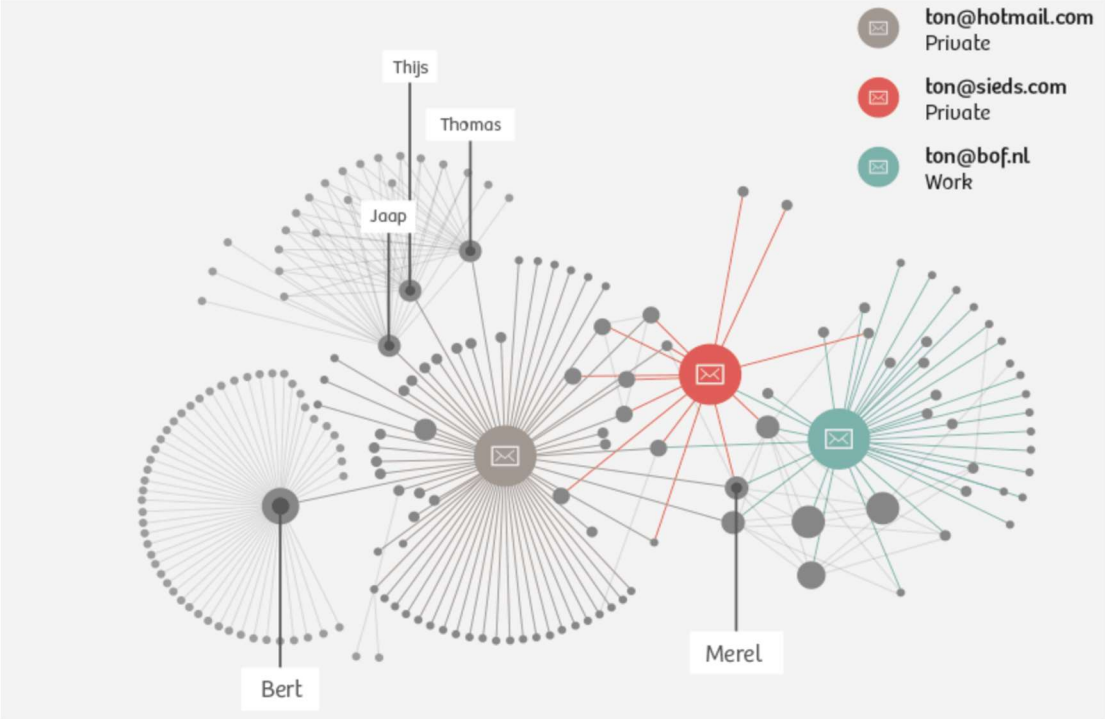
Oft sind mit Hilfe von Big Data Algorithmen aus diesen Metadaten mehr Informationen ableitbar, als aus den tatsächlich ausgetauschten Daten. Wenn ein Angreifer in der Lage ist, über längere Zeit den E-Mail Verkehr eines Benutzers zu beobachten, ist er im Stande ein sehr detailliertes Datenprofil über 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

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

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

aufschlussreichen Selbstversuch gezeigt, welche Informationen man beim Sammeln der Metadaten über eine Person anhäufen kann[133]. Nach einer Woche waren bereits 15.000 Datensätze angefallen.



Wie man in den Bild gut erkennen kann, gibt der Internet-Nutzer den Daten-Spionen nicht nur Inhalte sonder 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[134]. 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[135]“ 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[136].

---

[133] https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smartphone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt/
[134] https://www.divsi.de/mit-forscher-widerlegen-anonymitaet-von-metadaten/

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.

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.

Sechs Gefahrengruppen

Comidio hat die Internetgefahren in folgende sechs Gefahrengruppen (Threat-Typen) zusammengefasst. Auf Basis dieser Gefahrengruppen wurde die TrutzBox® entwickelt:

[135] http://www.globalcause.net

[136] https://resistsurveillance.org

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“[137] gibt eine recht gute Übersicht über Internet Zensur Europäischer Länder.

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

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 neun Poster veröffentlicht, die Internetnutzern aufzeigen, was sie bei der Nutzung des Internets beachten sollen[138].

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.

Allerdings hat jedes dieser Werkzeuge 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.

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 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:

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

- 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 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 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 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 zu auszustellen. Dabei wird gerade die chinesische Regierung beschuldigt, durch gefälschte Zertifikate auf verschlüsselte Daten bei Apple und Microsoft zugegriffen zu haben.[139]. Erste Zertifizierungs-Missbräuche sind in diesem Zusammenhang schon aufgedeckt worden[140].

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 zentralisierten Ansätze zu entgehen, ist im Internet eine Tendenz zu beobachten, die unter dem Namen „Eigenhosting“ bekannt ist. Eigenhosting bedeutet, dass der Internetnutzer selbst einen kleinen Server betreibt, auf dem E-Mail-, Cloud- und alternative Social Media Dienste laufen (z.B. *diaspora*[141] oder *ello*[142]) und seine Daten nur noch auf dem eigenen, häuslichen 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[143]).

Leider wird auch DNS[144] 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:

---

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

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

[141] https://diasporafoundation.org/

143 http://web.monkeysphere.info

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

FreedomBox

Ein erwähnenswertes Open-Source Projekt, das sowohl Eigenhosting als auch Anonymisierung zum Ziel hat, ist „FreedomBox“ [145]. 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“[146].

„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 Comidio TrutzBox®, 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 6, die die die Handhabung erleichtern soll.

De-Mail

Mit der De-Mail, „E-Mail made in Germany“[147] setzt die deutsche Bundesregierung die EU-Dienstleistungsrichtlinie (Richtlinie 2006/123/EG[148]) in nationales Recht um. Die Richtlinie verlangt, dass öffentliche Stellen ab Ende 2009 elektronische Kommunikation als verbindliches Übertragungsmedium akzeptieren.

---

145 http://freedomboxfoundation.org

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

147 http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/de_mail_node.html

148 http://de.wikipedia.org/wiki/Richtlinie_2006/123/EG_über_Dienstleistungen_im_Binnenmarkt

Damit sollte eigentlich eine sichere E-Mail Kommunikation in Deutschland eingeführt werden. Leider ist das misslungen, da mit einer fadenscheinigen Begründung auf eine Ende-zu-Ende Verschlüsselung verzichtet wurde[149]. BMI: „Eine Ende-zu-Ende Verschlüsselung gefährde das gesamte Ziel von De-Mail, die einfache – und ohne spezielle Softwareinstallation mögliche – Nutzbarkeit durch die Bürgerinnen und Bürger." Auch der Hinweis, man könne doch zusätzlich die De-Mails mit dem PGP-Verfahren verschlüsseln, bringt keine Verbesserung, da der Anwender wieder mit allen PGP-Verschlüsselungsproblemen alleingelassen wird (siehe auch Kapitel „TrutzMail - die unseres Wissens nach sicherste, und am einfachsten zu bedienende E-Mail"). Schließlich fragt sich der Anwender dann, was eigentlich der Mehrwert der aufwändigen De-Mail ist.

Realisiert und betrieben wird De-Mail von privatwirtschaftlichen Unternehmen, den De-Mail Providern.

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[150]:

- 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,[151]) 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

[149] https://www.datenschutzbeauftragter-info.de/de-mail-beschlossen-keine-ende-zu-ende-verschluesselung/

[150] https://netzpolitik.org/2016/volksverschluesselung-fuer-unfreie-buerger/

[151] https://geti2p.net/de/

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[152]“ 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[153].

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[154]. Aufgrund seiner komplexen Einstellmöglichkeiten, ist es allerdings mehr für technische Profis geeignet.

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

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

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

Die Webseite www.alternativeTo.net zeigt eine Übersicht der meist verbreiteten Browser-Plugins zum Schutz der Privatsphäre[155]. Sobald man allerdings tiefer in die Technik dieser Tracker-Filter einsteigt, werden einige Unterschiede in der Art und Weise wie diese Tools arbeiten, sichtbar[156].

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[157]. Wie soll ein Laie abschätzen können, ob er einem Plugin trauen kann?
- Frei verfügbare Browser-Plugins für Anonymisierungs-Web-Proxys, wie die von Startpage[158], Ixquick[159] und Immunityzone[160], schalten JavaScript und Cookies ab und können somit viele Webseiten nicht verarbeiten. Sie verhindern aber keine Daten-Tracker, die in die Webseiten programmiert werden. Alle diese zentral gehosteten Anonymisierungs-Web-Proxys haben außerdem den Nachteil, dass der 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 übergeben wird.
- 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.
- 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“[161] 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

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

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

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

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

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

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

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

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„[162].

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 Seiten filtert, nicht unbedingt das Beste ist[163]. 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 seine 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, und der Anwender kann sein E-Mail- und Browser-Programm weiterhin wie gewohnt weiter 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.

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

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

Leider werden zunehmend auch Tracking-Daten vom aufgerufenen Webservern selbst gesammelt. Diese werden dann für eigene Auswertungen genutzt, oder es werden fremde Datentracker-Dienstleister auf der Serverseite eingebunden und von dort aus Profildaten an die Tracker-Dienstleister übermittelt. Das kann auf der Browser-Seite nicht erkannt werden. Und selbst wenn, die aufgerufenen Webseite will man ja nicht blocken.

Hier zwei Beispiele (Stand 14.12.2015).

Die Seite welt.de lädt auf ihrer Seite das JavaScript „http://js.welt.de/resources/js/635/webtrekk.js“, und „geo.de“ lädt auf der Webseite http://www.geo.de/js/GEO/webtrekk_v3.js. Dabei handelt es sich um eine Software der Firma webtrekk.com, mit deren Hilfe welt.de bzw. geo.de Tracking-Daten sammeln kann. Solches serverseitige Tracken kann nicht durch eine Blocking-Liste verhindert werden. Hier sollte man clientseitig möglichst alles an Daten unterdrücken, die der Server zur Wiedererkennung (Fingerprinting) des Clients nutzen könnte. Genau das macht die TrutzBox zusätzlich zu ihren anderen Funktionen.

Ferner speichern beide Seiten, sowohl welt.de als auch geo.de, auf dem PC ebenfalls Cookies mit umfangreichen Browser-Profiledaten. Mit deren Hilfe ist der Webserver zu einem späteren Zeitpunkt in der Lage, den Nutzer wiederzuerkennen. Aber nicht nur Cookies liefern dem aufgerufenen Server Informationen über die Konfiguration seines Rechners und Browsers. Der aufgerufene Webserver erhält auch über weitere HTTP-Header, wie user-agent und accept-language, spezifische Nutzerdaten, mit deren Hilfe er ein Fingerprinting durchführen kann und auch durchführt.

Werkzeuge, die lediglich aufgerufene Tracker-Links blockieren, können diese mittlerweile übliche Art des Trackings, über die aufgerufene Seite nicht verhindern.

Diese Art des Trackings lässt sich nur verhindern, indem man **alle Daten**, die an **alle Server** übermittelt werden, auf solche nutzerspezifischen Daten hin überprüft und solche Daten löscht oder „neutralisiert“. Und ein Browser-Plugin wird dazu nie in der Lage sein.

Und genau das macht die TrutzBox®.

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.

Aber falls 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.

Drei technische Möglichkeiten gibt es, die IP-Adresse so zu verschleiern, dass der Server, von dem Daten abgerufen werden, die IP-Adresse des Clients nicht erkennen kann:

- VPN Gateways und Internet-Proxys
- Tor
- Mixed-Kaskaden (JonDos)

Bei allen drei Möglichkeiten 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[164].

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 drei IP-Adressen-Verschleierungstechniken

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 „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.

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“[165].

[164] http://www.heise.de/security/meldung/I-f-Tor-Deanonymisierung-zu-81-erfolgreich-2458992.html?wt_mc=nl.heisec-summary.2014-11-20
[165] https://www.heise.de/newsticker/meldung/VPN-Anbieter-Aktivisten-beklagen-Datenmissbrauch-3795523.html

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, verschweigen aber leider, wie sie das angestellt haben wollen.

Tor

Wenn Webseiten über das Tor-Netzwerk[166] aufgerufen werden, kann Tor die IP-Adresse verschleiern. Technisch ist es 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 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[167]. Nicht nur Geheimdienste sind gerade an dem Tor-Datentransfer sehr interessiert. Auch kriminelle Hacker haben sich solchen Exit-Servern bedient, um Schadcodes zu verteilen[168].

Selbst die Tor Entwickler warnen mittlerweile davor, sich zu sehr auf Tor zu verlassen[169]. 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-

166 https://de.wikipedia.org/wiki/Tor_(Netzwerk)

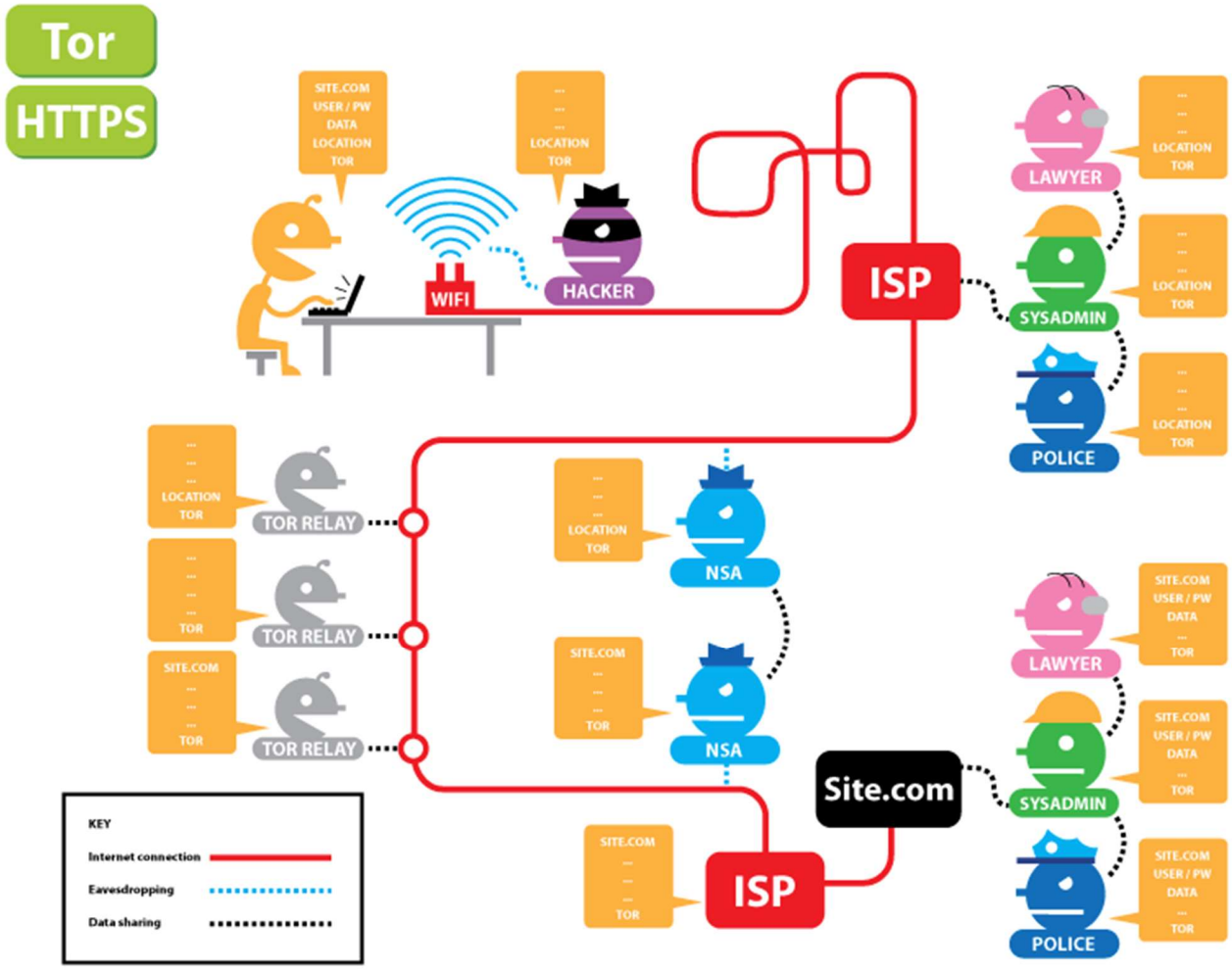
167 http://www.heise.de/newsticker/meldung/Neues-von-der-NSA-Tor-stinkt-1972983.html

168 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

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

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.



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 Austritts-Tor-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

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

Mixed Kaskaden

Ein dritter Ansatz, die IP-Adresse zu verschleiern, sind Mixed Kaskaden (JonDos). Mixed Kaskaden funktionieren ähnlich wie Tor, allerdings sind die Kaskaden (Proxy) Betreiber bekannt und werden vom Betreiber des Anonymisierungsdienstes zertifiziert. Es ist einem Angreifer somit kaum möglich, einen eigenen Proxy einzuschleusen. JonDos (https://www.anonym-surfen.de/jondo.html) bietet derzeitig als Einziger diese Technologie an.

Keine IP-Verschleierungstechnik ist perfekt

Vergleicht man die drei vorgestellten Anonymisierungsdienste, so bieten die VPN Betreiber den geringsten und JonDos den größten Schutz gegen die Aufhebung der Anonymisierung (also Rückverfolgung) der IP-Adresse. Ansonsten gelten für JonDonym die gleichen Abhörmöglichkeiten wie in der Tabelle bei TOR aufgeführt.

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.

Alle drei 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 möglich 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.privacytools.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[170]. 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 http://ip-check.info 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[171] oder JonDoFox[172] zu verwenden. Leider sind beide Browser derart restriktiv, dass normales Surfen im Internet bei vielen Webseiten sehr schnell zu Funktionsproblemen führt. Der Browser JonDoFox kann allerdings nachträglich vom Anwender sehr gut umkonfiguriert werden, sodass Comidio diesen Browser empfehlen kann.

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

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

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

[172] https://www.anonym-surfen.de/software_win.html

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 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 des Mail-Programms mit seinem Mail-Server zwar verschlüsselt, aber der Mail-Provider kann unverschlüsselte Mails lesen. Und die Kommunikation zwischen den Mail-Servern ist meist 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 tausende Lösungen für Chat- und Audio-/Video-Kommunikation im Markt etabliert. Firmen nutzen Video-Konferenz-System Services wie z.B. von Adobe oder Cisco, um intern oder mit externen Teilnehmen zu konferieren. Im Privatmarkt haben sich Skype und WhatsApp als Messenger und Konferenzwerkzeug durchgesetzt.

Zunehmend haben die Hersteller dieser Software auch Funktionen zum End-to-End Verschlüsseln der Kommunikationsinhalte eingebaut[173].

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.

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

Was ist eine „Privacy-Box“?

Was versteht man unter einer "Privacy-Box" bzw. was kann man von ihr erwarten?

Definition von Comidio:

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

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

Schutz für alle Internetaktivitäten: eine 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 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 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. Deswegen wird von einer Privacy-Box zusätzlich auch Internet-Sicherheit erwartet.

Schutz aller Geräte: eine 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.

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 für Apps auf PCs oder Smartphones nicht zur Verfügung stehen, 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 Privacy-Box auch verschlüsselten Datenverkehr kontrollieren soll. Ja, soll sie. Denn gerade Apps kommunizieren verschlüsselt mit Daten-Trackern, die die Privatsphäre kompromittieren. Einer 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 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 Privacy-Box möglichst ohne Änderung der Benutzer-Gewohnheiten automatisch funktionieren. Somit sollte der Nutzer alle seinen gewohnten 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 Privacy-Box den Nutzer nicht einschränken und in seinem Tun behindern.

Man muss der Privacy-Box vertrauen können: da eine Privacy-Box als eines der besten Überwachungsinstrumente missbraucht werden könnte, ist es unabdingbar, dass man der Privacy-Box vertrauen kann. Dazu gehört, dass sämtliche Software der Privacy-Box 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.

Natürlich hat eine 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, sich mit diesem zusätzlichen Device zu beschäftigen.

Aber die Vorteile einer Privacy-Box liegen auf der Hand: nur eine Privacy-Box, 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“ [174]

Mit Hilfe der TrutzBox, die der Benutzer vor seinen Internet-Router schaltet, wird kontrolliert, welche Daten vom Internet in sein internes Netzwerk gelangen dürfen und welche Daten er herausgeben möchte.

(© 2015 Comidio GmbH)

Dadurch gibt die TrutzBox die Kontrolle über die Daten an den Benutzer zurück. Die TrutzBox® ist somit ein Werkzeug zur „Digitalen Selbstverteidigung“.

Sie bietet folgende Sicherheits- und Anonymisierungsvorteile:

- Im Internet surfen, ohne dass Datenspuren des Nutzers von anderen mitgelesen werden können (TrutzBrowse)
- 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 auf Dienstleister im Internet angewiesen, die ihm nicht die erforderliche Sicherheit und Anonymität bieten,
- Video-Konferenzen und Chat (Messaging) TrutzRTC. Dadurch ist der Nutzer nicht mehr auf Dienstleister wie Skype oder Whatsapp angewiesen, bei denen er die Services mit seinen Daten bezahlt.

[174] 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 (Virenscanner, Firewall und DPI).

Somit kann der Internet-Nutzer mit Hilfe der TrutzBox® kontrollieren, welche Daten er wem geben möchte. Das Einmalige 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 Device sondern auch Fernseher, mobile Geräte wie iPhone, iPad, Android-Devices usw. als auch schon vorhandene oder zukünftige „Smart Home“ Devices 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 comidio.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 TrutzRTC.

Das Servicepaket beinhaltet:

- ein Kontingent von 5 TrutzMail Accounts pro TrutzBox® für eine Laufzeit von 12 Monaten (während der TrutzBox Betaphase waren es 24 Monate). Gleichzeitig erhält er regelmäßig Updates der Empfänger-Zertifikate – damit werden abgelaufene oder kompromittierte Zertifikate anderer TrutzMail Accounts Ihrer TrutzBox bekannt gemacht.
  Das Kontingent kann im Comidio Shop jederzeit um weitere TrutzMail Accounts erweitert werden
- Update Services für
  1. TrutzBase: Signaturen und Updates für Virenscanner
  2. TrutzBox® Software-Fehlerbeseitigungen, Sicherheits-Updates und kleinere funktionelle Erweiterungen
- TrutzContent: Updates für Filterlisten
  3. TrutzBrowse: Updates für Header-Ergänzungen und 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.

Abhängig davon, ob der Kunde die Services verlängert, erhält er folgende Leistungen:

Fall 1: Mit Vertragsverlängerung:

	#	Leistungen	1. Jahr Services automatisch mit TrutzBox gekauft	2. Jahr Services-Verlängerung gekauft	3./x. Jahr Services-Verlängerung gekauft
Services	1	Netzwerksicherheit (TrutzBase): Signaturen und Updates für Virenscanner	**Betrieb mit Updates** **60 €** 5 TrutzMail Adressen (à 1 € pro Adresse und Monat) über 12 Monate	**Betrieb mit Updates** **60 €** 5 TrutzMail Adressen (à 1 € pro Adresse und Monat) über 12 Monate	**Betrieb mit Updates** **60 €** 5 TrutzMail Adressen (à 1 € pro Adresse und Monat) über 12 Monate
Services	2	TrutzBox® Software: Fehlerbeseitigungen, Sicherheits-Updates und kleinere funktionelle Erweiterungen			
Services	3	Jugendschutz (TrutzContent): Updates für Filterlisten			
Services	4	Spurenlosese Surfen (TrutzBrowse): Updates für Header-Ergänzungen und Blacklists			
Betrieb	5	Sichere E-Mail (TrutzMail): - sichere E-Mail-Adressen je nach gekauftem Kontingent - Update der Empfänger-Zertifikate – damit werden abgelaufene oder kompromittierte Zertifikate anderer TrutzMail Accounts Ihrer TrutzBox® bekannt gemacht			
	6	Gewährleistung TrutzBox® (Hardware und TrutzBox® Services)	2 Jahre Gewährleistung		

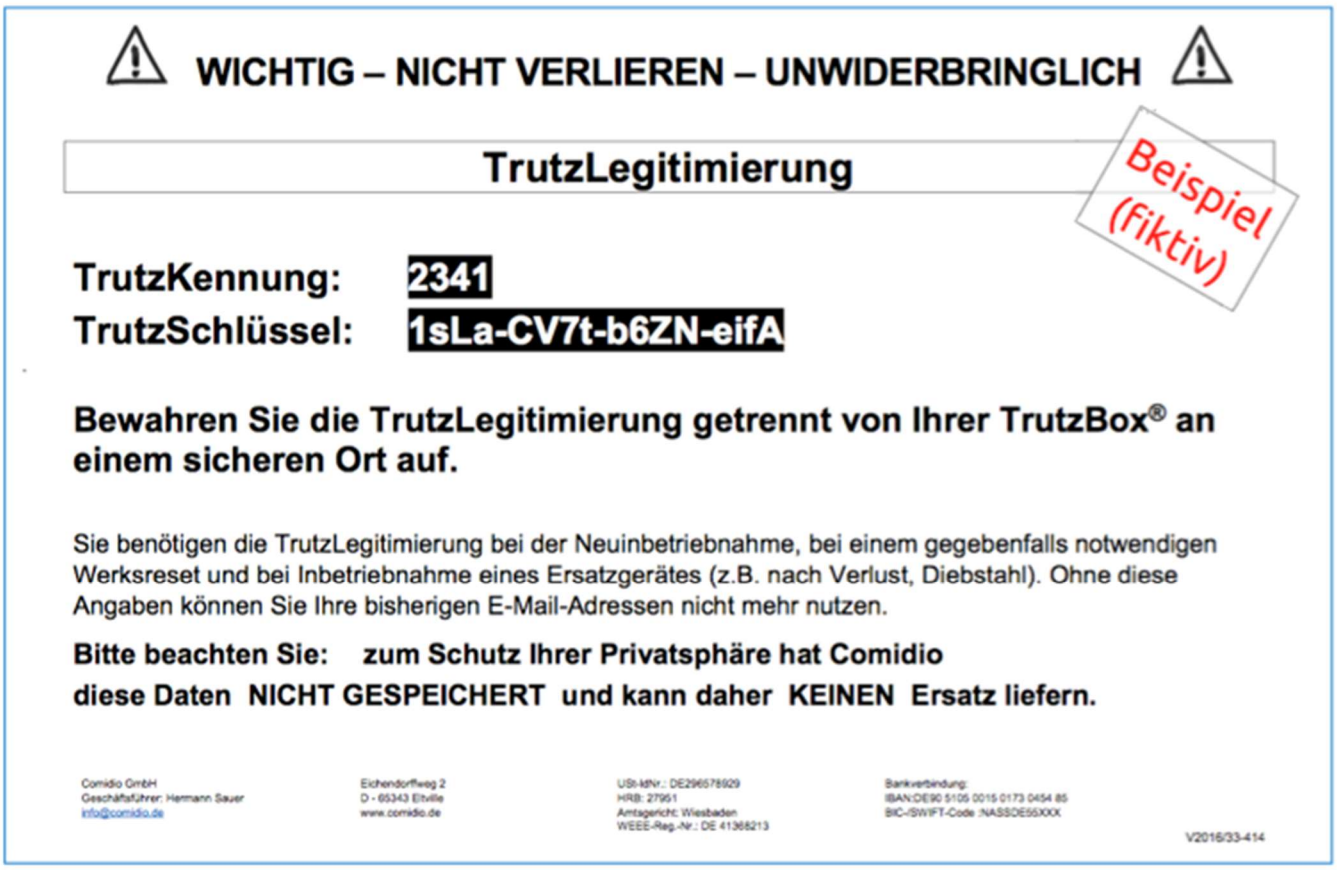
Fall 2: Ohne Vertragsverlängerung:

	#	Leistungen	1. Jahr Services automatisch mit TrutzBox gekauft	2. Jahr Services-Verlängerung nicht gekauft	3./x. Jahr Services-Verlängerung nicht gekauft
Services	1	Netzwerksicherheit (TrutzBase): Signaturen und Updates für Virenscanner	**Betrieb mit Updates** **60 €** 5 TrutzMail Adressen (à 1 € pro Adresse und Monat) über 12 Monate	**Betrieb mit Updates**	**Betrieb mit Updates**
Services	2	TrutzBox® Software: Fehlerbeseitigungen, Sicherheits-Updates und kleinere funktionelle Erweiterungen		Betrieb möglich (ohne Updates)	Betrieb möglich (ohne Updates)
Services	3	Jugendschutz (TrutzContent): Updates für Filterlisten			
Services	4	Spurenlosese Surfen (TrutzBrowse): Updates für Header-Ergänzungen und Blacklists			
Betrieb	5	Sichere E-Mail (TrutzMail): - sichere E-Mail-Adressen je nach gekauftem Kontingent - Update der Empfänger-Zertifikate – damit werden abgelaufene oder kompromittierte Zertifikate anderer TrutzMail Accounts Ihrer TrutzBox® bekannt gemacht		kein Betrieb	kein Betrieb
	6	Gewährleistung TrutzBox® (Hardware und TrutzBox® Services)	2 Jahre Gewährleistung		

Der Kunde kann somit 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.



(© 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. Nach dem Zurücksetzen der TrutzBox® auf Auslieferungszustand sind allerdings alle Einstellungen und die noch auf der TrutzBox® gespeicherten TrutzMails gelöscht. Bei Verkauf der TrutzBox® Hardware 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) 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.

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 comidio.de ein, wird ihm eine Übersicht seiner 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 SD-Karte, 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 SD-Karte) austauschen, da der Kunde mit Hilfe dieser TrutzLegitimierung die neue TrutzBox® Hardware, mit seinen registrierten TrutzMail Adressen, wieder in Betrieb nehmen kann.

Der Kunde kann auch seine Hardware nach Rücksetzung auf Auslieferungsstand ohne Risiko verkaufen, und der Käufer kann diese gebrauchte TrutzBox® Hardware nutzen, indem er diese mit seiner eigenen TrutzIdentifikation in Betrieb nimmt.

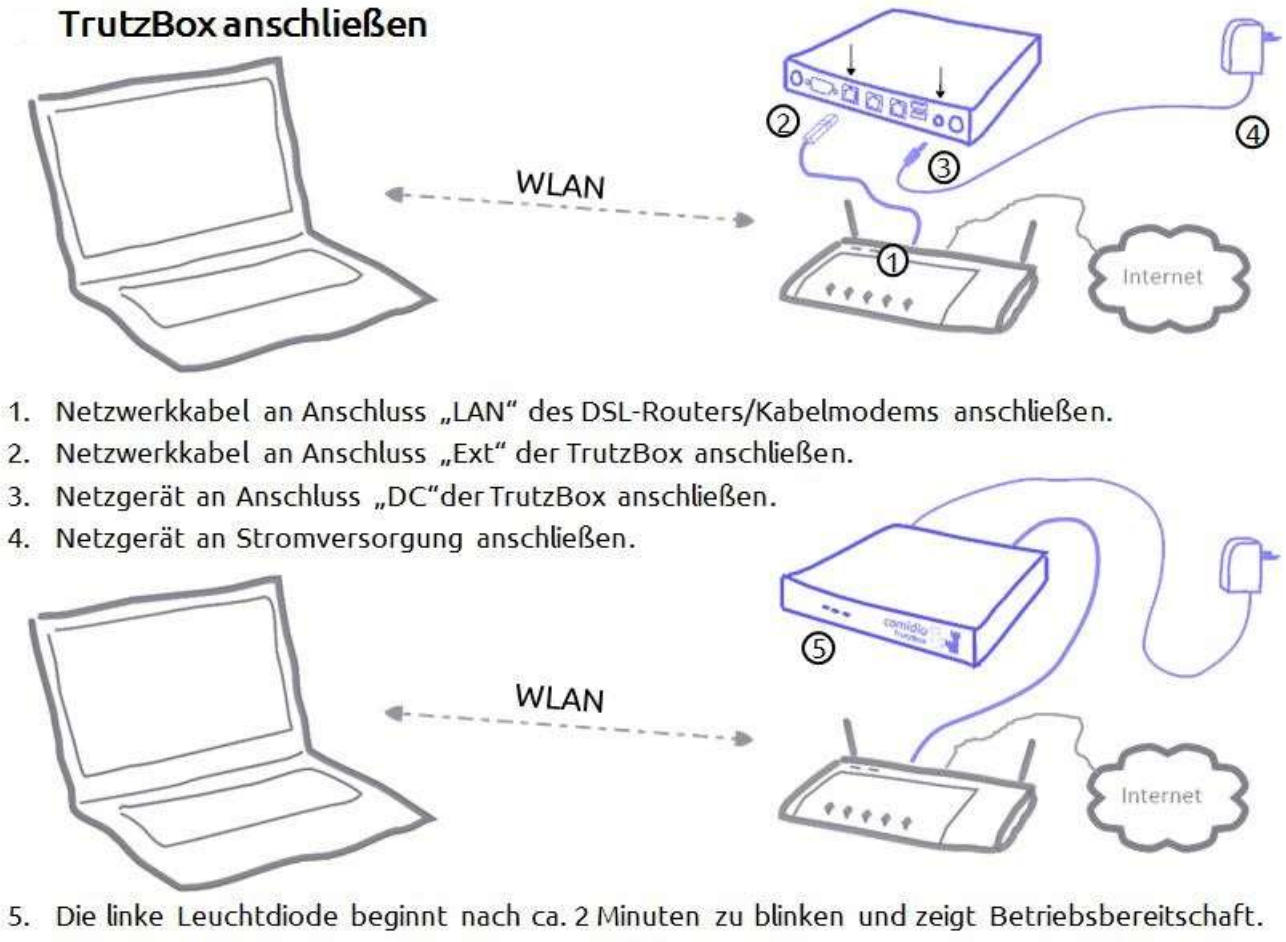
Comidio speichert die TrutzLegitimierung aus Sicherheitsgründen nicht. Falls der Kunde seine TrutzLegitimierung verliert, kann diese nicht wieder hergestellt werden. Er kann somit seine TrutzBox® mit seinen registrierten TrutzMails nicht mehr neu einrichten. Er verliert das Recht auf seine schon registrierten 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

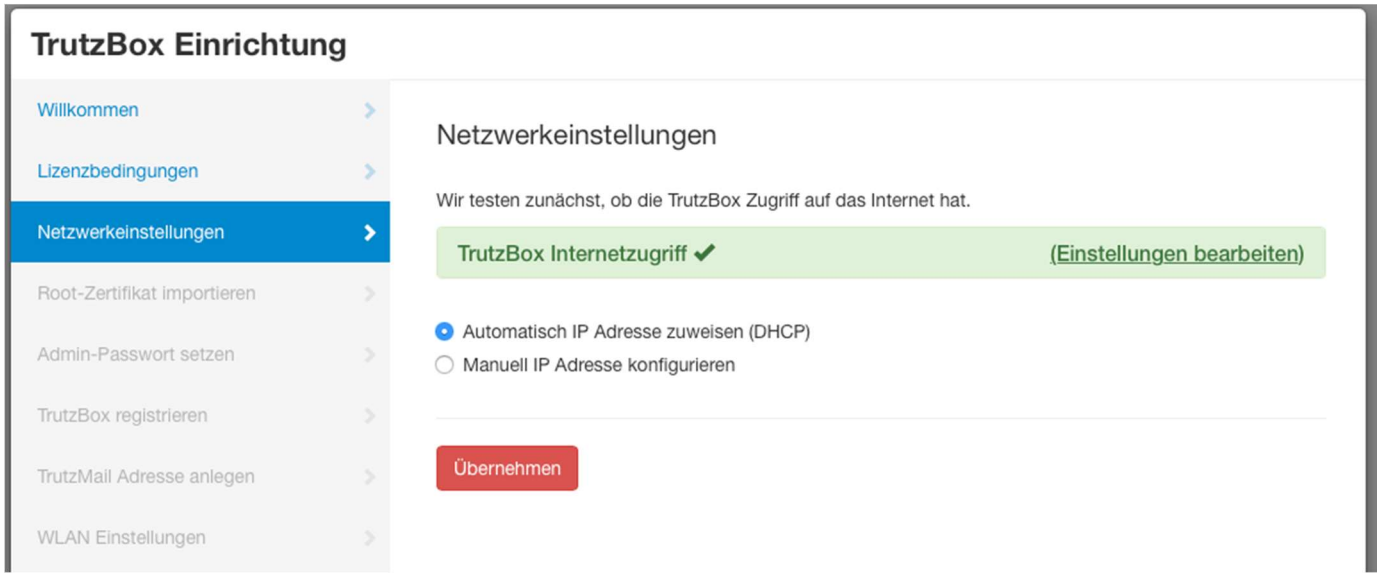
Die Verkabelung ist recht einfach, da die TrutzBox® lediglich an den Internet-Router angeschlossen werden muss.

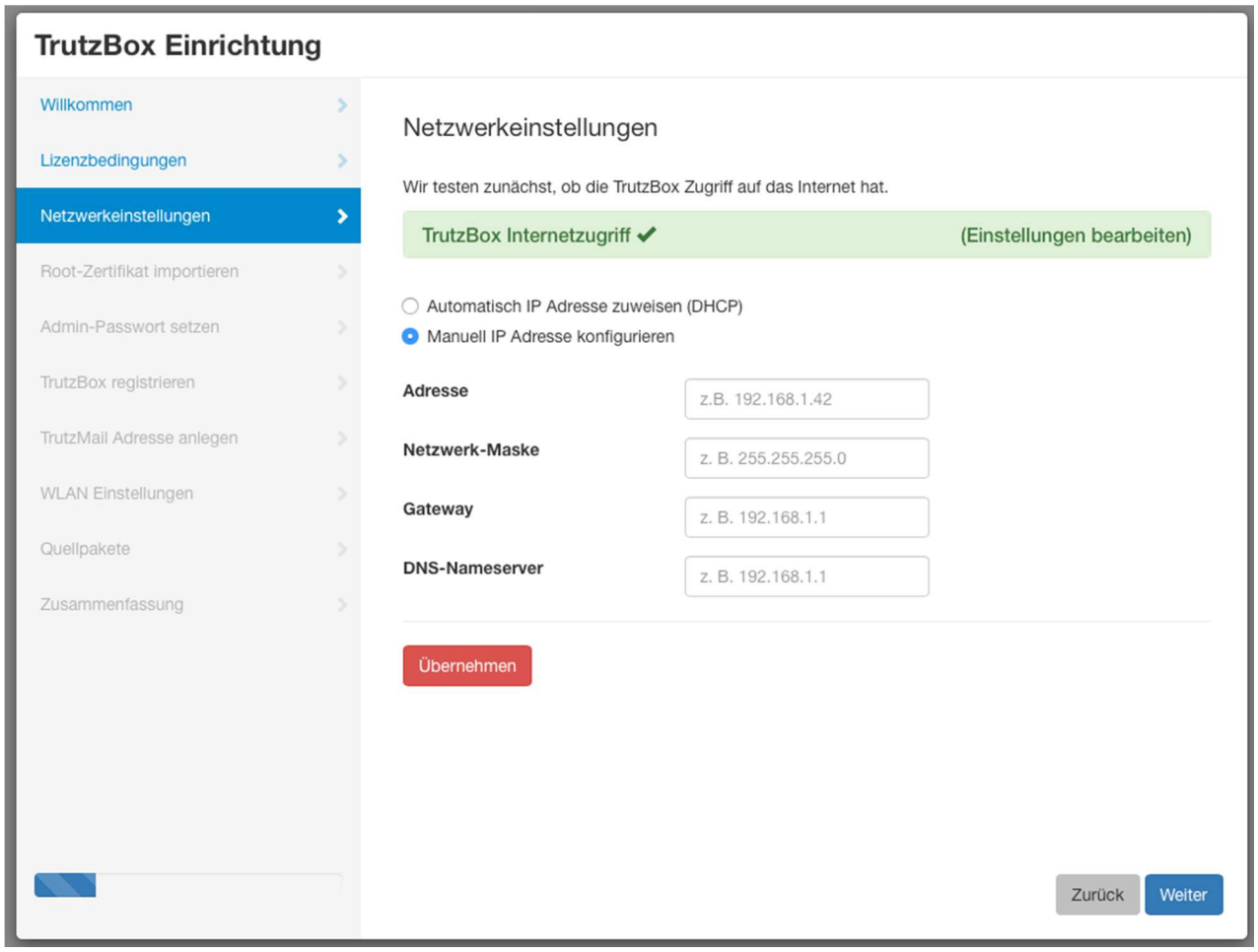


Schritt 2: TrutzBox® Setup

Das TrutzBox® Setup kann nun über einen am Internet-Router angeschlossenen PC ausgeführt werden. 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 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.





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

Nun sind nacheinander folgende Schritte durchzuführen:

1. Bestätigung der Lizenzbedingungen
2. TrutzBox Rootzertifikat importieren
3. ein TrutzBox Admin-Passwort setzen,
4. die TrutzBox mit Hilfe der mitgelieferten TrutzLegitimierung (TrutzKennung und TrutzSchlüssel) registrieren,
5. für sich selbst eine erste sichere TrutzMail Adresse vergeben und
6. eine individuelle WLAN-SSID und ein sicheres WLAN-Passwort festlegen.

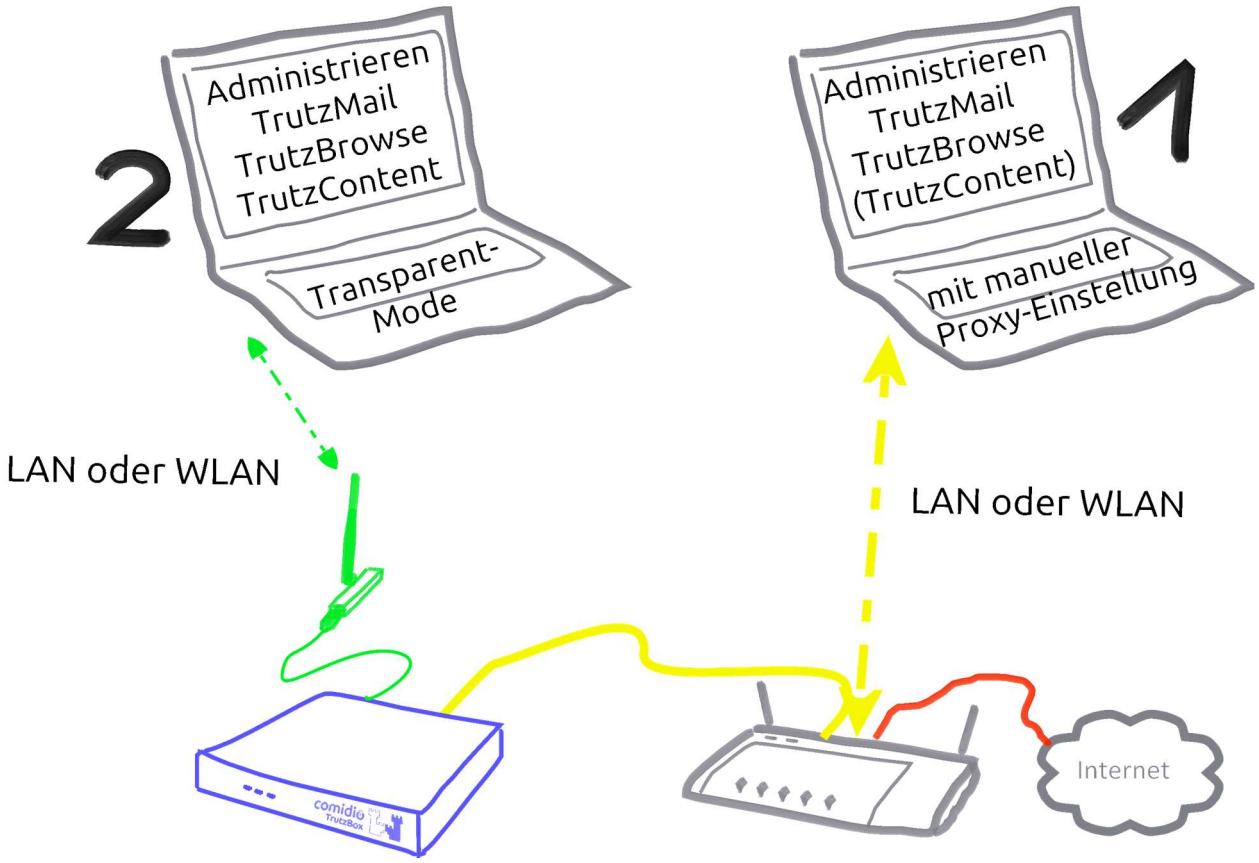
Mit diesen sechs Schritten wird die TrutzBox® eingerichtet. Die TrutzBox® prüft danach, ob die TrutzKennung und der TrutzSchlüssel (TrutzLegitimation) korrekt sind und ob die gewünschte erste TrutzMail Adresse noch frei ist. Falls nicht, müssen diese Daten geändert werden.

Danach prüft die TrutzBox, ob Updates für die ausgelieferte TrutzBox Version anstehen. Wenn ja, werden diese automatisch eingespielt.

Es erfolgt die Weiterleitung in die TrutzBox® Verwaltungsoberfläche (Administrator User-Interface [TrutzBox UI]). Danach ist die TrutzBox® betriebsbereit und kann von allen Internet-Geräten ab sofort genutzt werden.

Schritt 3: Benutzer Devices an der TrutzBox® anschließen

Es gibt zwei Möglichkeiten, ein Gerät (z.B. PC, mobiles Device, Fernseher ...) an die TrutzBox® anzuschließen, über einen Proxy-Eintrag (1) im Browser oder direkt per Netzwerk (2).

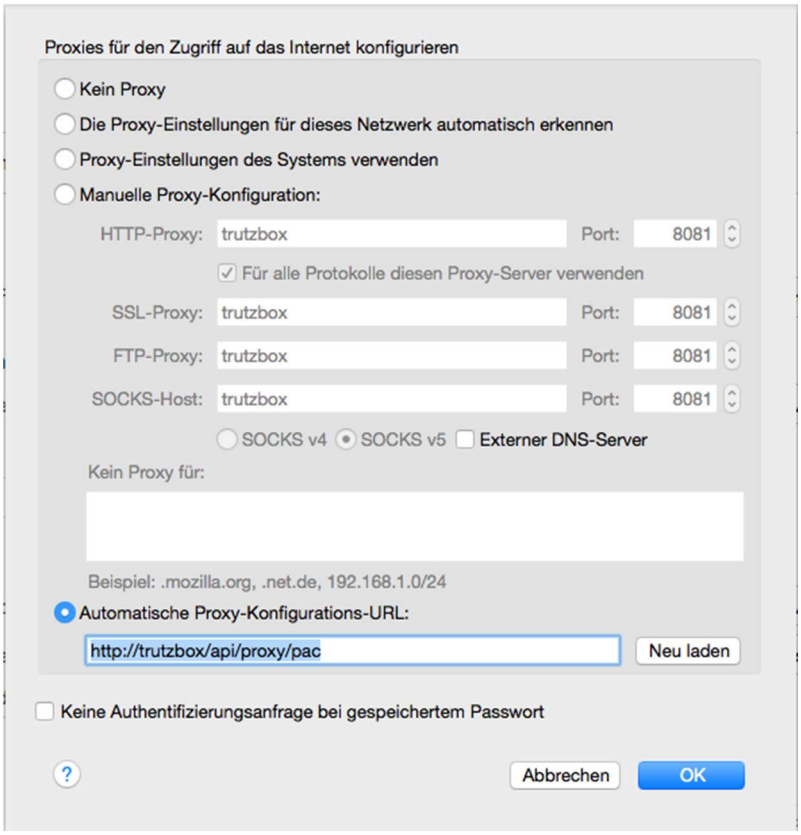


Für jedes Gerät kann individuell entschieden werden, über welche der beiden Anschlussmöglichkeiten das Gerät die TrutzBrowse und TrutzContent Funktionen der TrutzBox® nutzen soll. Comidio empfiehlt, zunächst ein Gerät im Proxy-Mode (Möglichkeit 1) z betreiben, um erste Erfahrungen mit der TrutzBox zu sammeln. Möglichkeit 2 sollte nur von erfahrenen TrutzBox Nutzern genutzt werden:

Möglichkeit 1: Internet Device bleibt am angeschlossenen Internet-Router angeschlossen (Proxy-Mode)

Die TrutzBox® kann auch von Geräten benutzt werden, die am Internet-Router angeschlossen bleiben, somit netzwerkmäßig nicht direkt an die TrutzBox® angeschlossen sind. Dazu muss eine Proxy-Einstellung im Browser durchgeführt werden. Hierfür 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:



Die Anschlussmöglichkeit 1 kann somit nur von Geräten genutzt werden, die die Möglichkeit bieten, einen Proxy zu konfigurieren.

Allerdings bedeutet dies, dass

- die Funktionalität von TrutzBase für diese Geräte eingeschränkt ist und
- TrutzContent (Jugendschutz) mit etwas technischem Wissen umgangen werden kann.

Geräte, die per Proxy die TrutzBrowse/TrutzContent Funktion nutzen, werden im TrutzBox® Administrator-Menü mit der Endung des Internet-Router Hostnamens (z.B. FRITZ!Box) aufgeführt.

Möglichkeit 2: Internet Device wird an TrutzBox Netzwerk angeschlossen (Transparent-Mode)

Um die volle TrutzBox® Funktionalität zu nutzen, können Geräte netzwerkmäßig direkt per WLAN oder LAN-Kabel an der TrutzBox® angeschlossen werden. Falls die Geräte direkt an der TrutzBox® angeschlossen sind, kontrolliert die TrutzBox die gesamte Internet-Datenkommunikation aller Anwendungen (nicht nur des Web-Browsers), die über Port 80 oder 443 erfolgen. Es brauchen 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. Das ist besonders beim Einsatz der TrutzContent Funktion wichtig (Jugendschutz).

Meist möchten Anwendungen (nicht der Browser) jedoch über Port 443 eine verschlüsselte Verbindung zu einem Server aufbauen. Das können beliebige Apps sein oder vom Hersteller mitgelieferte Anwendungen, wie

Adressbuch und Kalender, die ihre Daten mit einem Server synchronisieren. Solche Anwendungen authentisieren den Server über ein Zertifikat, das in der Apps fest einprogrammiert ist. Solche Datenkommunikation kann die TrutzBox® zwar erkennen, aber nicht entschlüsseln und somit auch nicht kontrollieren. Falls die TrutzBox® eine solche verschlüsselte Kommunikation erkennt, kann sie optional die Kommunikation auf diesen Server frei schalten (Security-Einstellung auf L10).

Falls ein Programm eines angeschlossenen Devices trotzdem Kommunikations-Probleme hat, kann man diese Symptome mit Hilfe der TrutzBox® analysieren und durch weitere Konfigurationsmöglichkeiten manuell beheben.

Beim Anschluss per LAN-Kabel werden die beiden freien LAN-Anschlüsse 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.

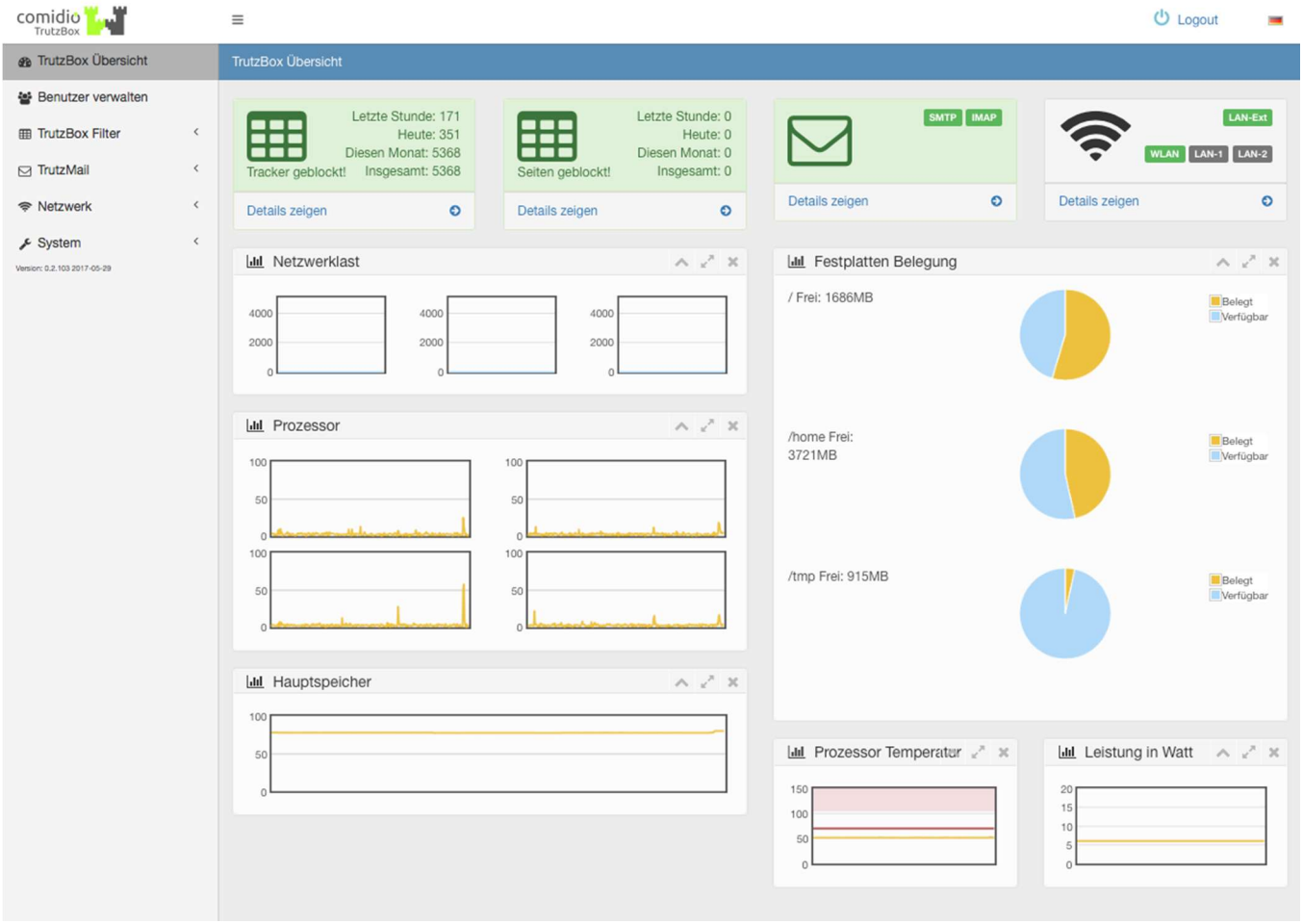
Sollen zukünftig alle Geräte die TrutzBox® nutzen, könnte das WLAN des Internet-Routers sogar abgeschaltet werden.

Details zu diesen Einstellungen sind dem TrutzBox® Handbuch unter comidio.de/wiki zu entnehmen.

Mit einem Internet-Browser kann mit http://trutzbox die Administrator-Bedienoberfläche der TrutzBox® aufgerufen werden und nach dem Login mit dem TrutzBox® Administrator-Passwort, das beim Setup vergeben wurde, können dann weitere Einstellungen vorgenommen werden (z.B. weitere TrutzBox® Benutzer einrichten und zusätzliche TrutzMail Adressen vergeben).

TrutzBox Administrator Oberfläche – Übersicht

Mit einem Browser-Aufruf von http://trutzbox lässt sich die TrutzBox Administrator Oberfläche starten. Die erste angezeigte Seite ist die TrutzBox Übersicht.



(© 2017 Comidio GmbH)

Dort werden folgende Daten angezeigt:

- eine Zusammenfassung der statistisch erhobenen Blocking-Daten von TrutzBrowse (Tracker geblockt) und TrutzContent (Seiten geblockt),
- Status der beiden Mail-Prozesse (SMTP und iMAP müssen beide grün sein),
- Netzwerk-Status (aktive Netzwerk-Adapter sind grün),
- Auslastung der TrutzBox (Netzwerk, CPUs und Hauptspeicher),
- Hardware-Daten, wie Auslastung des Speichermediums, Temperatur und aktueller Leistungsverbrauch.

Dabei bedeuten die Hardware-Daten folgendes:

Prozessor Temperatur (CPU):

- gelbe Linie, aktuelle Temperatur, hier bei ca. 40 Grad.
- rote Linie, die bisher höchste gemessene Temperatur, hier ca. 70 Grad.
- hell-rote Fläche, sollte nicht überschritten werden, TrutzBox schaltet sich automatisch bei ca. 105 Grad ab.

Leistung in Watt

- derzeitiger Leistungsverbrauch der TrutzBox, hier ca. 6 Watt; das ist der Leerlauf-Verbrauch einer APU2 TrutzBox mit WLAN-Modul.

TrutzBox Administrator Oberfläche – Account verwalten

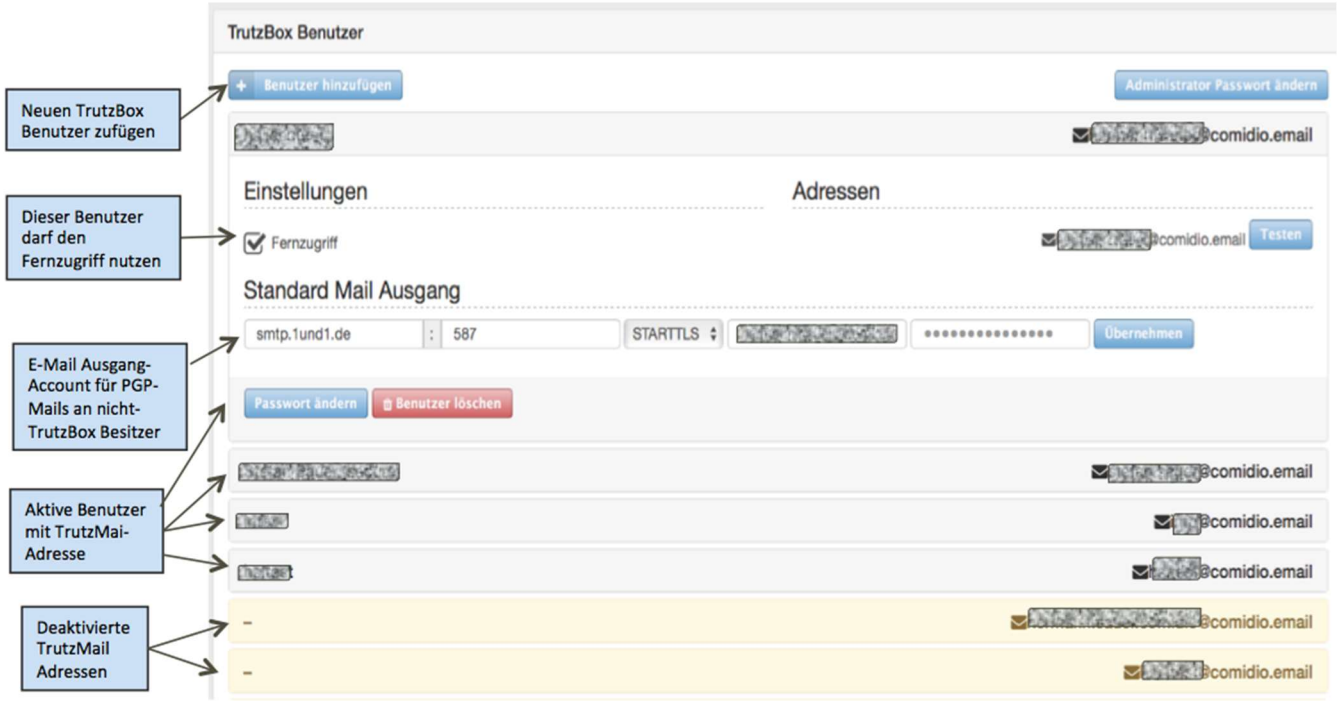
Die TrutzBox hat eine eigene Verwaltung ihrer Benutzer. Es gibt drei Arten von Nutzer-Accounts:

- der Benutzer „admin“ gibt es nur einmal und wird automatisch beim Einrichten (Setup) der TrutzBox angelegt. „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.
- Ein normaler TrutzBox Benutzer – der keine TrutzMail Adresse hat. Dieser kann für TrutzContent verwendet werden.
- Ein TrutzBox Benutzer, der auch eine TrutzMail Adresse hat. Diese TrutzMail Adresse kann aktiviert oder deaktiviert sein. Aktive TrutzMail Adressen werden benötigt für TrutzMails (zwischen TrutzBoxen), PGP-Mails an nicht-TrutzBox Besitzer, für Chat und um einen Video-Konferenzraum zu öffnen. Teilnehmer einer Video-Konferenz und TrutzBrowse Nutzer benötigen keine Benutzer-Id auf der TrutzBox.

Da die Anzahl der TrutzMail Adressen durch den Service-Vertrag begrenzt ist, ist es hiermit möglich, beliebig viele lokale Benutzer ohne TrutzMail Adresse an zu legen. TrutzMail Adressen müssen über alle TrutzBoxen hinweg eindeutig sein. Lokale Nutzernamen müssen lediglich auf der eigenen TrutzBox eindeutig sein.

Benutzer mit einer TrutzMail Adresse können aktiv oder deaktiviert sein. TrutzMail Adressen werden automatisch deaktiviert, wenn der Service-Vertrag ausläuft oder wenn die TrutzBox nach einem Reset auf Werkseinstellung neu aufgesetzt wird. Falls der Service-Vertrag es erlaubt, können deaktivierte TrutzMail Adressen re-aktiviert werden.

Im Menüpunkt „Account verwalten“ können weitere Benutzer hinzugefügt, 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.



(© 2017 Comidio GmbH)

Im Menüpunkt „Account verwalten“ ist eine Übersicht über den Service-Vertrag aufgelistet.

(© 2017 Comidio GmbH)

Dabei haben die Felder folgende Bedeutung:

- TrutzKennung - die TrutzKennung mit der diese TrutzBox in Betrieb genommen wurde
- Aktivierung - das Datum, an dem die TrutzBox erstmalig in Betrieb genommen wurde
- Service-Vertrag gültig bis - Datum an dem der Service-Vertrag abläuft
- TrutzMail Kontingent – wie viele TrutzMail Adressen diese TrutzKennung einrichten darf und wie viele davon derzeit aktiv sind

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.

- 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.

Warum hat die TrutzBox kein offizielles Zertifikat, das vom Browser automatisch anerkannt wird?

Das TrutzBox Zertifikat (2), das in jedes Gerät importiert werden muss, erfüllt zwei unterschiedliche Zwecke:

- Es wird zum einen vom Mail-Client, XMPP-Client und auch vom Browser genutzt, um die entsprechende TrutzBox Server-Software zu authentisieren, also um den TrutzBox Mail-Server, den -XMPP-Server und den –Web-Server (für TrutzBox UI, XMPP-Client und Webmin) zu authentisieren. Für diesen Zweck könnte man zwar ein offizielles Zertifikat kaufen, also ein Zertifikat, dessen Gültigkeit durch ein auf PC-Seite vorhandenes Stamm-Zertifikat bestätigt werden kann. Allerdings kann man ein solches Server-Zertifikat nur für eindeutige Domains, die aus dem Internet aus erreichbar sind, kaufen. Das ist bei der TrutzBox nur gegeben, wenn der TrutzBox Anwender für sich eine DynDNS-Adresse eingerichtet und Port 80/443 auf seinem Internet-Router geöffnet hat. Das ist oft nicht der Fall. Aus diesem Grund generiert die TrutzBox beim Setup ein eigenes Zertifikat das für die Authentisierung der Anwendungen auf Client-Seite importiert werden muss.

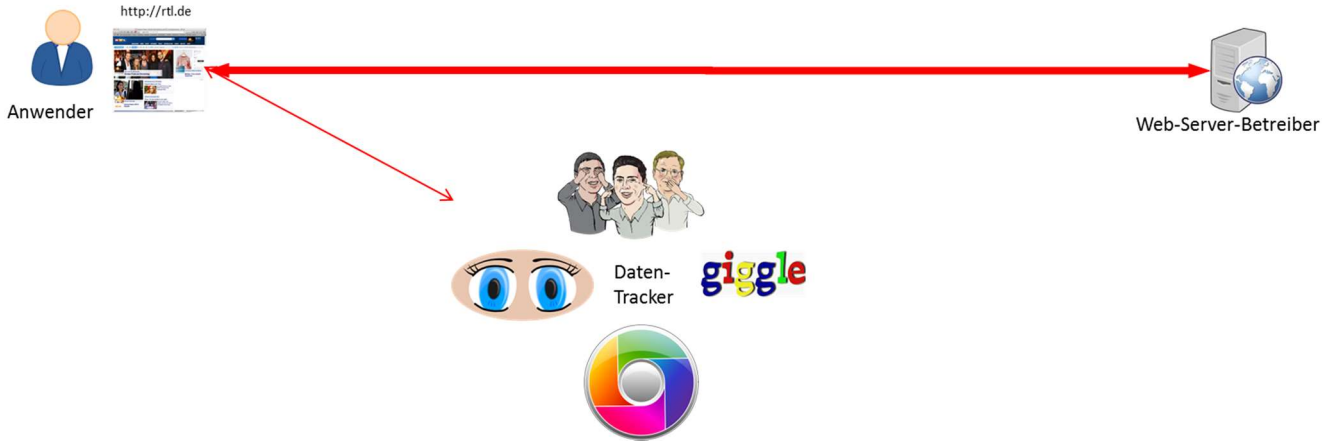
- Zum Zweiten wird das TrutzBox Zertifikat dazu verwendet, um für jede über TrutzBrowse aufgerufene SSL verschlüsselte Webseite, für die ein neues SSL-Zertifikat generiert wird, mit diesem TrutzBox Zertifikat zu signieren (sorry ich weiß, dieser Satz ist etwas kompliziert). D.h. das TrutzBox Zertifikat ist kein normales Server-Zertifikat, sondern ein Stamm-Zertifikat. Nur damit ist die TrutzBox in der Lage, eine verschlüsselte Verbindung zwischen Browser und Web-Server „aufzubrechen“ und neue, dynamisch beim Surfen generierte Server-Zertifikate zu signieren. Und nur wenn dieses Stamm-Zertifikat in den Client geladen wird, wird der Client jedes von der TrutzBox generierte und damit signierte Zertifikat, als gültig anerkennen. Ein solches Stamm-Zertifikat kann man nicht kaufen.

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 Setup der TrutzBox neu generiert. Die Schlüssel in den Zertifikaten werden dadurch ebenfalls erneuert.

TrutzBrowse - Im Internet surfen, ohne dass Dritte Datenspuren mitlesen können

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 TrutzBrowse Funktion ist kein „Werbeblocker“. In der Regel verhindert die TrutzBox® nicht, dass im Browser Werbung angezeigt wird. Diese Funktion kann der TrutzBox® Administrator allerdings bei Bedarf einschalten. 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 nicht mehr ohne ihr Wissen über Jahre gespeichert und gewinnbringend vermarktet werden. Informationen, die vom Server zum Browser gelangen (wie z.B. Werbung), sind somit i.d.R. unkritisch. Aber die Daten die vom Browser zu einem Server gehen müssen kontrolliert werden.

Wie bereits festgestellt, kann der Web-Server Betreiber oder Dritte, Sie beim Surfen im Internet ausspähen. Und das sogar Webseiten übergreifend. Dies geschieht, indem der „Ausspäher“ Sie durch Ihre einmalige Browser- und Betriebssystem-Einstellungen (Browser-Fingerprint) 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, die Domains von bekannten Trackern blockieren oder sogar speziell angepasste Browser (Tor-Browser und JonDoFox). 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 und JonDonym 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 Domain[175] o.ä.).
- Irgendwelche anderen Geräte im Haushalt Web-Zugriffe durchführen, für die es gar keine Plugins gibt (z.B. für Spielekonsolen und Fernseher).

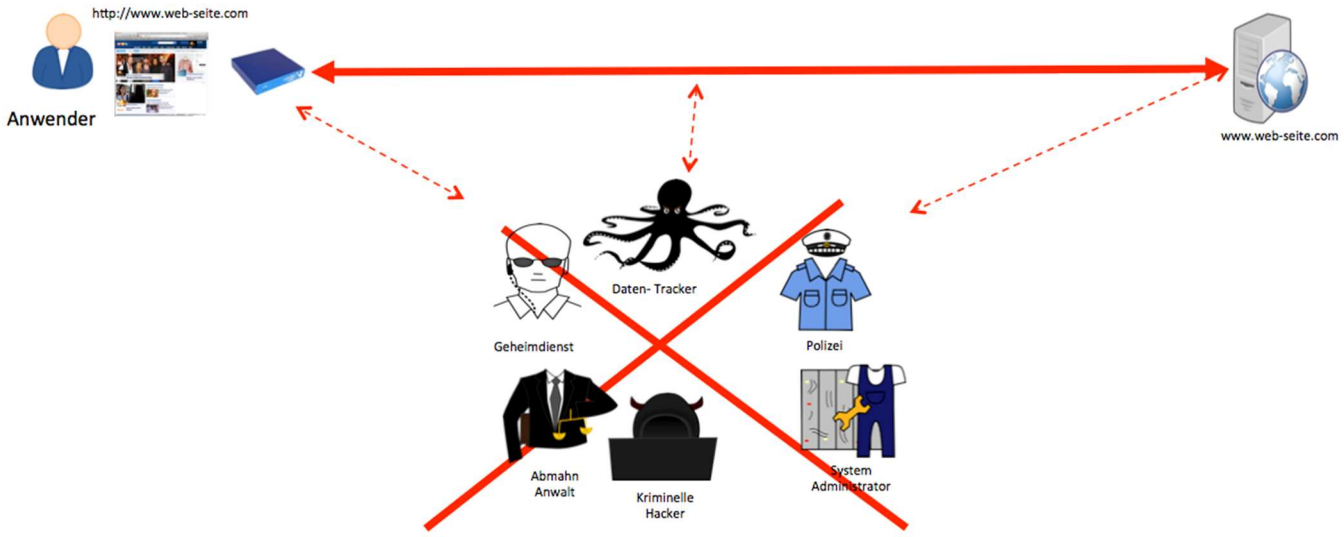
Die TrutzBox® umgeht durch ihre einzigartigen TrutzBrowse Architektur diese Einschränkungen. Mit ihrer Hilfe ist auch jeder Laie in der Lage, sich vor ungewolltem Ausspähen zu schützen. Für einen Daten-Tracker ist es nicht mehr so einfach möglich, diesen Schutz zu umgehen.

Die TrutzBox® Funktionen TrutzBrowse und TrutzContent wurden durch einen intelligenten Proxy (Stellvertreter) implementiert, der an zentraler Stelle (in der TrutzBox®) jeglichen HTTP-Verkehr zwischen dem gesamten Heimnetz und dem Internet überwacht. Dieser Proxy fasst alle Funktionen der gängigen Browser-Plugins zusammen und bietet darüber hinaus vieles mehr. Er stellt sicher, dass

- alle Browser 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 einer auf der TrutzBox® gespeicherten Blacklist verglichen 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.

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



(© 2016 Comidio GmbH)

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[176]. 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.

Derartigen Tracking-Servern 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 zu formatieren. 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

176 http://www.iana.org/assignments/message-headers/message-headers.xhtml
http://de.wikipedia.org/wiki/Liste_der_HTTP-Headerfelder

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.

Spurenloses Surfen im Internet aus Anwendersicht

Dank der TrutzBrowse Technology kann der Sicherheitsgrad einer jeden Webseite mit Hilfe des intelligenten Security-Sliders (Sicherheits-Schiebereglers) jederzeit individuell angepasst werden. 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 der problematischen Funktionen werden von TrutzBrowse gefiltert, und im Gegenzug eventuelle Funktionsstörungen der Seite vermieden.

Die Sicherheitsstufe sollte allerdings nur bei vertrauenswürdigen Webseiten reduziert werden.

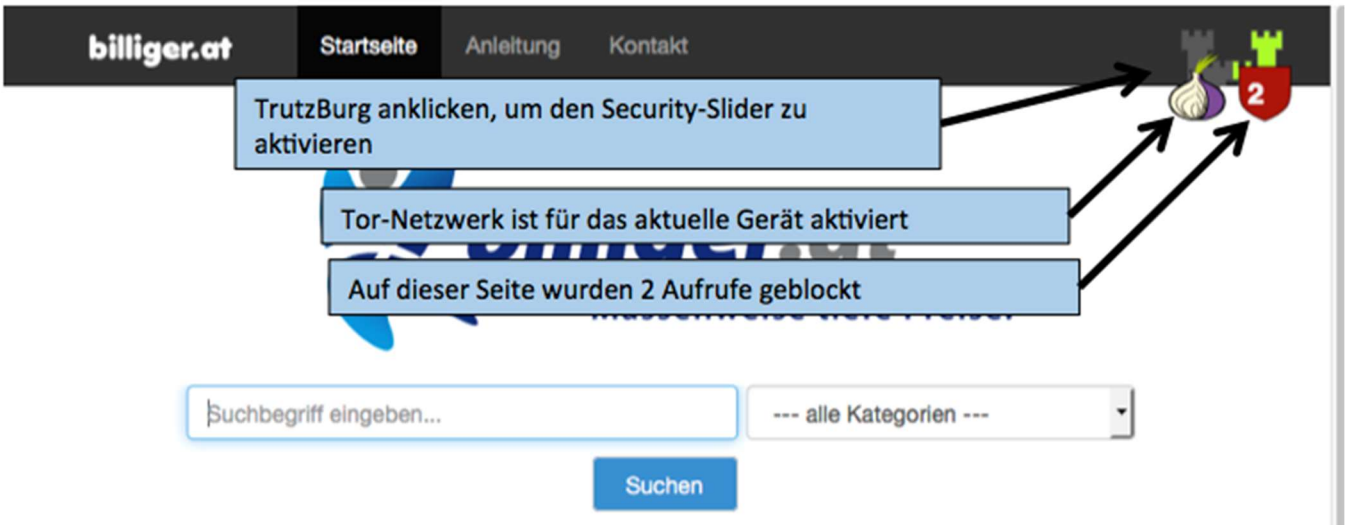
Immer wenn beim Surfen TrutzBrowse verwendet und somit die TrutzBox Anonymitätsfunktionen genutzt wurden, zeigt der Browser oben rechts das TrutzBurg Symbol an. Des Weiteren wird auf dem TrutzBurg Symbol angezeigt, ob Tor aktiv ist (also auch die IP-Adresse anonymisiert wurde) und wie viele Tracker blockiert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

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 1s berühren.

Die Position des TrutzBurg Symbols kann im Browser pro Gerät individuell eingestellt werden. Eine veränderte Position wird pro Seite gespeichert, sodass die TrutzBurg Position nur einmal angepasst werden muss.

Durch das Flag „TrutzBurg Symbol anzeigen“ (im UI unter Filter-Konfigurieren), kann der TrutzBox-Administrator das TrutzBurg Symbol abschalten und die Default-Ausgangsposition der TrutzBurg pro Gerät festlegen.

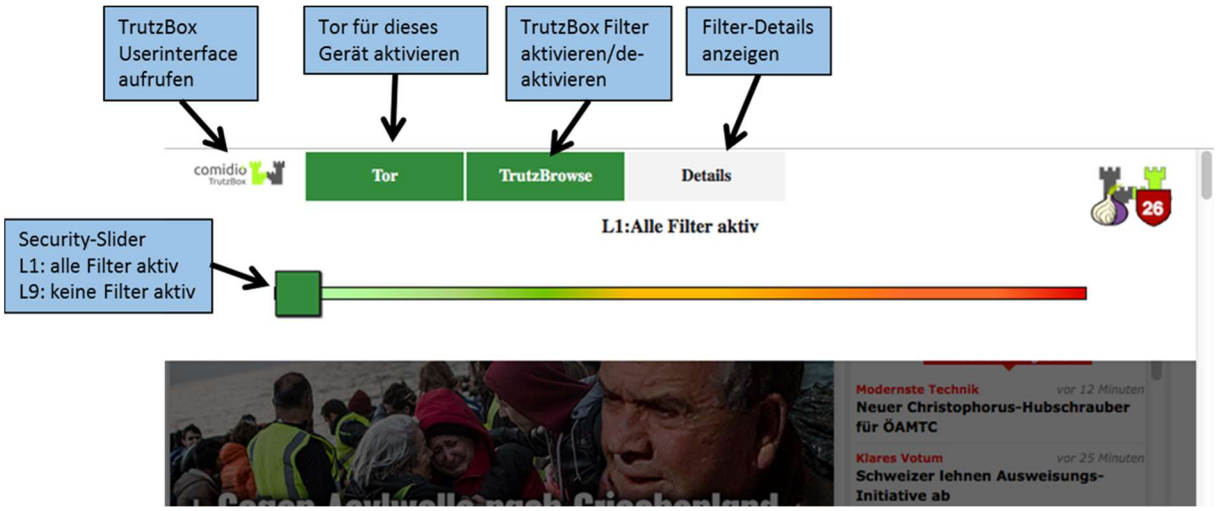
Der Anwender kann durch Anklicken des TrutzBurg Symbols den Security-Slider aktivieren:



(© 2015 Comidio GmbH)

Falls das TrutzBurg Symbol eine Funktion der Webseite überdeckt die somit nicht mehr erreichbar wäre, kann das TrutzBox Symbol hier auf eine andere Ecke der Webseite verschoben werden. So dass die dahinterliegende Funktion wieder bedienbar ist.

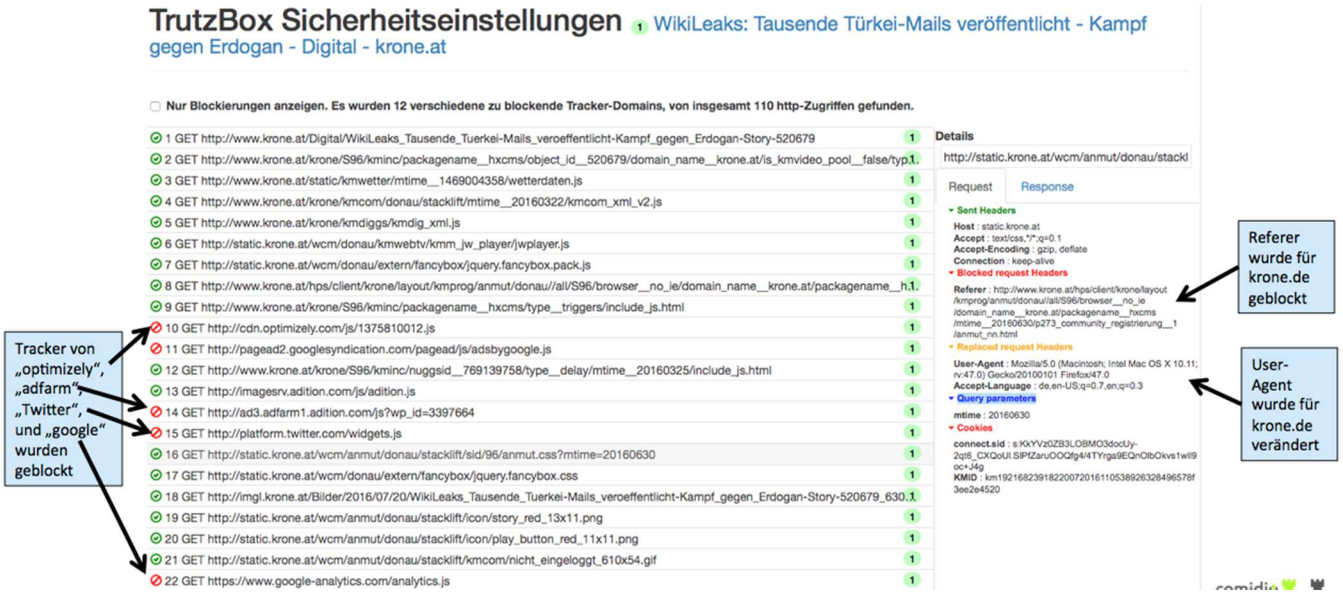
Nach Anklicken der TrutzBurg stehen der Security-Slider und vier weitere Funktionen zur Verfügung:



(© 2015 Comidio GmbH)

Standardmäßig steht der 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, 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.

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):

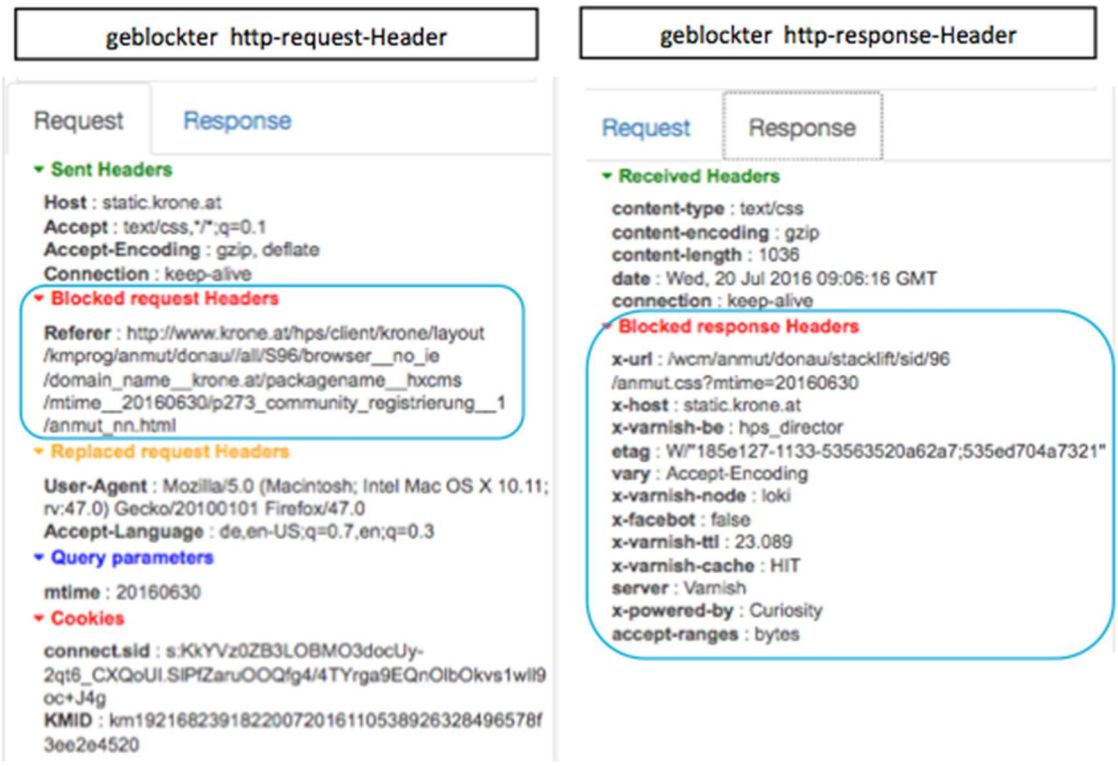


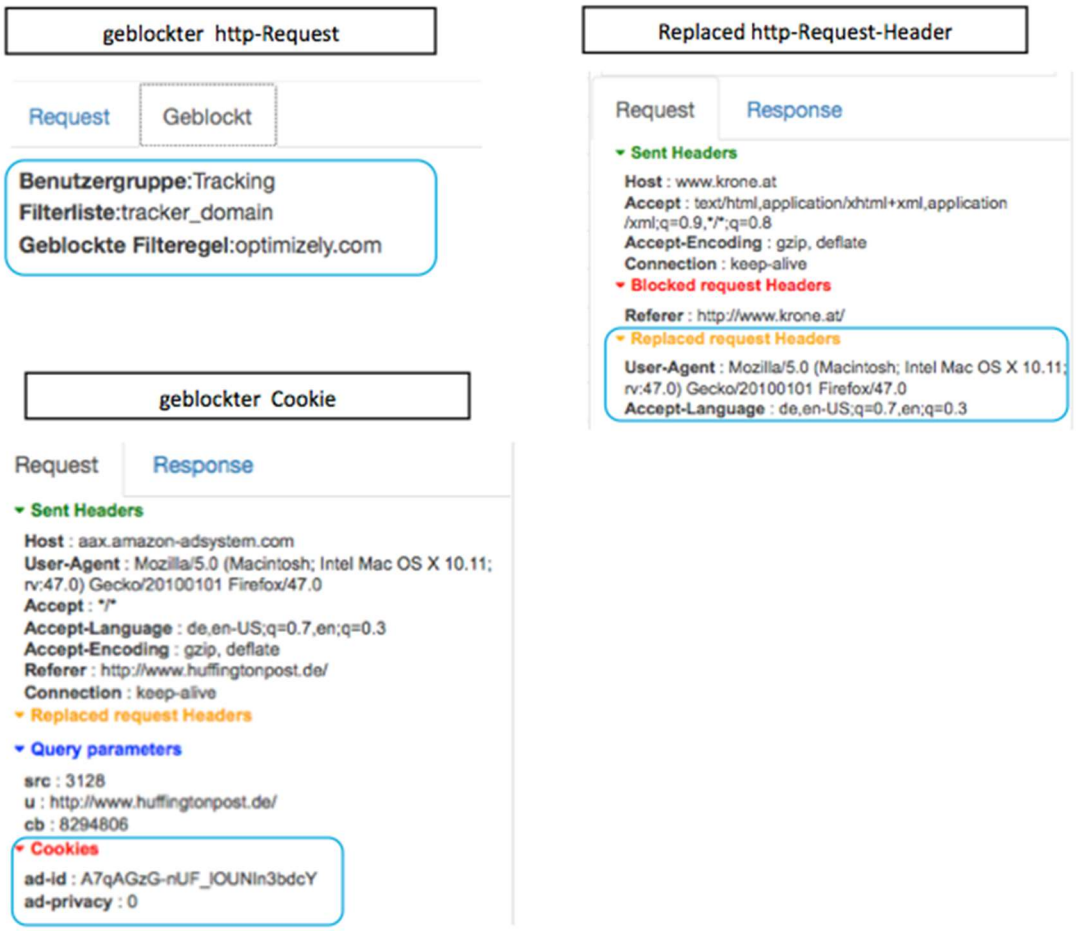
(© 2016 Comidio GmbH)

Geblockte HTTP-Aufrufe sind durch ⊘ gekennzeichnet.

Die Übersicht zeigt auch die HTTP-Header 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 weiteren Zugriff, den diese Webseite automatsch anstößt, werden auf der rechten Seite die bei jedem Aufruf übertragenen „http-Query Parameter“ und „http-header“, über die auch Daten zwischen Browser und Web-Server übertragen werden, angezeigt. Je nachdem, wie die TrutzBox® für die aktuelle Position des Security-Sliders konfiguriert ist, werden bestimmte HTTP-Header-Daten gar nicht (Blocked Headers) oder veränderte (Replaced Headers) an den Web-Server übermittelt:





(© 2016 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 nicht verarbeitet werden.

Veränderte Security-Slider Einstellungen werden für die aktuelle Webseite auf der TrutzBox® für zukünftige Aufrufe gespeichert, sodass beim wiederholten Besuch dieser Webseite der Security-Slider nicht mehr angepasst werden muss.

Spurenloses Surfen im Internet aus Sicht des TrutzBox Administrators

Der TrutzBox® Administrator kann die von Comidio ausgelieferten Default TrutzBrowse Filtereinstellungen für jede der 10 Sicherheitsstufen detailliert anpassen. Experten sind damit in der Lage, ihre Anonymisierung noch individueller zu steuern. Andere Nutzer der TrutzBox® werden dieses Feature weniger nutzen.

TrutzBox® Filter

Die TrutzBox überwacht Web-Zugriffe und ist somit in der Lage, unerwünschten Datenverkehr zu unterbinden. Die TrutzBox unterscheidet dabei, ob ein Gerät oder ein Benutzer eine Webseite direkt aufruft, oder ob ein Web-Server – nach dem Ladevorgang der bewusst aufgerufenen Webseite weitere Webseiten kontaktiert und diese ohne Wissen des Nutzers und ohne dessen Zustimmung lädt.

Die TrutzBox bietet hierfür zwei verschiedene Grundfunktionen an:

1. TrutzContent:

Ein Content-Filter, der verhindert, dass ein Gerät oder ein Nutzer direkt eine bestimmte Webseite aufruft. Beispiele für ungewollte Aufrufe:

- Ein Jugendlicher möchte eine Webseite mit jugendgefährdendem Inhalt laden.
- Ein Internet-Gerät, ruft unbemerkt im Hintergrund eine Webseite auf, ohne dass ein Nutzer das willentlich angestoßen hat, im Hintergrund eine Webseite aufruft. Das können Fernseher, Waschmaschinen oder Spielekonsolen sein (falls sie mit dem Internet verbunden sind), oder sogar der Standard Internet-Browser des Benutzer PCs, der wiederum eigenständig z.B. Mozilla oder Google oder den Server eines Plugin-Anbieters kontaktiert.

Die TrutzBox® prüft, ob der Kontakt zu einem solchen Server zulässig ist und blockt gegebenenfalls die Verbindung zu diesem Server.

2. TrutzBrowse : :

Ein Benutzer oder ein internetfähiges Gerät hat erlaubterweise eine Webseite aufgerufen. Beim Laden der Seite kontaktiert diese Webseite jedoch weitere Web-Server(oftmals kommerzielle Daten-Tracker), die evtl. an den Nutzerdaten interessiert sind. Die TrutzBox überwacht Aufrufe auf andere Web-Server, die während des Ladevorgangs der willentlich aufgerufenen Webseite indirekt ohne Wissen des Nutzers kontaktiert werden.

Um sowohl im Fall 1 (TrutzContent) als auch im Fall 2 (TrutzBrowse) festzustellen, ob eine Seite die gerade kontaktiert wird, „unerwünscht“ ist, gleicht die TrutzBox® jede aufgerufene Webseite mit den ihr bekannten Webseiten (Filterlisten) ab. Comidio liefert ca. 110 Filterlisten, die 55 unterschiedliche Internet-Themengebiete abdecken. Diese Filterlisten werden regelmäßig aktualisiert. Der TrutzBox® Administrator kann bei Bedarf auch eigene Filterlisten hinzufügen.

Vorgehensweise der TrutzBox®:

Wenn ein Internet-Nutzer eine Webseite aufruft, dann prüft die TrutzContent Funktion zunächst, ob der PC und/oder der Nutzer, der diesen Webseitenaufruf angestoßen hat, diese Seite überhaupt aufrufen darf. Soll diese

Webseite gemäß den Filterlisten blockiert werden, dann bekommt der Internet-Nutzer im Browser eine Fehlermeldung angezeigt.

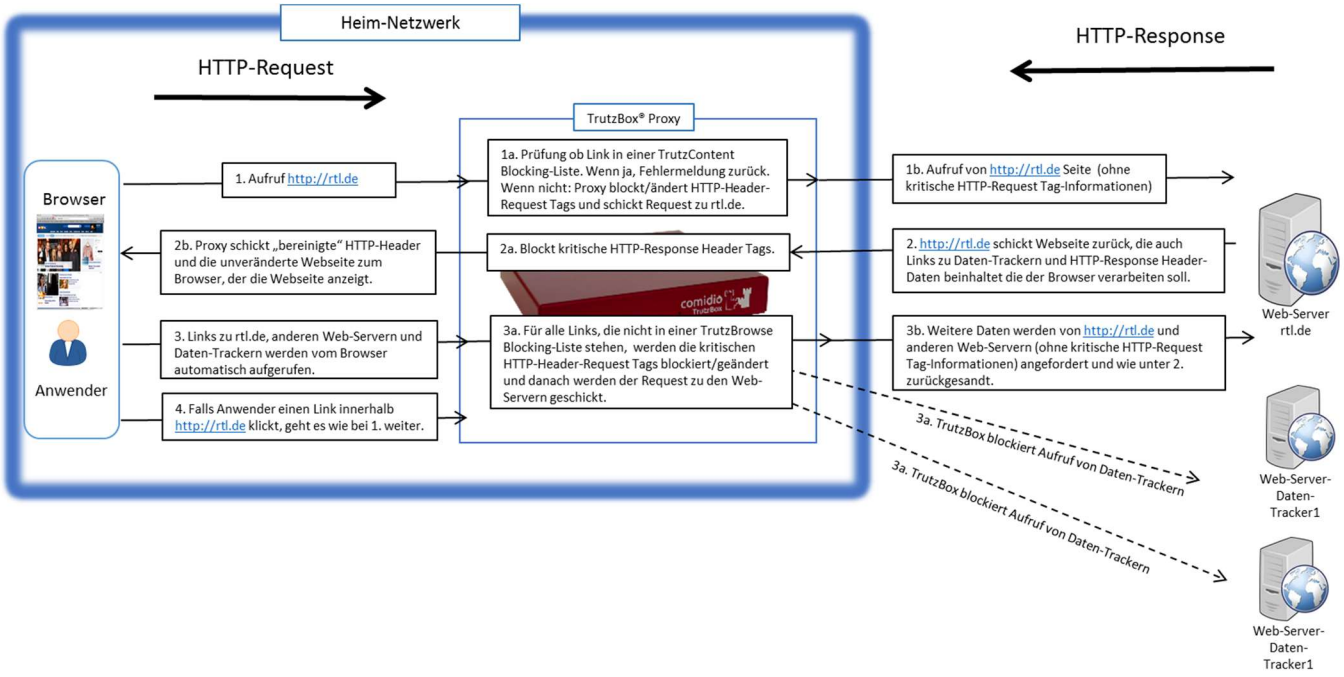
Falls die Webseite aufgerufen werden darf, lässt die TrutzBox® zwar die Daten vom Web-Server zum Browser passieren, aber sie überwacht jeden Aufruf weiterer Web-Server, die die Webseite selbstständig danach kontaktiert. Meist lädt eine Webseite weitere Inhalte von vielen anderen Web-Servern. Bei jedem Kontakt mit einem anderen Web-Server als dem ursprünglich aufgerufenen Web-Server, überprüft die TrutzBox®, ob sich dieser später aufgerufene Web-Server in einer Filterlisten-Gruppe „TrutzBrowse“ befindet. Falls sie dort aufgeführt ist, wird die Verbindung zu diesem Server geblockt.

Somit werden Daten-Tracker-Aufrufe, die in den meisten Webseiten einprogrammiert wurden, unterbunden, und Daten-Tracker können das Nutzerverhalten nicht ausspionieren.

TrutzBrowse HTTP-Header-Filter

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 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.

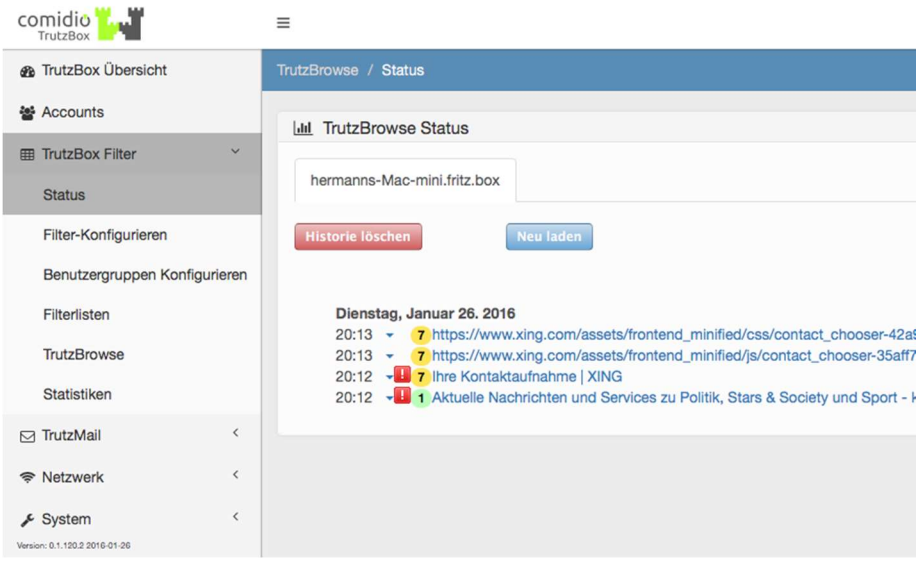
Die TrutzBox® ist mit ihrer TrutzBrowse Funktion somit in der Lage, den gesamten HTTP Datenaustausch im Internet zu kontrollieren und soweit diese HTTP-Header-Daten nicht unbedingt benötigt werden, diese zu blockieren bzw. zu verfälschen.



(© 2015 Comidio GmbH)

Daten-Kommunikation beobachten und Filter anpassen

Die TrutzBox® bietet dem Administrator umfangreiche Funktionen, um die Internet-Kommunikation von Browsern und sonstigen Apps zu kontrollieren. Der Menüpunkt TrutzBox Filter -> Status zeigt die Kommunikation für das Gerät, das gerade verwendet wird. Über weitere Tabs kann hier auch die Kommunikation anderer Geräte abgerufen werden.



Mit Klick auf den angezeigten Link werden wie im Browser des Anwenders, die Aktivitäten des Proxy-Filters, die für diesen Link ausgeführt wurden, angezeigt.

Durch Anklicken des Pfeils neben der Uhrzeit wird ein Menü aktiviert, das es erlaubt, für diesen Link, den Security-Slider-Level zu ändern. Das ist vor allem für nicht-Browser Apps nützlich, die keinen Security-Slider anzeigen können.

Die farblich gekennzeichneten Ziffern zeigen die für diesen Zugriff angewandte Slider-Position, somit den Security-Level.

Die Symbole links neben der Slider-Stellung zeigen den Proxy-Status. bedeutet, dass Tracker gefunden und gestoppt wurden. Das halbe Durchfahrtsverbotsschild wird angezeigt, wenn TrutzContent zugeschlagen hat. Also eine Seite aufgerufen wurde, die durch TrutzContent gesperrt wurde.

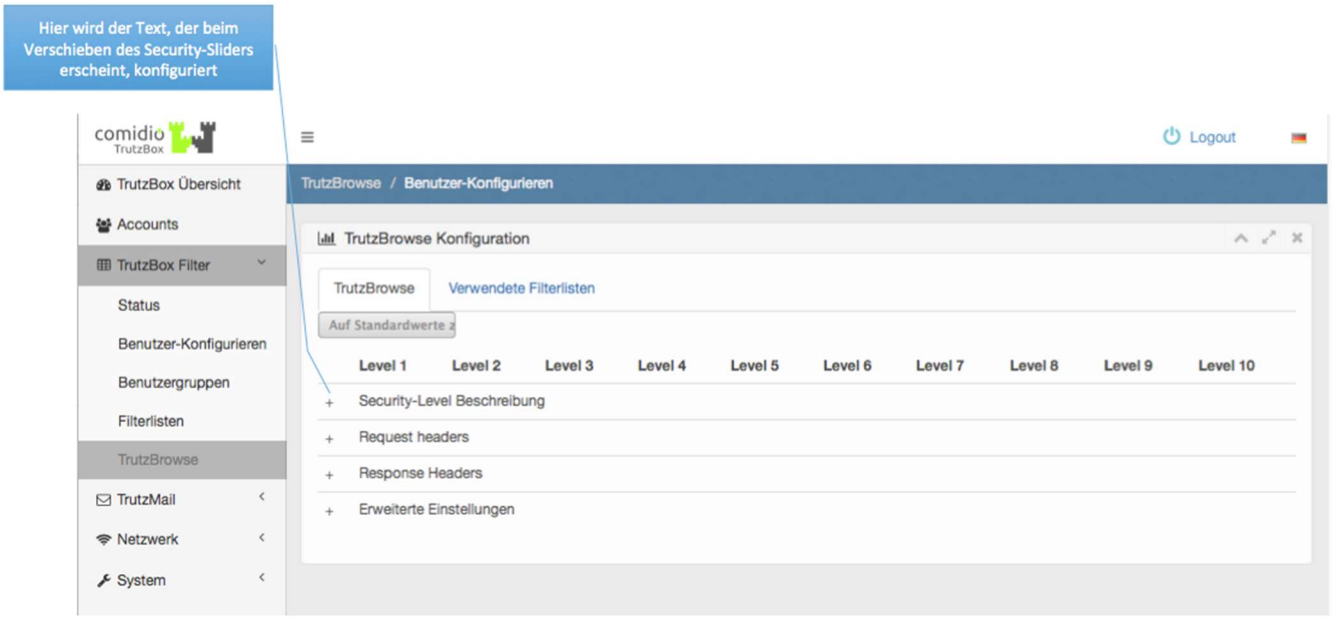
Vor dem http-Zugriff können folgende Stichwörter stehen:

- **SKIP**: bedeutet, dass der SecSlider für diesen Zugriff auf L10 steht und somit keine Filterung stattgefunden hat. Der TrutzBox-Proxy hat diesen Zugriff direkt weitergeleitet.
- **ERROR**: bedeutet, dass ein Client versucht, über den TrutzBox Proxy eine verschlüsselte End-to-End Verbindung zu einem Server aufzubauen, die der Proxy nicht entschlüsseln kann. Solche Verbindungen lässt der TrutzBox-Proxy nicht zu, da Clients damit testen wollen, ob sie „unbeobachtet“ einen Server erreichen können, was dann nicht funktioniert. Normalerweise reagieren die Programme dann auf eine solche Fehlermeldung und bauen eine „saubere“ verschlüsselte Verbindung mit einem zertifizierten Schlüssel auf. Das sollte keinen Einfluss auf die Funktionalität des Programms haben.
- **CONNECT**: mit einem http-CONNECT (https://en.wikipedia.org/wiki/HTTP_tunnel) möchte ein Client einen transparenten Kommunikationstunnel zwischen sich und einem Server aufbauen. Wenn danach aber keine weitere Kommunikation stattfindet, kann es bedeuten, dass der Client keine Kommunikation durch einen Proxy (wie die TrutzBox) durchführen möchte; dieses “Vorhaben” zeigt die TrutzBox an.

TrutzBrowse konfigurieren

Mit der TrutzBox® kann der TrutzBox® Administrator jedes internetfähige Gerät oder einen einzelnen Internet-Nutzer, individuell konfigurieren. Des Weiteren kann unter dem TrutzBox® Filter-Menü (TrutzBox® Filter -> TrutzBrowse) auch die Security-Slider Einstellung für jede Position angepasst werden.

Für jede Position des Security-Sliders können durch „Aufklappen“ des „+“-Symbols, die Beschreibung der Slider-Position, die HTTP-Request und HTTP-Response-Header, Cookies und Domain-Blocker Listen angepasst werden:



(© 2015 Comidio GmbH)

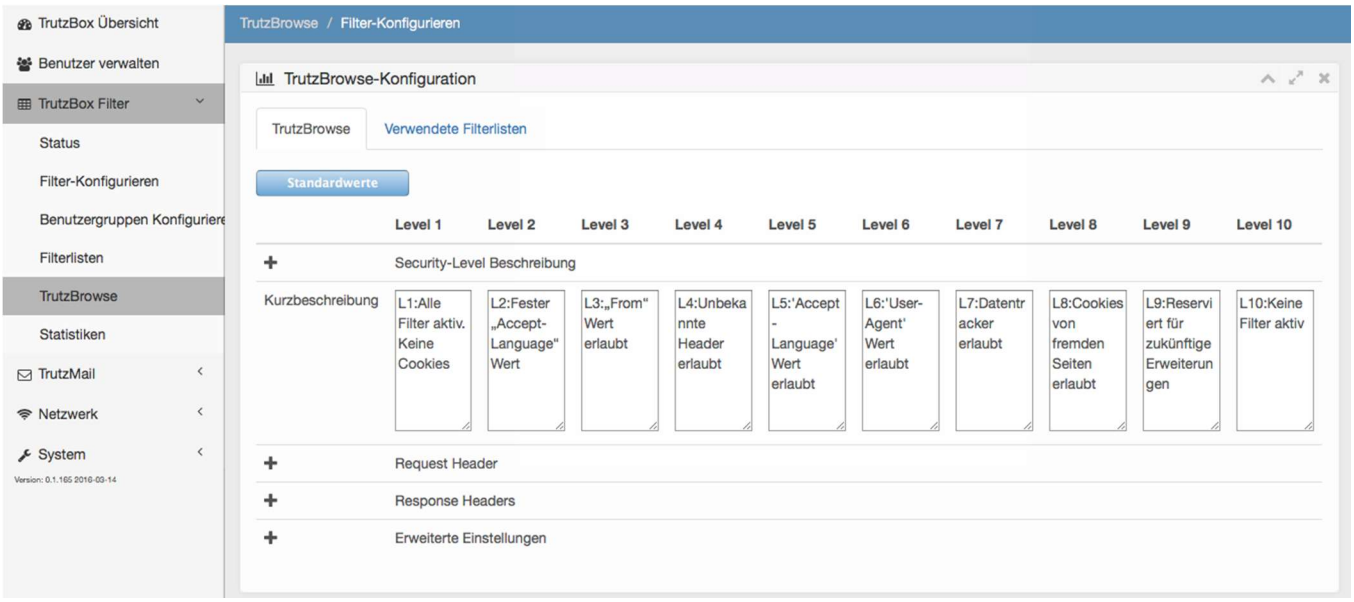
Comidio hat nach vielen Tests eine Standard Konfiguration festgelegt, die allerdings vom Administrator der TrutzBox® flexibel für seine Sicherheitsbedürfnisse verändert werden kann.

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.

Diese Slider-Stellung macht Sinn z.B. bei Apps auf Android oder iOS, da diese i.d.R. gegen ein eigenes Zertifikat prüfen. Wenn der Slider auf L10 gestellt und die Webseite neu geladen wird, dann wird kein TrutzBox® Slider Symbol injiziert, da der Proxy nicht mehr aktiv in die Kommunikation eingreift. Im Menüpunkt TrutzBox® Filter-> TrutzBrowse kann der Administrator diese Security-Slider Beschreibungen für jeden Level anpassen:



Diese Default Einstellung legt fest, welche HTTP-Request und -Response-Header-Daten durchgeleitet oder geblockt werden:

Standardwerte

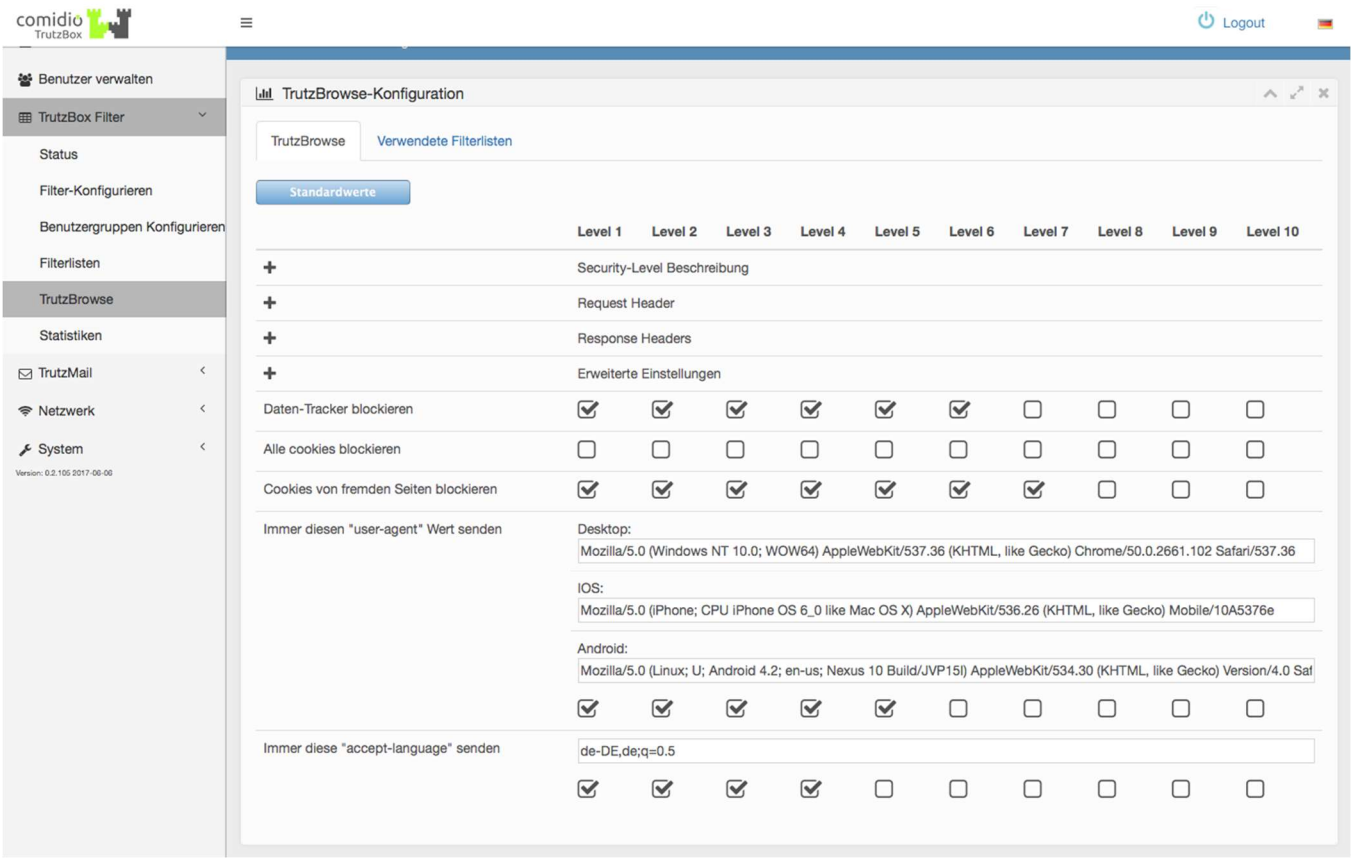
	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7	Level 8	Level 9	Level 10
+	Security-Level Beschreibung									
+	Request Header									
x-requested-with	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
upgrade-insecure-requests	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
access-control-request-method	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
access-control-request-headers	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
content-length	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
origin	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
content-type	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
date	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
host	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
if-modified-since	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
pragma	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
accept	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
accept-charset	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
accept-encoding	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
accept-language	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
connection	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
authorization	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
dnt	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
from	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑
user-agent	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑
Restliche Header erlauben	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑

Standardwerte

	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7	Level 8	Level 9	Level 10
+	Security-Level Beschreibung									
+	Request Header									
+	Response Headers									
allow	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
access-control-allow-origin	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
access-control-allow-credentials	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
access-control-expose-headers	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
access-control-max-age	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
access-control-allow-methods	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
access-control-allow-headers	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
www-authenticate	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
proxy-authenticate	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
cache-control	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
content-encoding	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
content-length	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
content-type	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
date	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
expires	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
last-modified	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
location	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
pragma	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
content-language	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
retry-after	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
title	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
content-disposition	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
connection	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
content-security-policy	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
x-content-type-options	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
x-frame-options	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
strict-transport-security	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
x-webkit-csp	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
x-xss-protection	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
content-security-policy-report-only	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
link	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑
server	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
x-powered-by	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Restliche Header erlauben	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑
+	Erweiterte Einstellungen									

(© 2016 Comidio GmbH)

Zusätzlich können folgende „erweiterten Einstellungen“ auch für jede Security-Slider Stellung vorgenommen werden:



(© 2017 Comidio GmbH)

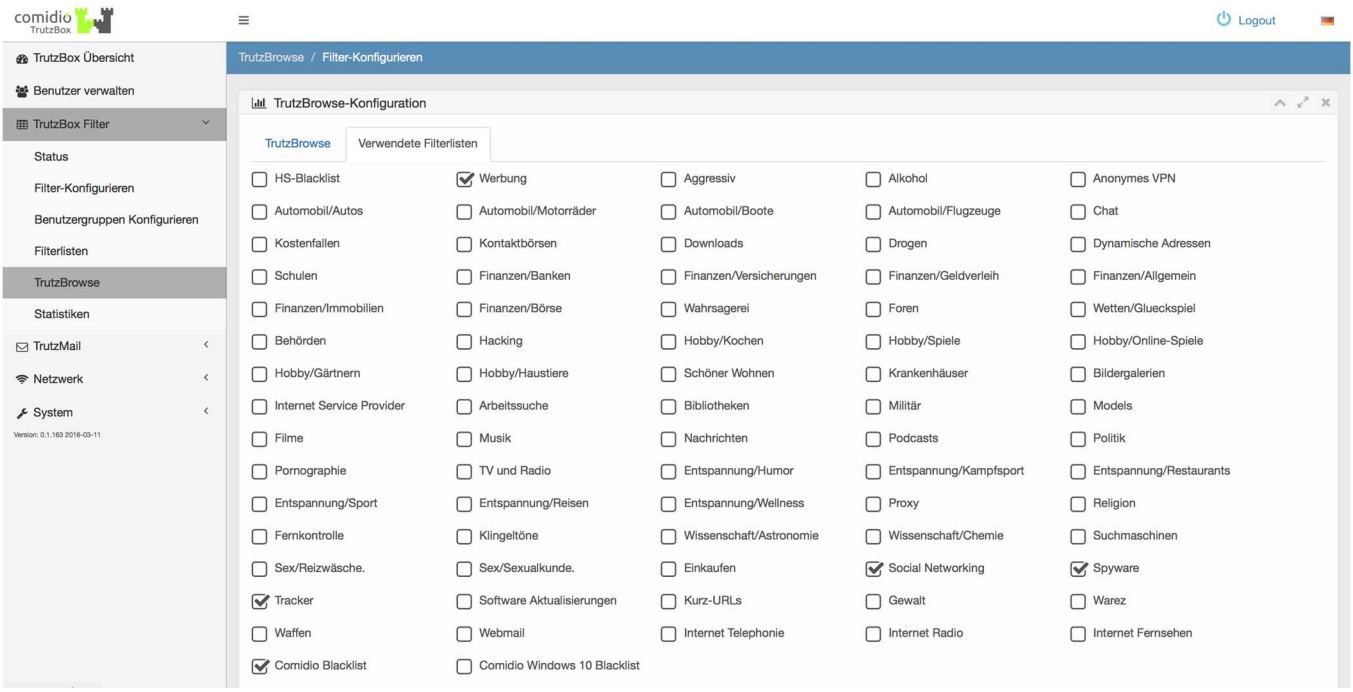
In der Standard-Einstellung sind folgende Einstellungen eingestellt:

- 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 Filterlisten

Unter der Lasche „Verwendete Filterlisten“ werden die Filterlisten aktiviert, die beim Browsen über die TrutzBox® (TrutzBrowse) aktiv sein sollen. Wie man dieser Default Liste entnehmen kann, sind standardmäßig keine

Filterlisten zu Werbefirmen aktiviert. D.h. TrutzBrowse filtert keine Werbung in den angezeigten Webseiten heraus. Dies kann der TrutzBox® Administrator aber an dieser Stelle aktivieren, indem er „Werbung“ aktiviert.



(© 2015 Comidio GmbH)

Die optimale TrutzBrowse Einstellung

Die 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 Block „most-common-user-agents“ findet man dazu gute Anregungen:

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

Weitere Hinweise auf HTTP-Header Anonymisierung sind bei der Beschreibung von Squid[177], JonDo[178] und bei Lutz Donnerhacke[179] zu finden.

Auch die standardmäßig eingestellten TrutzBrowse Filterlisten sind Erfahrungswerte, die einen Kompromiss zwischen möglichst hoher Bedienerfreundlichkeit (möglichst wenig den SecSlider verschieben müssen) und hoher Anonymität im Internet darstellen.

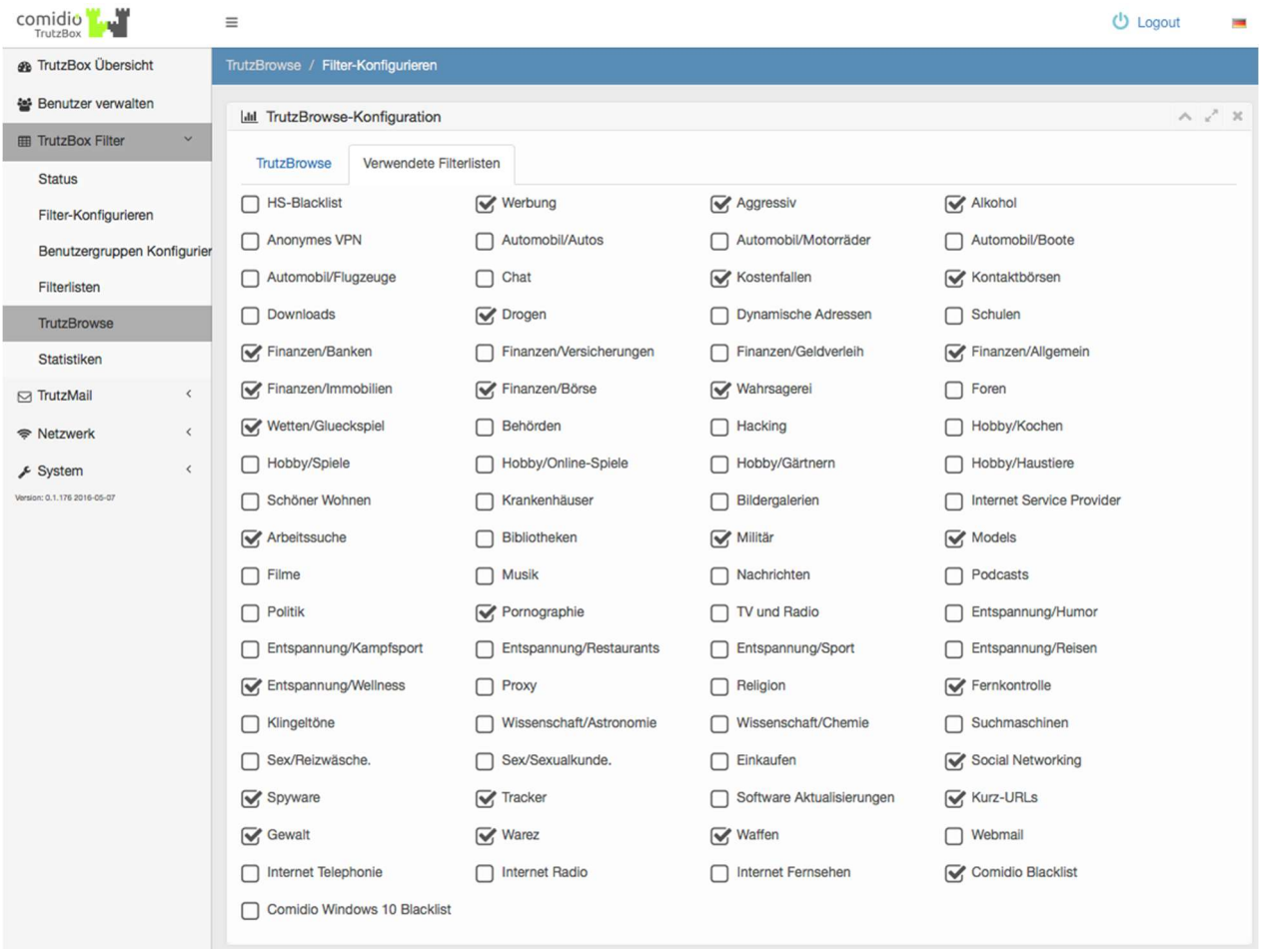
Wer noch mehr Anonymität und Schutz im Internet möchte, der kann zwei weitere Punkte „strenger“ einstellen:

- Cookies auch für aufgerufene Seiten auf L1 Sperren:

und

- und im Tab „verwendete Filterlisten“ weitere Filter aktivieren:

[177] 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
[178] http://ip-check.info/description.php?lang=de
[179] http://altlasten.lutz.donnerhacke.de/mitarb/lutz/anon/web.en.html



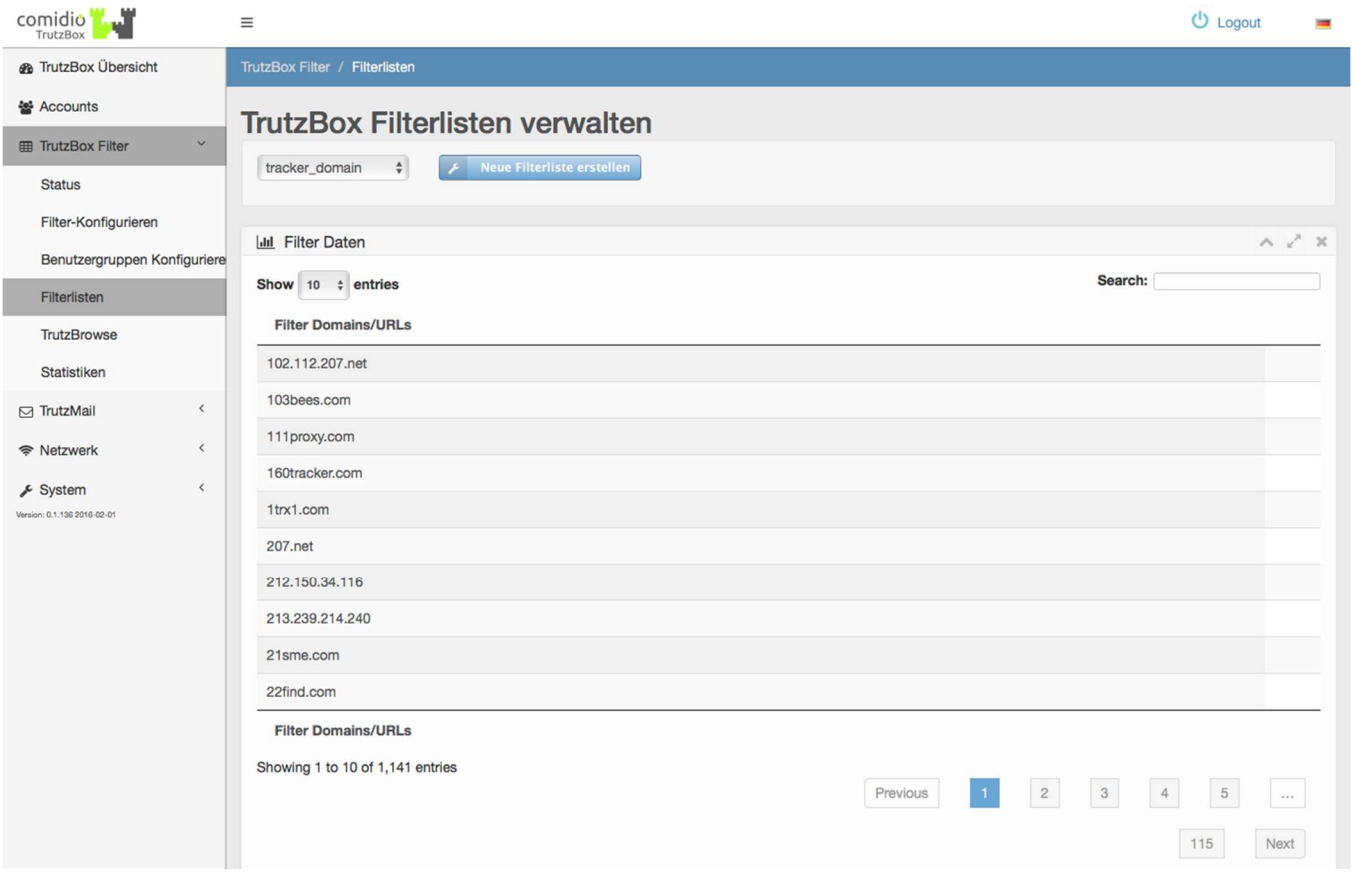
(© 2015 Comidio GmbH)

TrutzBox® Filterlisten

Unter dem Menüpunkt TrutzBox Filter -> 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.

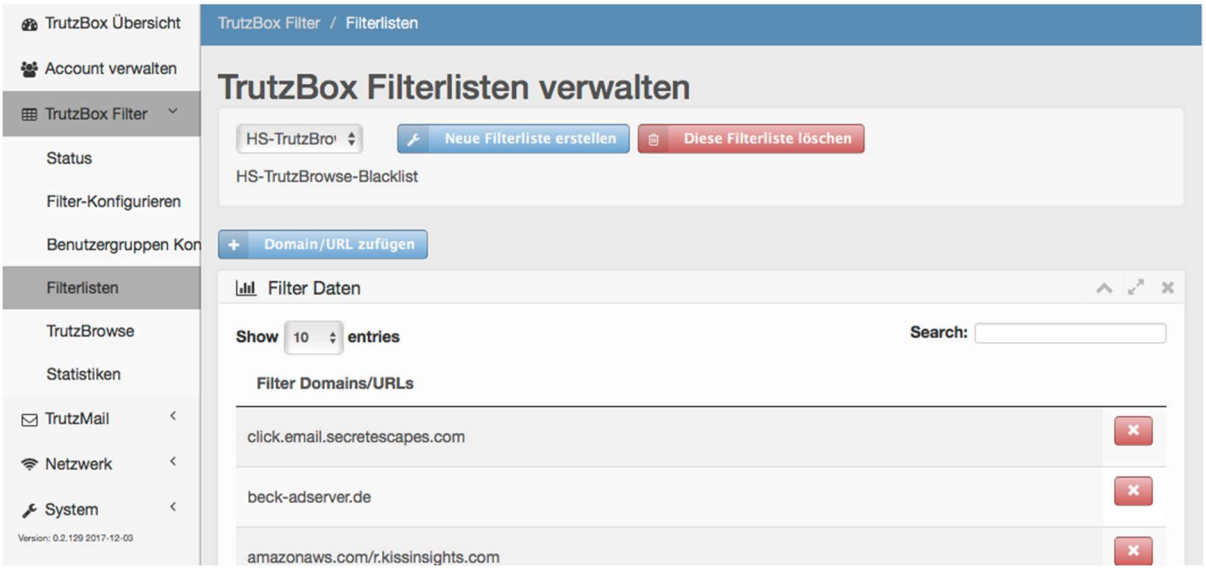
Die von der TrutzBox® verwalteten Filterlisten finden sowohl bei TrutzBrowse als auch bei TrutzContent Verwendung:



(© 2015 Comidio GmbH)

In diesem TrutzBox® Filterlistenmenü 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. Dazu muss eine neu angelegte Black- oder White-Liste allerdings zunächst unter TrutzContent oder TrutzBrowse entsprechend aktiviert werden. Bei einem automatischen Systemupdate durch Comidio werden nur Standard-TrutzBox Black- und White-Listen angepasst, die selbst verwalteten Listen werden dadurch nicht verändert.

Bei selbsterstellten Filterlisten können sowohl Einträge manuell editiert als auch Listen komplett gelöscht 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.

Derzeit werden Änderungen an den eigenen TrutzContent Black- und Whitelists erst nach einem Neustart des Proxy-Servers berücksichtigt. Das ist ein Feature der TrutzBox, das in zukünftigen TrutzBox Releases noch optimiert wird. Sobald Eintrage geändert wurden, muss. die TrutzBox neu gestartet werden (bitte immer nur über das TrutzBox-Userinterface). Es ist auch möglich nur den Proxy neu zu starten, indem in Webmin (erweiterte Einstellungen) unter „System“->“Kommandozeile“ der Befehl "service comidio-trutzbox-node restart“ abgesetzt wird (ohne Hochkomma).

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 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.

Wie in diesem Kapitel beschrieben, bietet die TrutzBox® sehr viele Möglichkeiten, den Datenverkehr zwischen einem Device 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.

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 [180]. 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[181], 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[182], der auch auf dem Firefox Code basiert, tauscht regelmäßig Daten mit seinen Erschaffern aus.

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[183].

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

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

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

[182] https://cliqz.com/

[183] 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

schwierig, hier die optimalen Plugins und die richtigen Einstellungen zu finden. Allerdings gibt es glücklicherweise zwei kostenlose Browser, für die diese Einstellungen bereits optimiert wurden: JonDoFox und den Tor-Browser.

Beide optimierten Browser basieren auf Firefox. Aber beide Browser sind so restriktiv eingestellt, dass ein normales Surfen im Internet sehr schnell zur Spaßbremse wird. Daher wird es im täglichen Betrieb recht schnell notwendig, einige Einstellungen im Browser anzupassen. Während der Tor-Browser auf einer älteren Firefox Version mit einigen Einschränkungen basiert und sich kaum an die eigenen Bedürfnisse anpassen lässt, basiert JonDoFox auf einer aktuellen Firefox Version und lässt sich einfacher an eigene Bedürfnisse anpassen (Details siehe nächstes Kapitel). Leider übernehmen alle Browser, die auf Firefox basieren, auch deren sicherheitskritischen Fehler aus dem Firefox Source-Code[184].

Zur Analyse, was in einem Browser beim Laden und Verarbeiten einer Webseite intern genau vor sich geht, haben alle Browser versteckte Schalter eingebaut. So lässt sich diese Funktion bei Chrome mit Eingabe der URL: chrome://net-internals/ freischalten.

Den sicheren JonDoFox Browser zusammen mit der TrutzBox nutzen

Den sichersten Browser, den man auch im Zusammenspiel mit der TrutzBox nutzen kann, ist JonDoFox der Firma JonDoNym[185]. Dieser kann für alle gängigen Plattformen unter https://www.anonym-surfen.de/jondofox.html kostenlos heruntergeladen und installiert werden. Nachdem in JonDoFox der TrutzBox Proxy konfiguriert und das TrutzBox Zertifikat geladen wurde, kann man über die TrutzBox surfen.

Aber der Browser ist sehr restriktiv und bei den meisten Seiten wird man mit den Standard-Einstellungen Probleme bekommen. Da der Browser standardmäßig JavaScript sperrt, die TrutzBox allerdings Javascript benötigt um die TrutzBurg einzublenden, muss man, falls man die TrutzBurg sehen möchte, zunächst Javascript für die Domain „trutzbox“ erlauben. Des Weiteren benötigt das TrutzBox-UI dann auch einen Cookie und lädt spezielle Schriften von der TrutzBox. Das muss im Browser für die TrutzBox auch noch erlaubt werden.

Die Firma JonDos hat mittlerweile entschieden, ihren JonDoFox-Browser nicht weiter zu entwickeln. Statt dessen haben sie den Tor-Browser für ihre Bedürfnisse angepasst. Diese neue „JonDoBrowser“ kann man derzeit unter https://jondobrowser.jondos.de/ herunterladen (Sourcen: https://github.com/jondos). Bevor man das TrutzBox-Zertifikat importieren kann, müssen mit about:config zwei Einstellungen geändert werden:

- security.nocertdb true -> false

[184] 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

[185] https://www.anonym-surfen.de/

- security.pki.sha1_enforcement_level 2 -> 0

TrutzContent – nicht nur Kinder- bzw. Jugendschutz

Der Administrator ist in der Lage, für angeschlossene Geräte oder einzelne Nutzer den Browser-Zugriff auf bestimmte Web-Inhalte zu blockieren. Damit können Eltern ungeeignete Inhalte für Kinder oder Jugendliche sperren. Mit der Funktion TrutzContent ist es auch möglich, den Zugriff auf unerwünschte Web-Adressen (Domains oder URLs) von Smart Devices, die selbst keinen Internet-Browser haben (Haushaltsgeräte, Uhren, Fitness-Armbänder...), zu sperren.

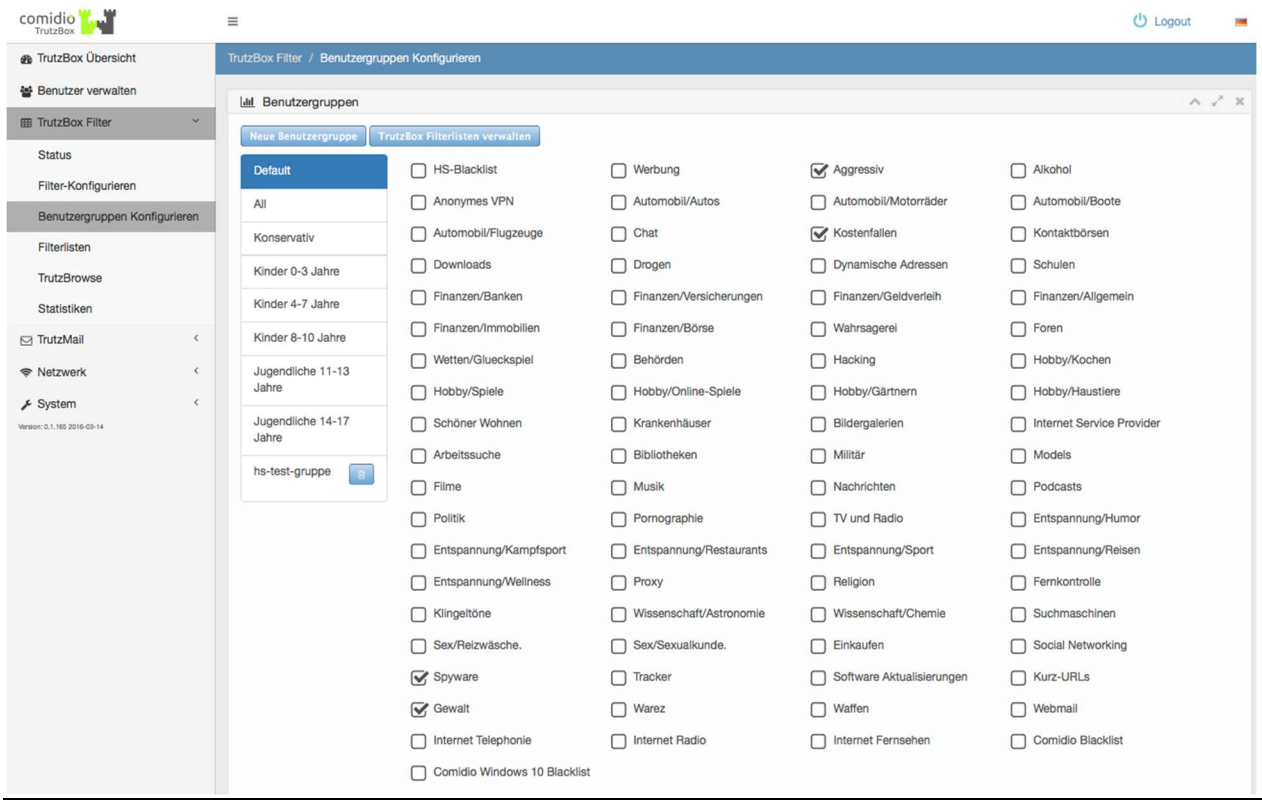
Im Menü TrutzBox Filter -> Benutzer-Konfigurieren können für ein Gerät, für einen Benutzer oder auch für eine Webseite Zugriffs-Einschränkungen konfiguriert werden.

Geräte oder Benutzer im Zugriff auf das Internet einschränken

Der Administrator kann für jedes einzelne, an der TrutzBox® angeschlossene Gerät im Haushalt (auch beispielsweise einen Fernseher) speziell konfigurierte Blocking-Listen (Benutzergruppe) zuweisen. Comidio stellt dazu eine vordefinierte Liste von Benutzergruppen zur Verfügung.

TrutzContent Benutzergruppen konfigurieren

Die TrutzBox® stellt über den Menüpunkt „TrutzBox Filter“ -> „Benutzergruppen konfigurieren“ eine Funktion zur Verfügung, einzelne TrutzContent Domain-Filterlisten in „Benutzergruppen“ zusammenzufassen und neue eigene Benutzergruppen zu definieren:



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 „Status“ sehen. Noch mehr solcher ungewollter Kommunikation kann man beobachten, wenn man das entsprechende Gerät an das sichere Netzwerk der TrutzBox anschließt (Transparent-Mode). Erst dann ist die TrutzBox in der Lage, die komplette Kommunikation eines Geräts zu kontrollieren, in „Status“ anzuzeigen und ggf. zu unterbinden.

Solche Kommunikation, die die TrutzBox im Menüpunkt „Status“ anzeigt, kann durch TrutzContent Filterlisten verhindert werden. Standardmässig sind hierzu allen Geräten schon die Filterlisten der Gruppe „Default“ zugeordnet. Um weitere Sperren solcher ungewollten Zugriffe einzurichten, solle man unter „Filterlisten“ sich zusätzlich eine eigene neue Blacklist, z.B. mit dem Namen „TrutzContent-Blacklist“ anlegen und im Menüpunkt „Benutzergruppen konfigurieren“ die Gruppe Default um diese Liste erweitern, indem man dort diese neue Liste aktiviert.

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

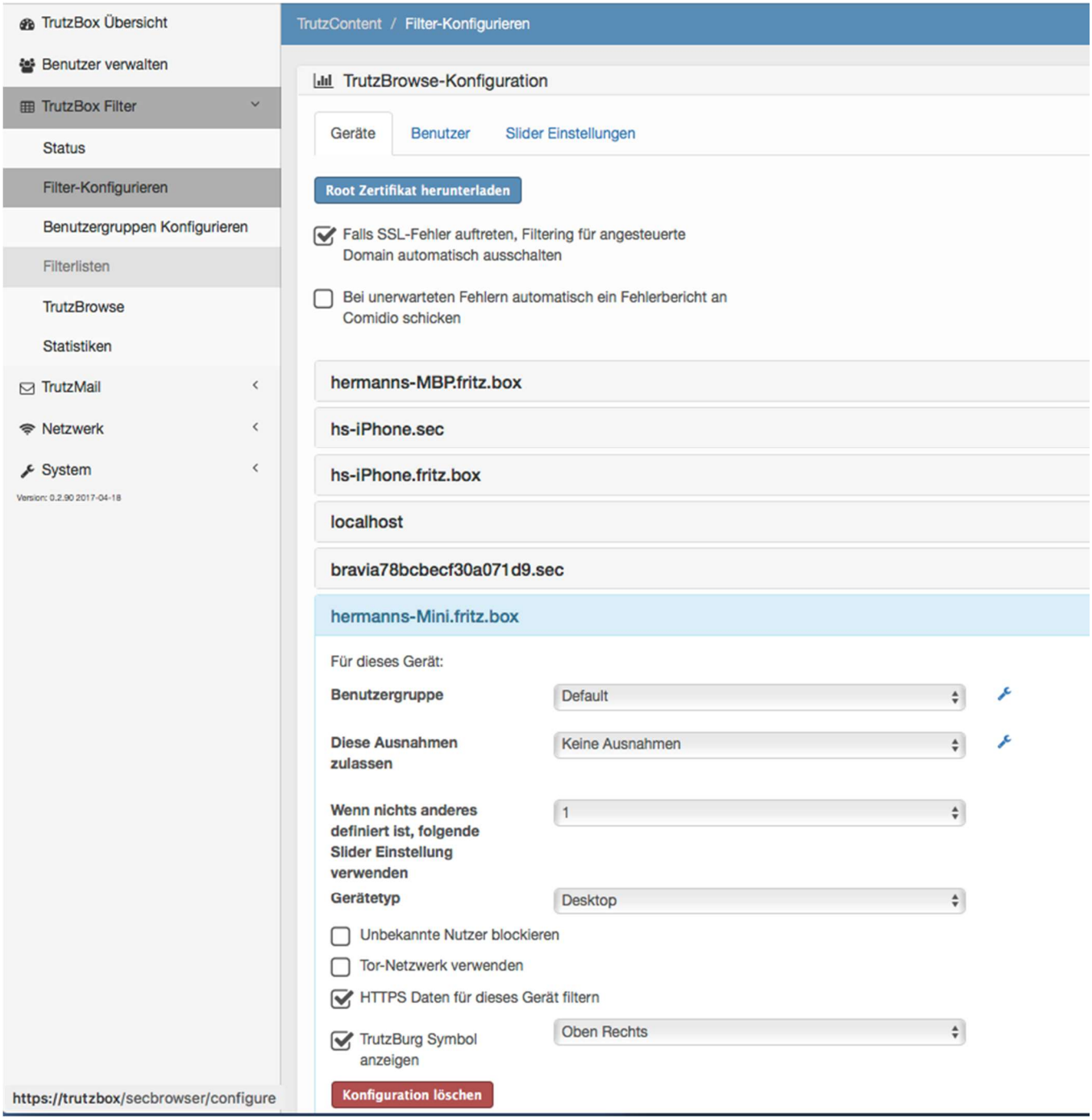
safebrowsing.googleapis.com

getpocket.cdn.mozilla.net

img-getpocket.cdn.mozilla.net

Zugriffsfilter für Geräte Konfigurieren

Im Menüpunkt „Filter-Konfigurieren“ -> „Geräte“ werden alle Geräte aufgelistet, die sich zuvor mit dem TrutzBox Proxy verbunden hatten. Der Name des Devices entspricht dem Host-Namen des Gerätes an dem der Top-Level Domain-Namen des Routers angehängt wurde. Hier im Beispiel bedeutet „.fritz.box“, dass das Gerät am Internet-Router (hier an der FRITZ!Box) angeschlossen ist/war und „.sec“ bedeutet, dass das Gerät an der TrutzBox angeschlossen ist/war:



Falls ein Zugriff über die Fernverbindung (VPN) stattgefunden hat, wird das Gerät hier zwar auch aufgezeigt, aber aus technischen Gründen kann in diesem Fall oft kein Host-Name ermittelt werden.

Hier ist es möglich, das Gerät einer Benutzergruppe zuzuordnen und damit die Zugriffsbeschränkung der Benutzergruppe zuzuordnen. Über das Feld „Diese Ausnahmen zulassen“ ist auch möglich, dem Gerät eine „Whitelist“ zuzuweisen, also eine Liste erlaubter Domains. Mit einer solchen Whitelist ist es möglich, Standard-Blockierungen, die von Comidio vorgegeben werden, aufzuheben. Eine Whitelist muss zuvor in „Filterlisten“ als Whitelist angelegt sein und kann dann hier direkt unter „Diese Ausnahmen zulassen“ für ein Gerät aktiviert werden.

Aber auch jede zusätzliche Blocking-Liste muss zuvor in „Filterlisten“ angelegt werden und einer eigenen Benutzergruppe zugeordnet sein.

Wenn nichts anderes definiert ist, folgende Slider Einstellung verwenden

Die Einstellung "Wenn nichts anderes definiert ist, folgende Slider Einstellung verwenden" biete 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.

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, welche Webseite er liefern soll. Der tatsächlich gesendete „user-agend“ Wert kann unter „TrutzBrowse“->“immer dieser user-agend Wert senden“ angepasst werden.

Tor-Netzwerk verwenden

Mit dem Schalter „Tor Netzwerk verwenden“ kann die Pseudonymisierung der IP-Adresse aktiviert werden, indem dieses Gerät bei TrutzBrowse das Tor-Netzwerk[186] verwendet. Allerdings ist hierbei zu beachten, dass die Internet-Nutzung langsamer sein kann und manche Web-Server bei der Benutzung von Tor zusätzliche Probleme

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

bereiten können. Es gilt allerdings zu beachten, dass die IP-Adresse trotz aktiviertem Tor-Netzwerk vom Server ermittelt werden kann. Siehe hierzu das Kapitel über Tor.

Wenn das Tor-Netzwerk aktiviert ist, kann das Gerät bzw. der entsprechende Benutzer auch mit seinem Browser Tor-Hidden-Services mit „.onion“-Adressen aufrufen. Alle sonstigen TrutzBrowse Funktionen sind weiterhin zusätzlich aktiv.

Verschlüsselte Applikation (SSL)-Verbindungen

Mit dem Schalter „Falls SSL-Fehler auftreten, Filtering für angesteuerte Domain automatisch ausschalten” ist es möglich, für Anwendungen, die eine verschlüsselte Verbindung zu ihrem Server aufbauen möchten, für diesen Server automatisch einen Slider-Eintrag auf L10 (Umgehung des Proxys) zu setzen. Siehe auch Kapitel “Spezielle Security-Slider Einstellungen”.

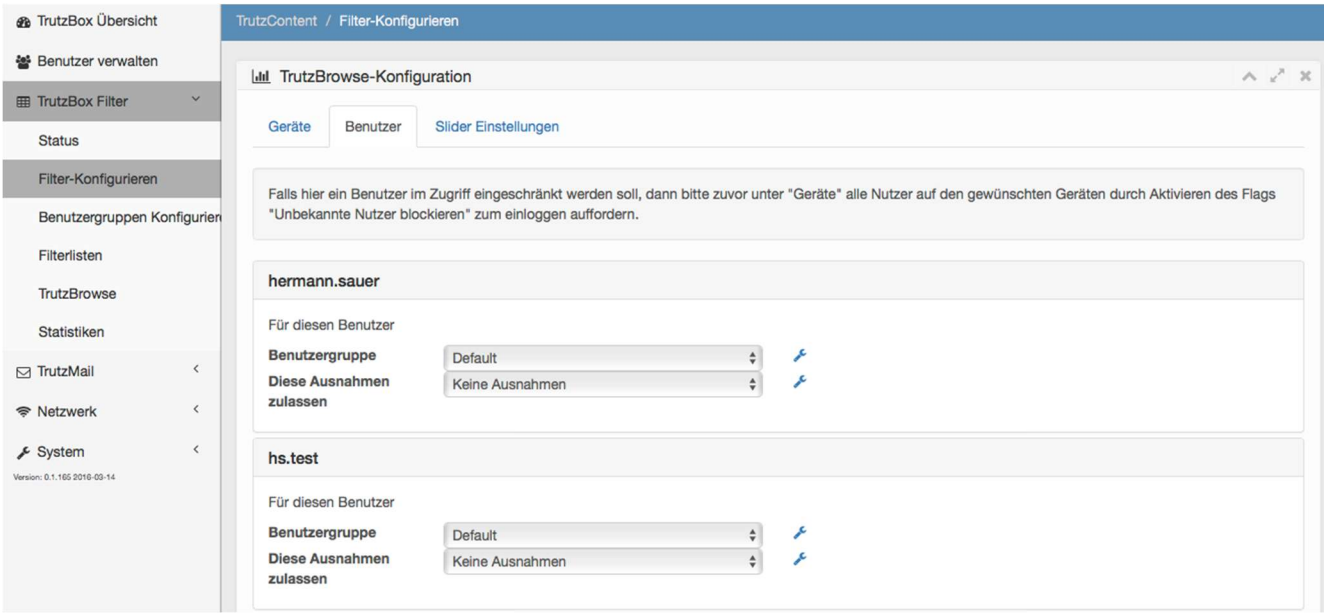
TrutzBox Symbol im Browser (TrutzBurg) abschalten und Standard-Position festlegen

Für jedes angeschlossene Gerät ist es möglich, die Anzeige der TrutzBurg abzuschalten. Das ist dort sinnvoll, wo 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 im Menü "Filter-Konfigurieren" für das gewünschte Gerät das Flag "TrutzBurg Symbol anzeigen" deaktivieren. Die 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, ist das Symbol immer oben rechts im Browser-Fenster angeordnet.

Zugriffsbeschränkungen für Benutzer: Jugendschutz

Des Weiteren kann hier auch für jedes Gerät festgelegt werden, ob sich ein Nutzer zunächst einloggen muss („Unbekannte Nutzer blockieren”). Damit wird vor einem Zugriff aufs Internet auf diesem Gerät eine Login-Maske angezeigt, mit dem sich ein Benutzer zunächst mit seinen TrutzBox® Account-Daten (Name und Passwort) einloggen muss. Da dann TrutzContent weiß, wer hier gerade ins Internet geht, ist es möglich, für einzelne Personen eine benutzerspezifische Blocking-Liste und auch eine White-Liste unter der Lasche „Benutzer“ anzulegen.



(© 2015 Comidio GmbH)

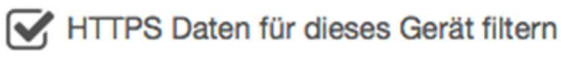
Somit können für Kinder und Jugendliche altersgerechte Zugriffsrechte für jede einzelne Person und/oder benutztes Gerät festgelegt werden. Ebenso sind für „Smart Home“ Geräte besondere Zugriffsrechte einstellbar.

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.

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 Zertifikat sicher, dass die Verbindung legitim und damit sicher ist.

Falls man nicht möchte, dass die TrutzBox auch SSL-Verbindungen kontrolliert, kann mit dem Flag „HTTPS Daten für dieses Gerät filtern„ für jedes an der TrutzBox angeschlossene Gerät diese Funktion abschalten:

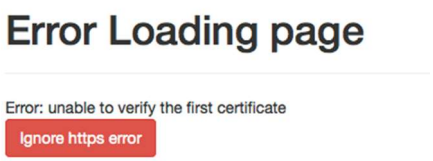


(© 2017 Comidio GmbH)

Wenn dieser Haken nicht gesetzt ist, kontrolliert die TrutzBox keine SSL-Verbindungen. Unverschlüsselte http-Verbindungen werden weiter kontrolliert.

Gegenüber dem Server verhält sich die TrutzBox® wie ein Browser und akzeptiert alle ihr bekannten Zertifikate. Die Liste der 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 Basis- (Root) -Zertifikate, die der Firefox Browser standardmäßig akzeptiert, geladen. Dadurch werden sie auch von der TrutzBox® akzeptiert. Die Liste dieser Stamm-Zertifikate wird von der TrutzBox von /usr/share/ca-certificates/Mozilla regelmässig übernommen.

Falls die TrutzBox ein Server-Zertifikat nicht als vertrauenswürdig erkennt, wird der Anwender gefragt, ob er trotzdem diese Seite laden möchte.



(© 2015 Comidio GmbH)

Die TrutzBox® hat selbst ein Root-Zertifikat (Stamm-Zertifikat), das über die TrutzBox® Bedienoberfläche heruntergeladen werden kann und sowohl in den Browser als auch in den E-Mail-Client importiert werden sollte. Damit wird verhindert, dass der Browser und auch der 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 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 jedes Programm importiert und bestätigt werden.

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.

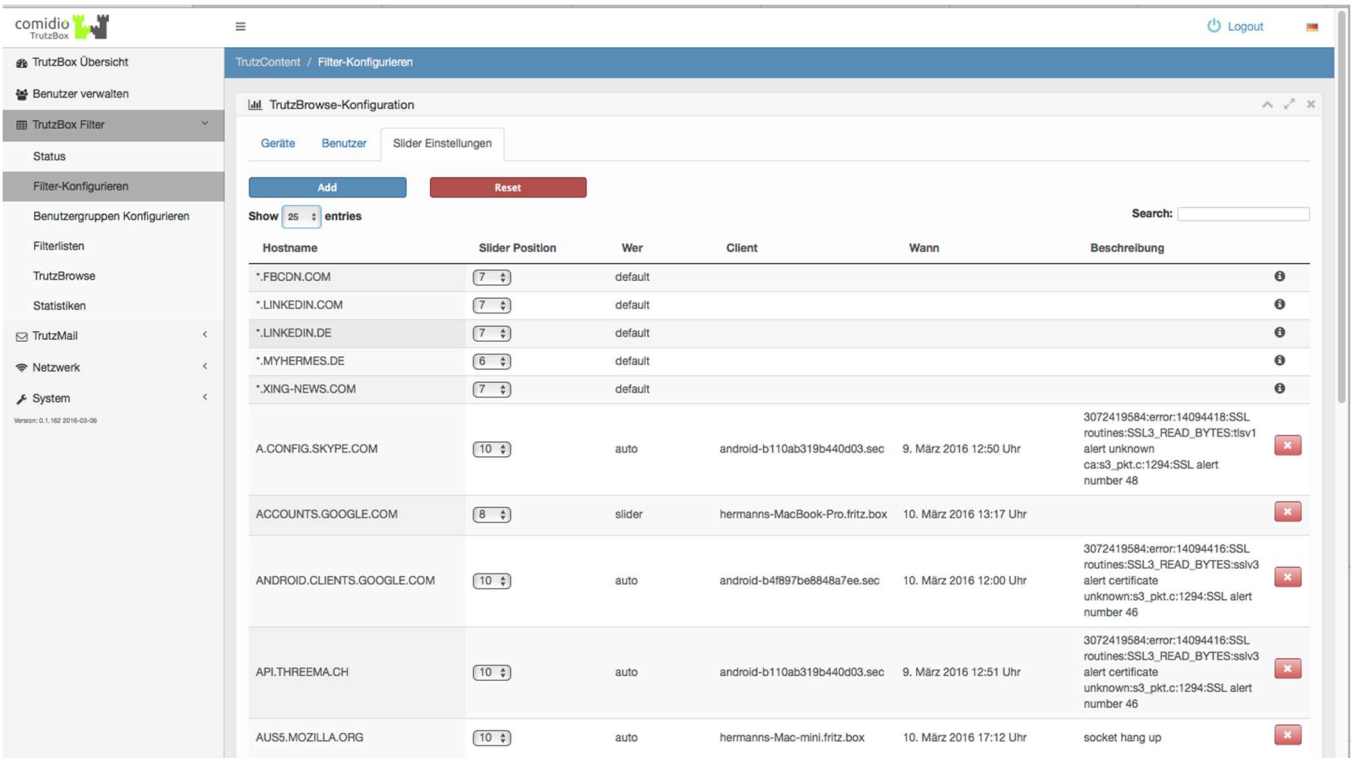
Wenn man in Chrome den Befehl: chrome://net-internals/#proxy absetzt, dann kann man sehen, ob der Proxy aktiv ist. Wenn der Proxy aus irgendeinem Grund nicht funktioniert, schaltet chrome auf direct-mode um (anders als in firefox).

Spezielle Security-Slider Einstellungen

Neben dem Browser und dem Mail-Client, nutzen auch andere Anwendungen (App) oft ein Zertifikat, um den Server zu authentisieren. Allerdings ist dazu normalerweise das erwartete Server-Zertifikat fest in die App einprogrammiert und lässt sich somit vom Anwender nicht kontrollieren. Da solche Apps trotzdem oft über Port 443 und damit im Transparent-Mode über den TrutzBox® Proxy kommunizieren, funktioniert die Kommunikation dieser Apps mit seinem Server nicht.

Solche Verbindungen werden unter dem Menüpunkt „Status“ mit einer entsprechenden Fehlermeldung angezeigt und müssen um den Proxy der TrutzBox® geleitet werden, indem eine Ausnahmeregel auf der TrutzBox® konfiguriert wird. Eine solche Ausnahmeregelung kann im Menüpunkt noch unter „Status“ im Menü „Slider Einstellungen ändern“ eingerichtet werden.

Alle gesetzten Slider-Einstellungen für einzelne URLs (Server) werden auf der TrutzBox gespeichert und können unter dem Menüpunkt „Slider Einstellungen“ auch manuell verwaltet werden.



Comidio liefert für einige oft genutzte Web-Server Standard Slider-Stellungen aus, die mit dem Symbol gekennzeichnet sind. Diese können zwar nicht gelöscht werden, aber der TrutzBox® Administrator kann den von Comidio vorgegebenen Security-Level auf seine Bedürfnisse anpassen. So ist es z.B. möglich, die Slider-Position einer solchen Default-Einstellung auf L1 zu stellen.

Die Gründe für diese Standard-SecSlider Einstellungen sind unterschiedlich:

z.B.

- apple und iCloud sind notwendig, damit die Standard-Anwendungen auf Apple-Rechner und iPhone noch Daten mit Apple-Servern austauschen können

Die Freischaltung der Domains

- facebook und fbcdn (Facebook)

- licdn und linkedin (Linkedin)

sind notwendig, damit man sich auf deren Servern einloggen kann. Nur den SecSlider von z.B. facebook.de auf L9 zu schieben genügt nicht um sich erfolgreich auf Facebook einzuloggen. facebook.de verzweigt auf facebook.com und fbcdn.com und ohne diese Freischaltung blockiert die TrutzBox den Cookie von facebook.de. Und da die TrutzBox standardmäßig auf L1 Third-Party-Cookies verbietet, würden facebook.com und fbcdn.com nicht auf den Session-Cookie von facebook.de zugreifen können und ständig nach einem Login fragen.

Wichtig ist noch zu verstehen, dass diese Standard-Einstellung nur für TrutzContent aktiv sind und somit keinen Einfluss auf TrutzBrowse haben. Wenn man eine Web-Seite aufruft, die einen Tracker von z.B. Facebook aufruft, dann wird dieser Facebook-Aufruf trotzdem gesperrt. Diese Tracker-Blockierung funktioniert bei anderen Seiten, die auf L1 stehen, trotz der Standard-Freischaltung dieser Server, da in TrutzBrowse immer die SecSlider Einstellung der aufgerufenen Seite „vererbt“ wird.

Durch Add können eigene neue Slider-Stellungen für Hosts eingetragen und mit auch wieder gelöscht werden.

Durch einen „*“ im Hostnamen können alle URLs, die mit dem Namen rechts neben dem „*“ enden, angesprochen werden. Falls der Proxy eine URL findet, die in dieser Liste mehrmals eingetragen ist, wird der Security-Level des längsten passenden Eintrags verwendet.

Wenn die Option „Falls SSL-Fehler auftreten, Filtering für angesteuerte Domain automatisch ausschalten” im Menü “Filter-Konfigurieren” aktiviert ist, trägt hier der TrutzBox® Proxy automatisch eine Freischaltung (L10) von Servern ein, die beim Verbindungsaufbau mit dem Server einen Verbindungsfehler verursacht haben.

Es gibt somit vier Möglichkeiten, wie ein Security-Slider Eintrag in diese zentrale Datenbank erfolgen kann. Alle Benutzer und Geräte nutzen diese Datenbank.

Die Liste der „Slider Einstellungen“ zeigt unter der Rubrik „wer“ an, wer oder was die Ursache für die Slider-Anpassung war. Es werden diese vier Fälle unterschieden:

1. „default“: Standard-Einstellung von Comidio; diese können vom Benutzer geändert, aber nicht komplett gelöscht werden.
2. „slider“: Eine Slider-Einstellung eines Benutzers durch den Security-Slider im Browser hat stattgefunden. In diesem Fall wird auch angezeigt, wann die Änderung stattgefunden hat und von welchem Client (Device) sie durchgeführt wurde.
3. „admin change“: Neuer Eintrag hier in dieser Maske. Hier können auch unqualifizierte Eintrage „*.domain.com“ vorgenommen werden, allerdings nur auf der linken Seite des Domain-Namens.
4. „auto“: Die TrutzBox erkennt einen SSL-Fehler und das Flag „Falls SSL-Fehler auftreten, Filtering für angesteuerte Domain automatisch ausschalten” ist aktiviert. Dieser Eintrag findet allerdings nur statt, falls es dazu noch keinen Eintrag durch den Benutzer gibt. Also keinen automatischen Eintrag wenn zuvor Fall 2 oder Fall 3 für diese Domain aufgetreten ist. In diesem Fall wird auch angezeigt, wann die Änderung stattgefunden hat, von welchem Client (Device) sie angestoßen wurde und welcher Verbindungsfehler die Ursache für diesen automatischen Eintrag war.

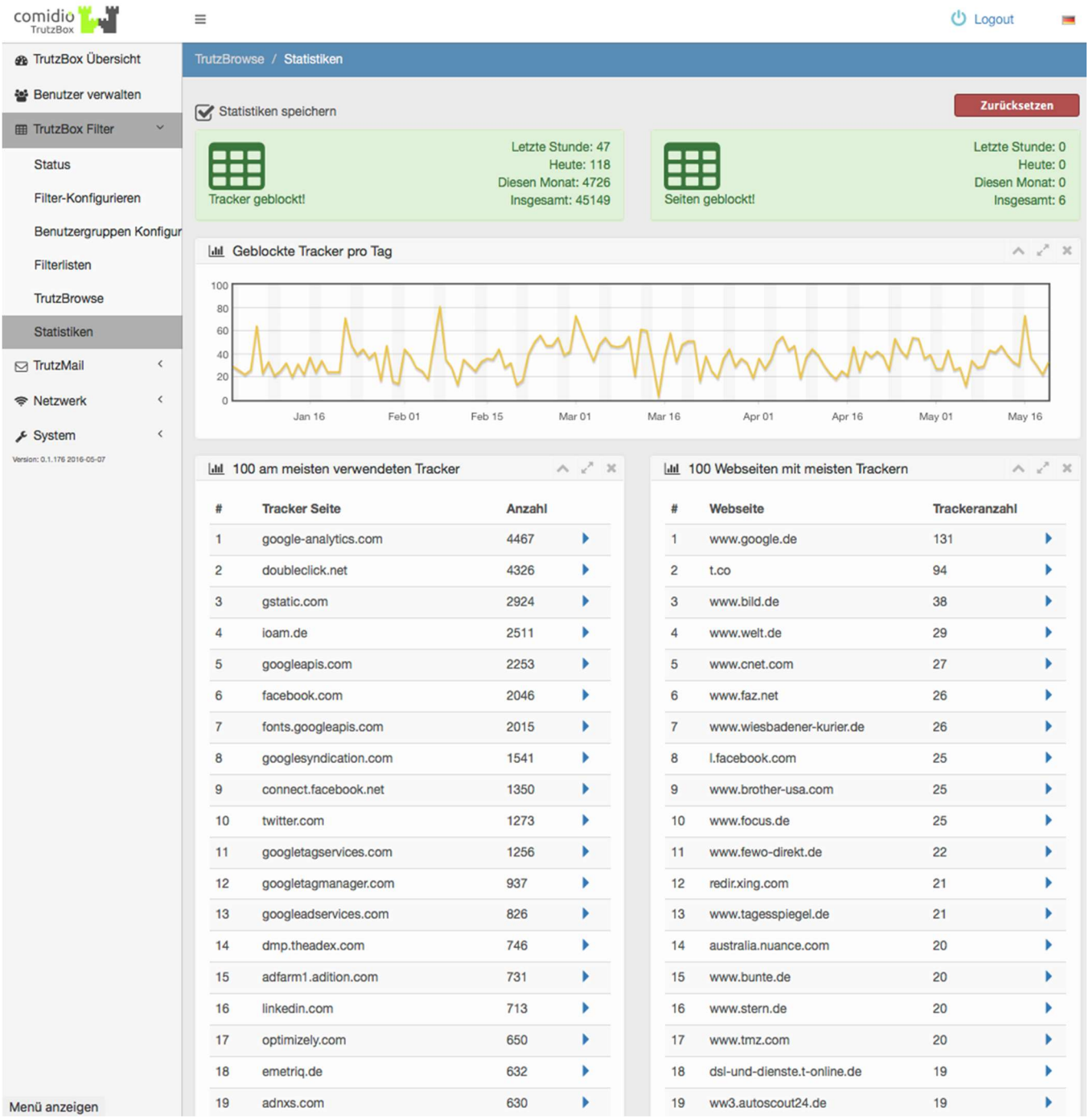
Gelegentlich kann es auch vorkommen, dass nicht eine App, sondern der Browser einen „socket Hang up“ Fehler auslöst. Z.B. bei ixquick.de. Ein Automatischer L10 Eintrag kann verhindert werden, wenn an dieser Stelle ixquick.de auf L1 gestellt wird.

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).

Mit Hilfe dieser 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. 5 Monaten. Erstaunlich ist die riesige Anzahl geblockter Tracker von über 45.000 für einen einzelnen Internet Benutzer:



(© 2015 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 zum 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[187] 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.

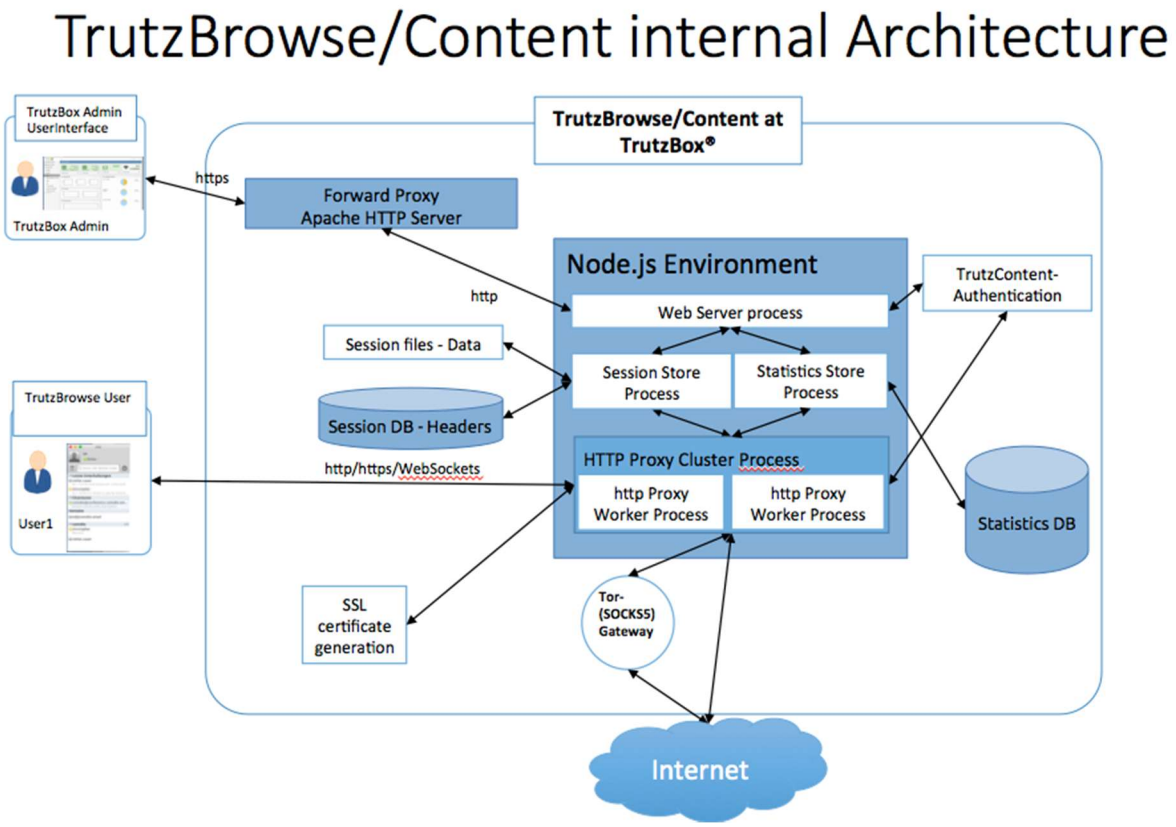
Neben der Generierung der SSL-Zertifikate, der Kontrolle der jeweilig zu blockierenden Seiten und der Anpassung der http-Header übernimmt dieser dieser auch:

- 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[188], die gerade die Ver- und Ent-schlüsselung beschleunigt und den Prozessor entlastet.

187 http://nodejs.org
188 https://de.wikipedia.org/wiki/AES_(Befehlssatzerweiterung)

Um eine bessere Ausfallsicherheit und den Zugriffs-Durchsatz zu erhöhen, wurde der eigentliche http-Proxy, der die angeforderten http-Zugriffe durchführt, mehrfach instanziiert.



(© 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

Unterschied zwischen TrutzBrowse und TrutzContent

TrutzContent: ist der Content-Filter der TrutzBox. Content-Filter bedeutet, dass, wenn ein Gerät (z.B. PC oder der Fernseher) eine bestimmte Webseite kontaktieren möchte, die TrutzBox prüft, ob dieses Gerät diese Seite aufrufen darf. Wenn nicht, wird der Zugriff auf diese Webseite blockiert.

TrutzBrowse: ist die Überprüfung von implizit aufgerufenen Webseiten. Also von Seiten, die der Benutzer nicht selbst aufgerufen hat, sondern automatisch, durch eine andere Webseite nachgeladen werden soll.

Im ersten Fall (TrutzContent) wirken die in "Filter-Konfigurieren" eingestellten Benutzergruppen, um zu erkennen, ob die Seite überhaupt aufgerufen werden darf, und, falls ja, den zur Anonymisierung eingestellten SecSlider-Level des Servers(TrutzBrowse-Einstellung). Im zweiten Fall (TrutzBrowse) wird der SecLevel der vorherigen Seite übernommen (also die Seite, die diesen impliziten Zugriff initiiert hat), um diese Slider-Einstellung auch für diesen Server zur Anonymisierung zu verwenden.

Diese Unterscheidung 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 sein Profil an Facebook liefert.

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 implizierter Aufruf ist, wurden für diese Unterscheidung im 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 Unterscheidung ist der http-Parameter "Referrer", aber auch das Timing zwischen zwei Server-Aufrufen spielt eine Rolle. So kann es vorkommen, dass bei fehlendem Referrer-Hinweis eine zu schnell angeklickte zweite Webseite irrtümlich als TrutzBrowse erkannt wird. In diesem Fall übernimmt die TrutzBox dann irrtümlicher Weise den SecLevel der vorherigen Seite.

DieTrutzBox kann somit nicht immer mit 100% Sicherheit feststellen, ob der Anwender die Seite bewusst aufgerufen hat oder ob sie implizit nachgeladen wurde. Wenn man z.B. zu schnell nach dem Laden einer Seite einen Link dieser Seite in einer Mail anklickt, dann kann es vorkommen, dass die TrutzBox 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. Dies stellt allerdings keinerlei Einschränkung im Grad der Anonymisierung dar.

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 TrutzContent-Filter aktiviert ist. Dieser „Nebeneffekt kann aber durch ein Browser-Refresh einfach umgangen werden.

Black- und Whitelist Zuordnung bei TrutzContent/TrutzBrowse

TrutzContent Zugriffe werden unter „Status“ angezeigt

TrutzBrowse-Zugriffe können im Menü aufgerufen werden unter „Status“ oder im Browser unter „Details“.

In welchem Fall eine Blacklist herangezogen wird, ist für TrutzContent und TrutzBrowse unabhängig voneinander einstellbar. So können z.B. Zugriffe auf „facebook.de“ bei TrutzContent erlaubt werden, damit Facebook genutzt werden kann, aber der Aufruf eines Shops, der indirekt facebook.de kontaktiert um ihre Profildaten an Facebook zu melden, über TrutzBrowse blockiert werden.

TrutzContent Black- und Whitelists werden über die Benutzergruppen-Definition einer Benutzergruppe zugeordnet (da darüber auch der Jugendschutz gesteuert wird, bzw. alle bewusst aufgerufenen Links).

TrutzBrowse Blacklists (hier gibt es keine Whitelists) werden in „TrutzBrowse“->“Verwendete Filterlisten“ zugeordnet.

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 sein. Die derzeit angebotenen E-Mail-Verschlüsselungslösungen basieren alle auf PGP[189] oder S/MIME[190]. 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 für den Laien in der Bedienung zu kompliziert, da der Benutzer zunächst einmal eine funktionale Erweiterung (Plugin) zu seinem E-Mail-Programm installieren muss. 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. 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.

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“[191] und in den folgenden Abschnitten, beschrieben worden sind[192]. 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[193].

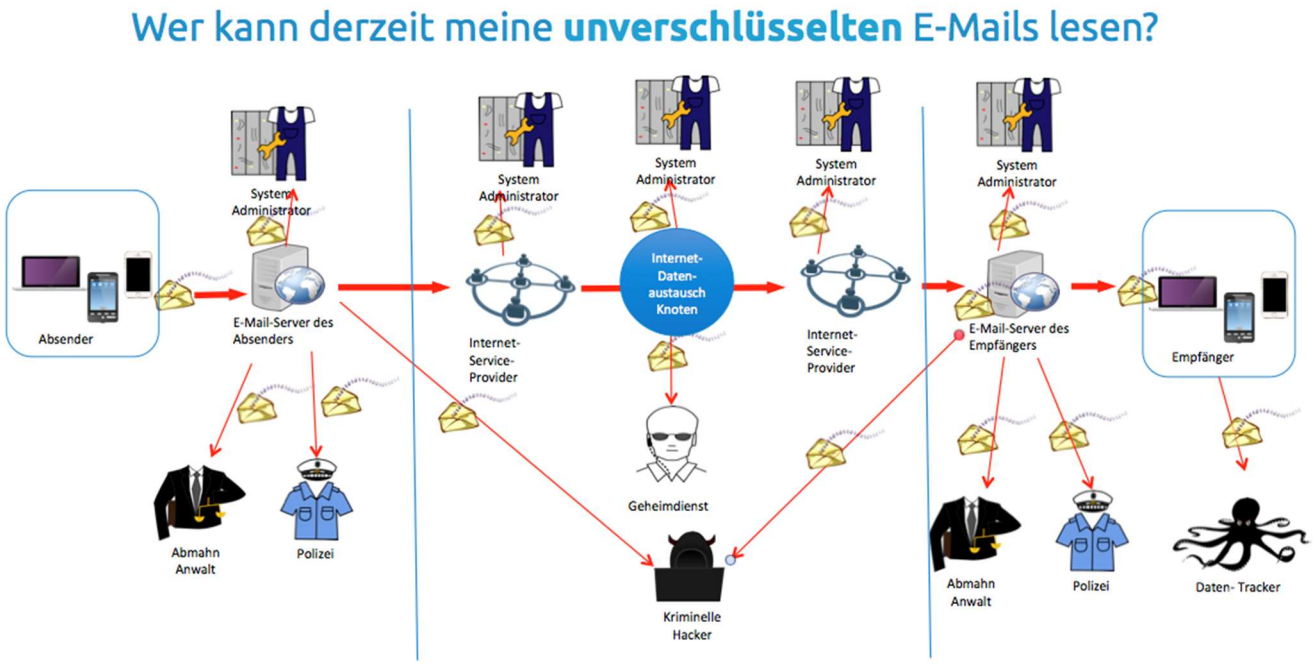
Es gibt zwar E-Mail-Provider, die behaupten, sichere E-Mail-Dienste anzubieten, aber auch diese sind nur so sicher wie es die zum Einsatz kommende Technologie zulässt. Lediglich das sich noch im Entwicklungsstadium

---

189 http://de.wikipedia.org/wiki/Pretty_Good_Privacy
190 https://de.wikipedia.org/wiki/S/MIME
191 http://secushare.org/PGP
192 http://www.heise.de/security/meldung/Massentaugliche-E-Mail-Verschluesselung-gesucht-2557237.html?wt_mc=nl.heisec-summary.2015-02-23
193 http://www.heise.de/security/meldung/Haufenweise-Fake-PGP-Schluessel-im-Umlauf-3297175.html?wt_mc=nl.heisec-summary.2016-08-18

befindliche sichere E-Mail-System „DIME“[194] plant, ein sicheres E-Mail-System mit verbesserter Technologie anzubieten. Die zu Grunde liegende Technologie ist ziemlich komplex und erfordert die Unterstützung möglichst vieler E-Mail-Provider. Ob sich diese Technologie auf dem Markt durchsetzen kann, ist noch fraglich. Falls ja, könnte die TrutzBox® Lösung dazu kompatibel gemacht werden.

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.



(© 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 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

[194] http://www.zdnet.de/88201628/lavabit-gruender-erlaeutert-entwicklungsstand-des-darkmail-projekts/

Servers ausfindig gemacht werden. Eine gute Übersicht über die Gefahren bei E-Mails und deren Lösungen gibt das „Privacy-Handbuch“[195].

Die allgemeinen Security-Anforderungen bei Kommunikation über öffentliche Netze sind:

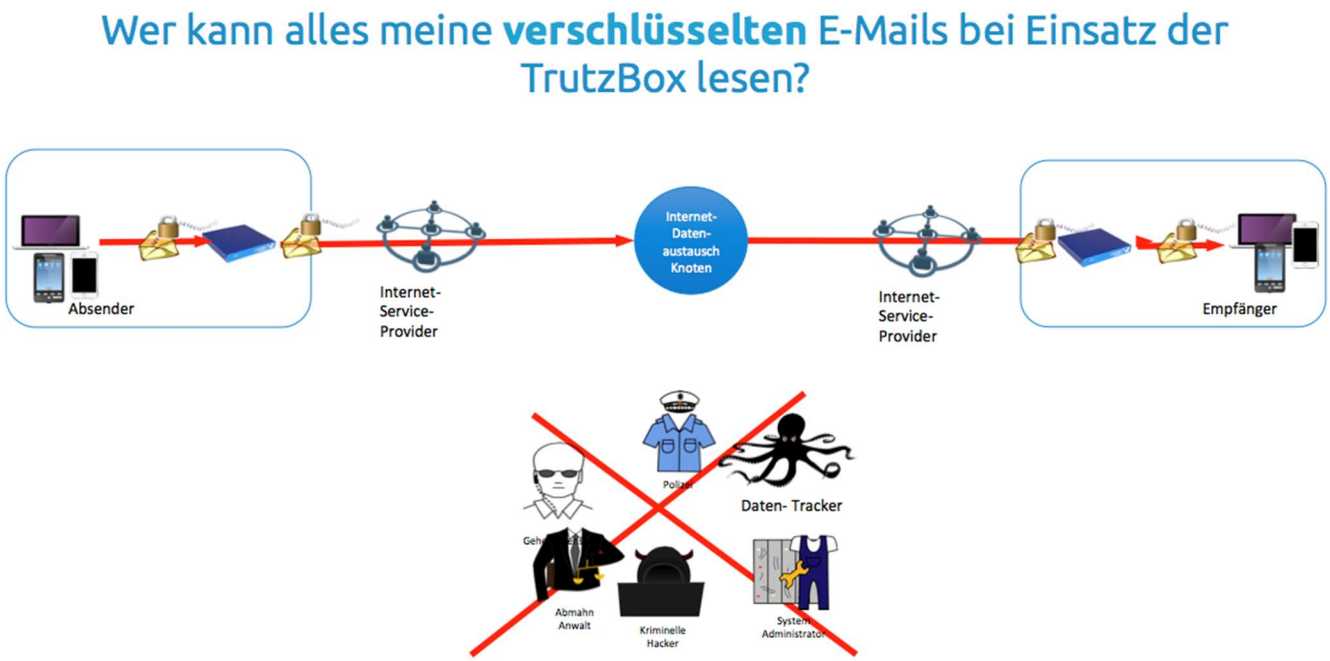
- **Authentizität** - die Gesprächspartner wissen zuverlässig, mit wem sie kommunizieren
- **Vertraulichkeit** - kein Dritter kann mithören oder Daten ändern
- **Perfect Forward Secrecy** - (*Folgenlosigkeit)* - bei abgefangenen Nachrichten kann niemand nach Beendigung der Sitzung den geheimen Langzeitschlüsseln 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:
- **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. Eine Lösung wäre, die E-Mails direkt zwischen Absender und Empfänger auszutauschen

[195] http://de.wikibooks.org/wiki/Privacy-Handbuch:_E-Mail_Kommunikation

(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 Mail-Server, mit dem sich das gewohnte E-Mail-Programm des Benutzers verbinden kann. Der Anwender ist damit nicht mehr auf einen fremden E-Mail-Provider angewiesen. Der Benutzer wird sozusagen zu seinem eigenen E-Mail-Anbieter (Stichwort Eigenhosting“). Und wird ein großer E-Mail-Anbieter gehackt und 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 den TrutzBoxen automatisch durchgeführt.

In manchen Ländern kommt es vor, dass Behörden die E-Mail-Provider auf Herausgabe von E-Mail-Passwörtern zwingen (Lavabit[196]). Da Comidio keinerlei geheime Daten von seinen Kunden hat, kann Comidio derartigen

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

behördlichen Informationsersuchen zwar Folge leisten, aber Behörden können so nicht an die geheimen Schlüssel 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 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 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[197] . 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, 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) [198] [199] . 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.

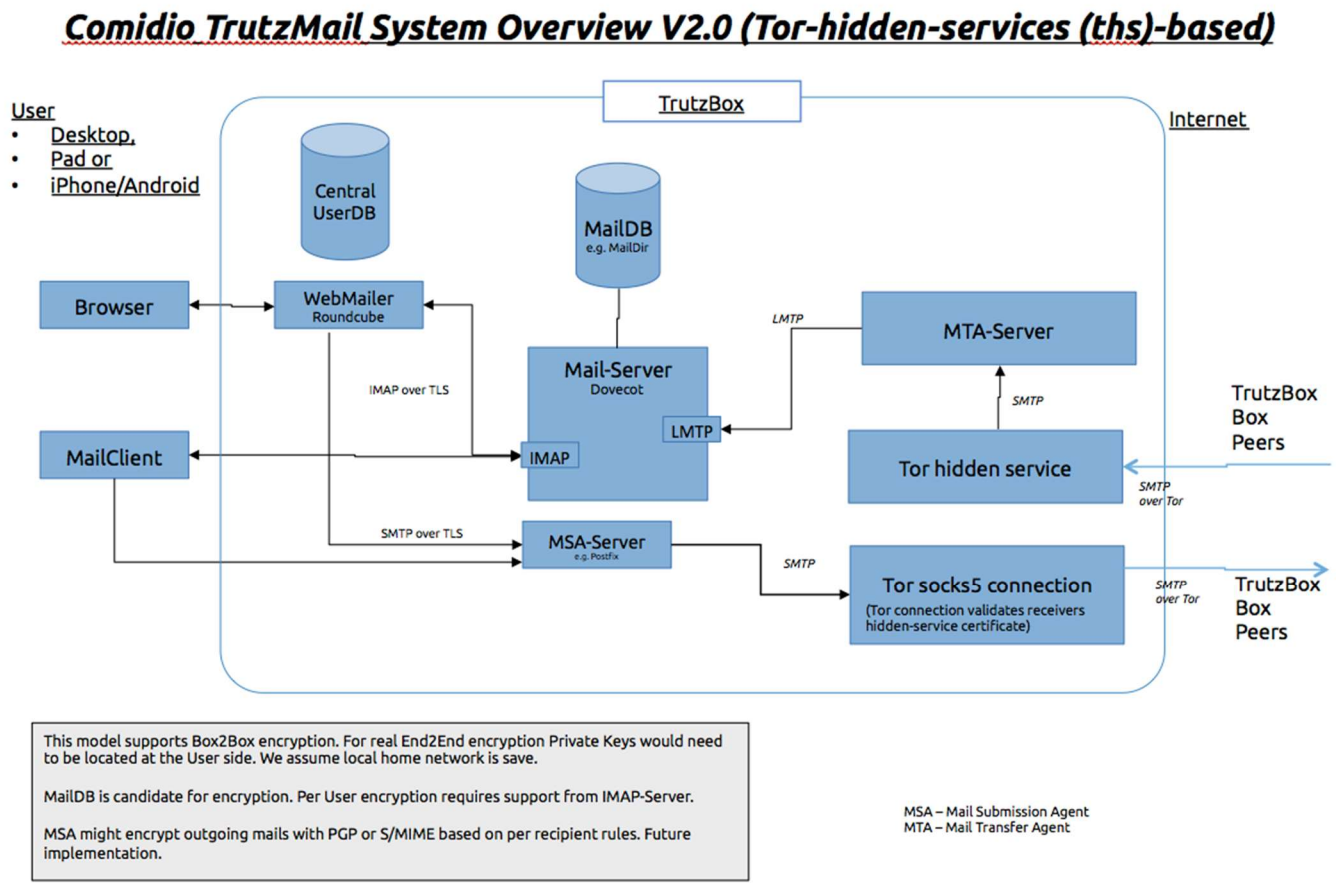
Beim Anlegen einer neuen TrutzMail Adresse wird auf der TrutzBox ein neuer Tor-hidden-service konfiguriert und im Tor-Netzwerk bekanntgegeben. Dabei bekommt jede TrutzMail Adresse auch eine .onion-Adresse zugeordnet. Falls dann eine andere TrutzBox® Kontakt aufnehmen möchte, um eine TrutzMail zu übermitteln, 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.

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

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

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

Nachstehend ist eine Übersicht der Comidio TrutzMail Architektur abgebildet:



(© 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 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 weiter verwenden. Er muss lediglich einen neuen E-Mail-Account in seinem E-Mail-Programm konfigurieren.

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 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 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:

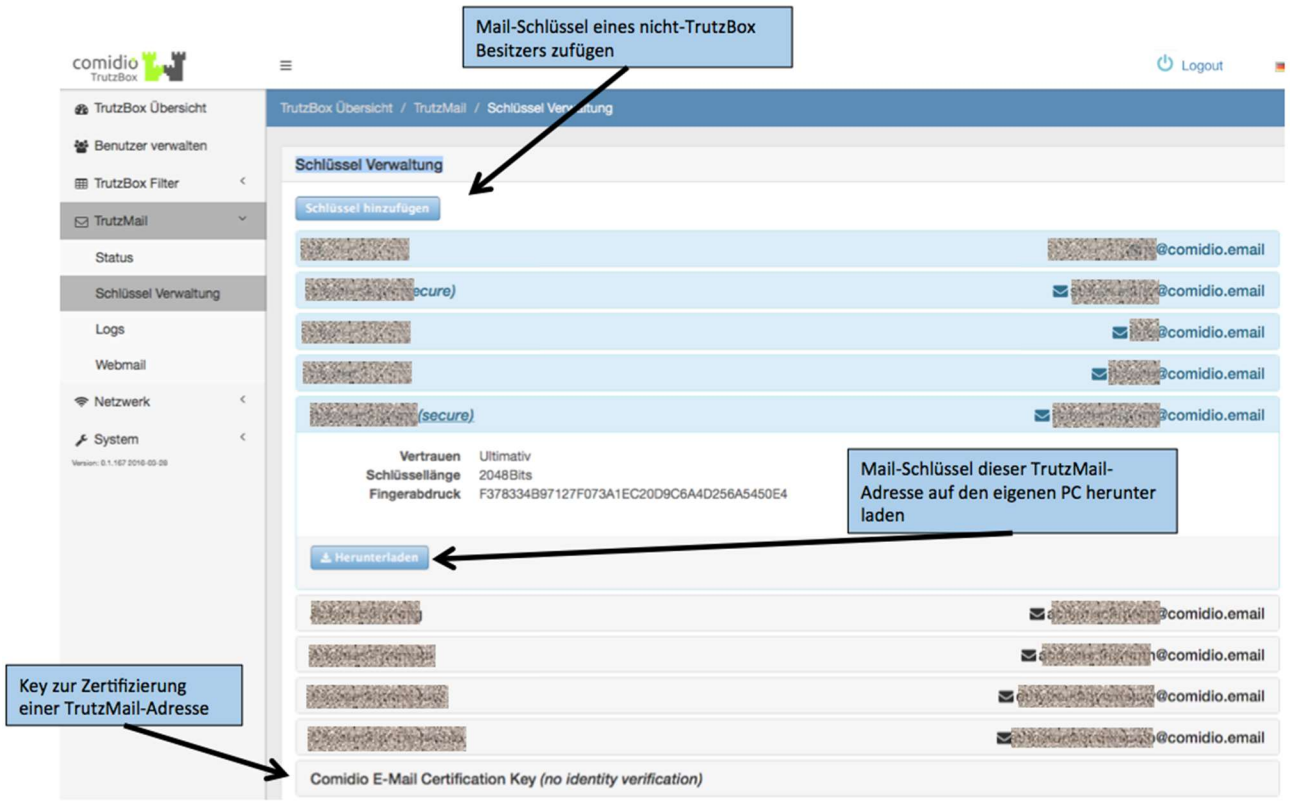
- Eine unverschlüsselte E-Mail, die von einem normalen Mail-Account an die TrutzBox gesendet wurde, hat im Betreff-Feld [UU], also unsigniert, unverschlüsselt.
- Eine verschlüsselte TrutzMail, die von einer TrutzBox an eine TrutzBox gesendet wurde, hat im Betreff-Feld [SE], signiert, encrypted.
- Eine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

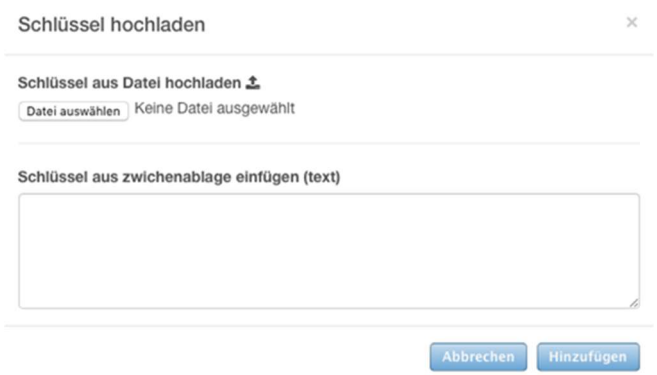
TrutzBox Schlüssel-Verwaltung

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 „TrutzMail“ -> „Schlüssel Verwaltung“ bekannt gemacht werden:



(© 2015 Comidio GmbH)

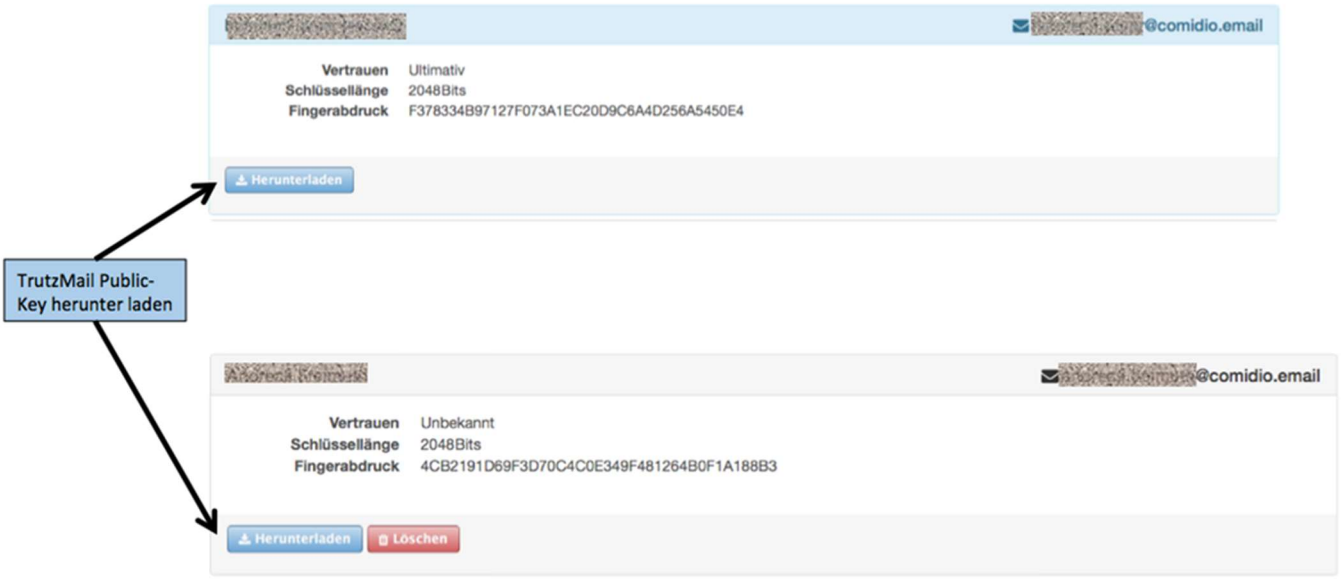
Mit dem Menüpunkt „Schlüssel Zufügen“ kann dieser neue Schlüssel importiert werden, indem er aus einer Datei geladen oder indem er aus der Zwischenablage eingefügt wird:



(© 2015 Comidio GmbH)

Sobald die TrutzBox einen öffentlichen Schlüssel für einen Mail-Empfänger, dessen Mail-Adresse nicht mit @comidio.email endet, kennt, wird diese E-Mal damit verschlüsselt.

Ein „TrutzBox Besitzer“ kann einem „Nicht TrutzBox Besitzer“, die Möglichkeit geben, ihm, dem TrutzBox Besitzer eine verschlüsselte E-Mail an die TrutzBox zu schicken. Hierfür erhält der Nicht-TrutzBox Besitzer den öffentlichen Schlüssel des TrutzBox Besitzers. Der öffentliche Schlüssel einer jeden TrutzMail Adresse kann unter „TrutzMail“ -> „Schlüssel Verwaltung“ herunter geladen und an einen anderen Mail-Versender geschickt werden:



(© 2015 Comidio GmbH)

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

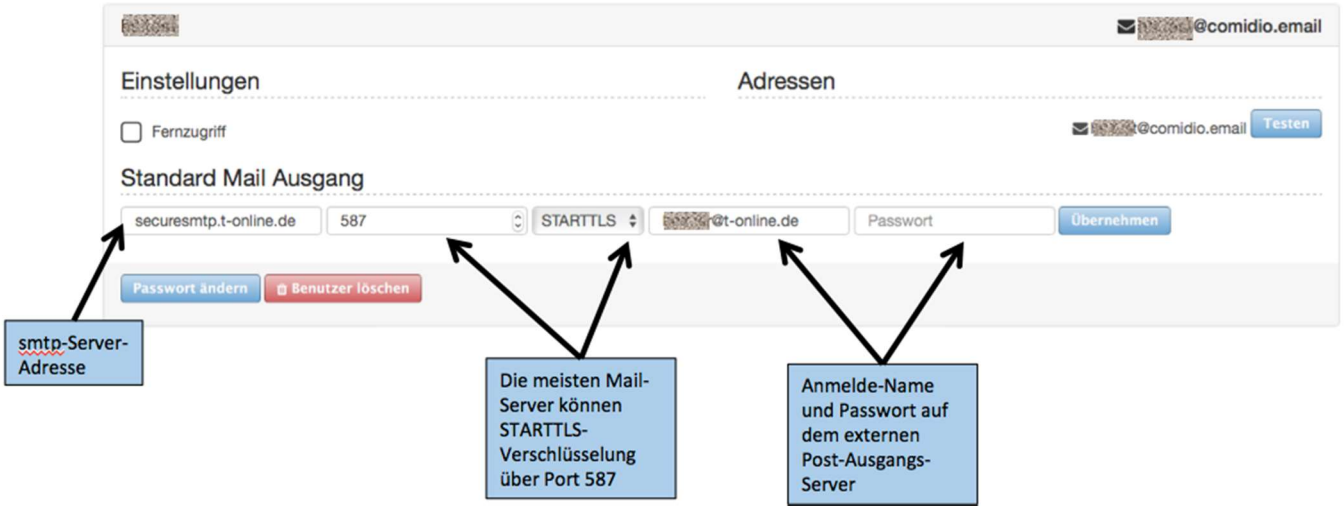
Empfangen von Standard-E-Mails

Um E-Mails von einem TrutzMail Account auch von 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. 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 weiterleitet.

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

Das von Comidio betriebene E-Mail-Gateway leitet externe E-Mails an die entsprechende TrutzBox weiter. Es kann jedoch aus Sicherheitsgründen, keine E-Mails von einer TrutzBox an einen „normalen“ E-Mail-Account weiterleiten. Um von der TrutzBox aus auch normale Standard-Mail-Accounts adressieren zu können, muss zuvor ein externes Mail-Gateway auf der TrutzBox eingerichtet werden. Dieses Mail-Gateway kann ein ganz normaler SMTP-Server eines Standard-Mail Accounts bei einem öffentlichen Mail-Anbieter sein. Somit ist es dem TrutzBox Administrator möglich, hier den E-Mail-Account seines eigenen öffentlichen E-Mail-Providers einzutragen.

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):



(© 2015 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 automatisch die Mail mit dem PGP-Verschlüsselungsverfahren, und 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. Somit muss für eine E-Mail mit der Adresse eines Standard-Accounts, der Public-Key zuvor auf der TrutzBox importiert werden. Ansonsten 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 authentifiziert wird.

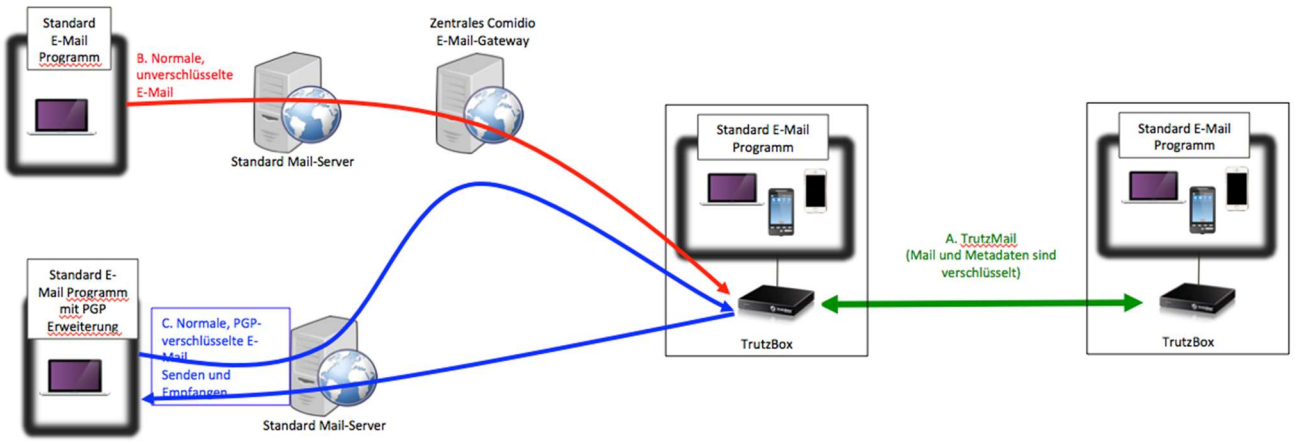
Natürlich können TrutzMails, die zwischen TrutzBoxen ausgetauscht werden, vom Anwender selbst auch zusätzlich mit PGP verschlüsselt werden.

Mail-Austausch über die TrutzBox: Zusammenfassung

Obige Beschreibungen lassen erkennen, dass es 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 unverschlüsselten E-Mails gesendet werden.



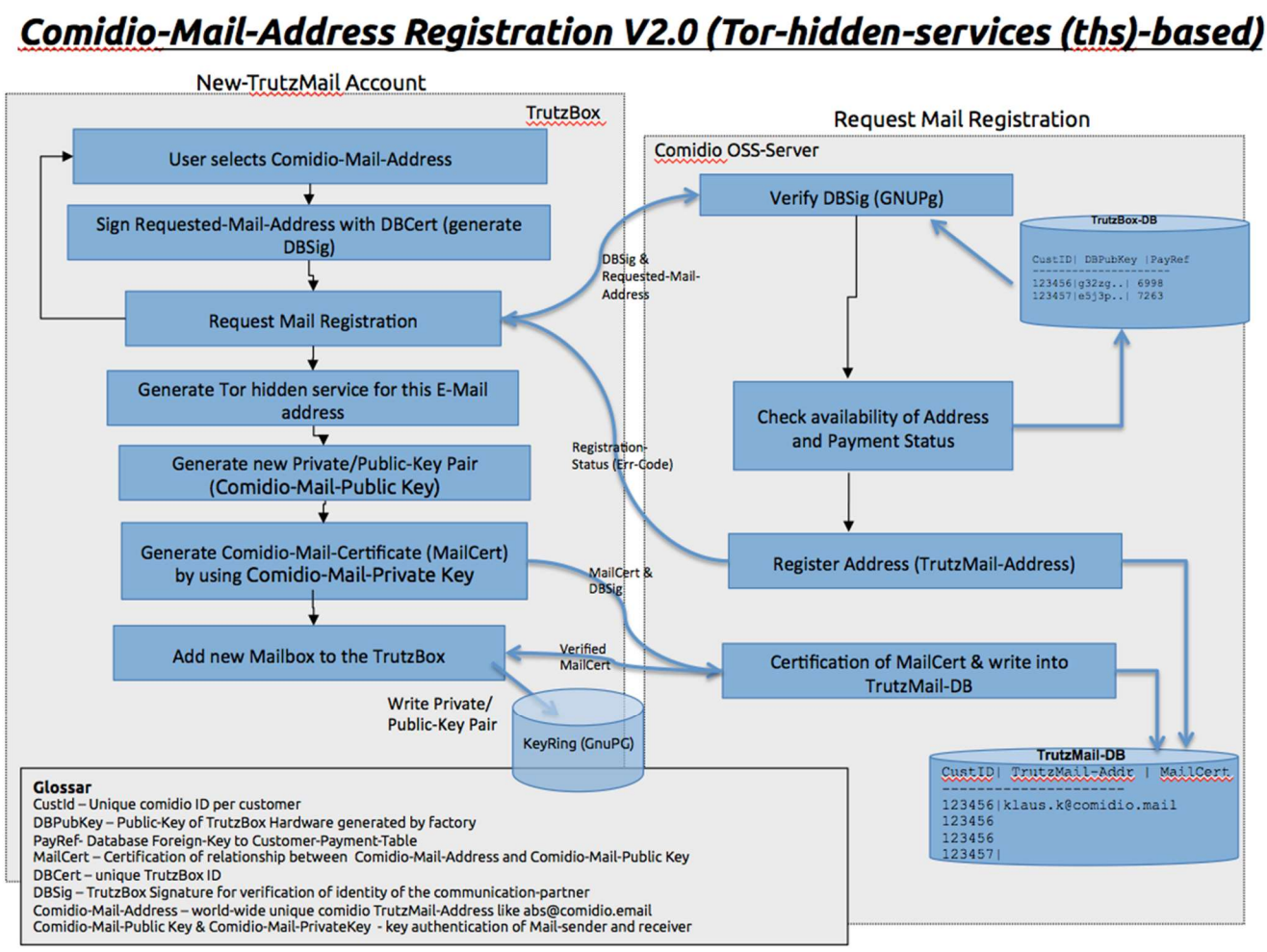
E-Mails über die TrutzBox können drei Wege gehen:
- A. TrutzMail – zwischen TrutzBoxen - immer verschlüsselt inkl. Metadaten
- B. Empfang unverschlüsselter E-Mails von Nicht-TrutzBox-Besitzern
- C. Senden und Empfangen von PGP-verschlüsselten E-Mails zu Nicht-TrutzBox-Besitzern

Aus Sicherheitsgründen können von der TrutzBox keine unverschlüsselten E-Mails gesendet werden.

Neue TrutzMail Adresse registrieren

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 E-Mail Adresse auch geprüft, ob der Kunde sein Kontingent bezahlt 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, die direkt zwischen TrutzBoxen ausgetauscht werden. Comidio kennt lediglich alle TrutzMail Adressen und deren Zertifikate (Public-Keys).



TrutzMail Certificate 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 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 der 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 „TrutzMail“ -> „Status“ eine Funktion „Mail-Schlüssel erneuern“. 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 wieder verwenden

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 eingerichtet wurde. Alternativ kann eine andere TrutzBox® Hardware verwendet werden, sofern sie dieselbe TrutzLegitimation hat wie die TrutzBox®, mit der diese TrutzMail Adresse erstmalig registriert wurde.

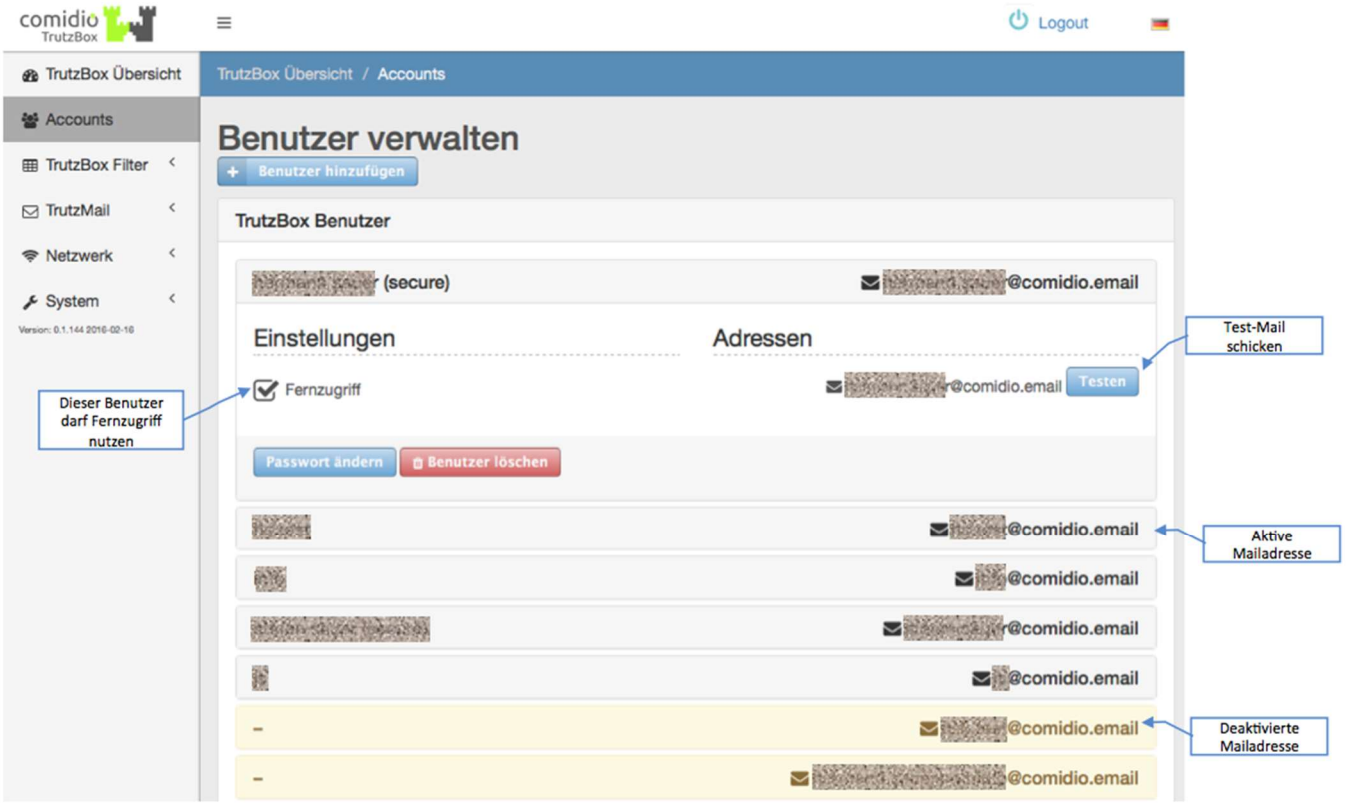
TrutzBox® Benutzer und TrutzMail Accounts verwalten

Da der Nutzer seinen normalen E-Mail-Client für alle E-Mail-Funktionen verwenden kann, bemerkt er nicht, wie im Hintergrund die E-Mails sicher ausgetauscht werden. Lediglich die E-Mail-Adresse, die mit @comidio.email endet zeigt ihm an, dass es sich um eine sichere E-Mail handelt.

Der TrutzBox® Administrator nutzt die Einrichtungsbedienoberfläche der TrutzBox® (Admin Userinterface), um beim Anlegen eines neuen TrutzBox Benutzers zu vermerken, ob sich dieser nur lokal auf der TrutzBox®

einloggen können soll, um TrutzContent zu nutzen oder auch ein TrutzMail Konto erhalten soll. Hier kann auch festgelegt werden, ob für diesen Benutzer der Fernzugriff erlaubt sein sollte. Wenn Fernzugriff hier aktiviert wird, dann generiert die TrutzBox für diese Mail-Adresse ein VPN-Zertifikat und ein OpenVPN-Konfigurations-File, das automatisch dieser Mailadresse zugesendet wird.

Durch drücken des Testen-Knopfes kann man dieser Mail-Adresse eine Test-Mail schicken.



(© 2015 Comidio GmbH)

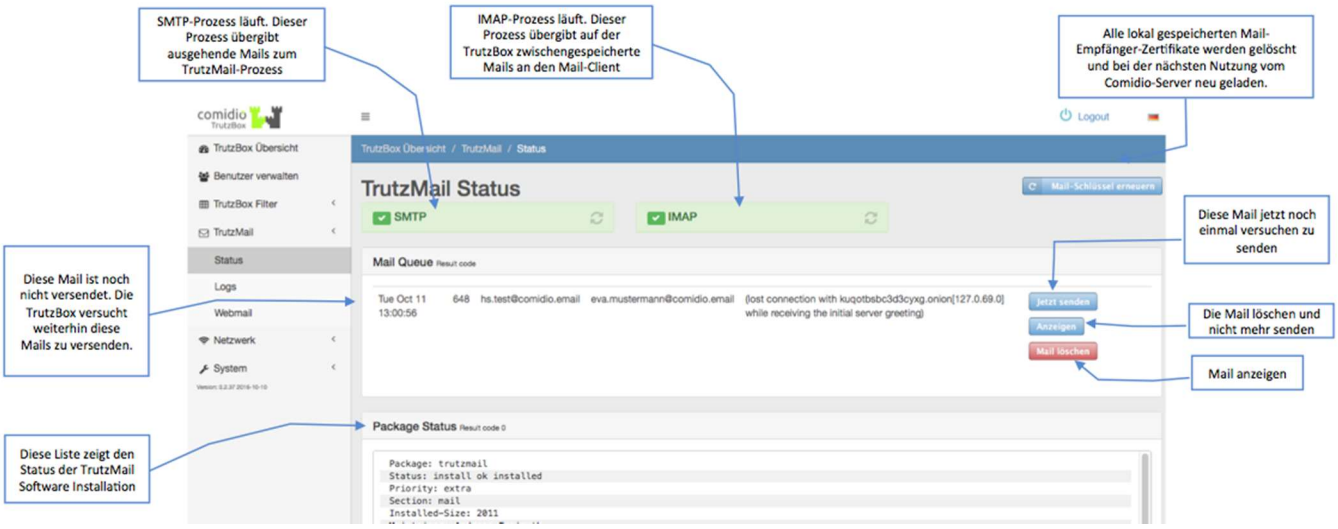
TrutzMail Adressen, die irgendwann einmal mit einer TrutzIdentifikation eingerichtet aber dann nachträglich gelöscht wurden, werden hier mit einem „Reaktivieren“-Knopf angezeigt.

(© 2016 Comidio GmbH)

Mit diesem Knopf kann die TrutzMail Adresse nachträglich wieder für diese TrutzBox reaktiviert werden.

TrutzMail Versand kontrollieren

Darüber hinaus bietet die Bedienoberfläche dem Verwalter der TrutzBox® auch Funktionen, die es ermöglichen, Probleme bei der Zustellung von E-Mails zu erkennen und gegebenenfalls zu beheben:



(© 2015 Comidio GmbH)

Mit dem Knopf „TrutzMail anzeigen“, kann man sich die Mail anzeigen lassen. Da allerdings Mails Base64 codiert sind, sind diese nicht lesbar. Indem der Mail-Text in www.base64decode.org kopiert wird, kann der Mail-Text decodiert werden.

Unter „TrutzMail“-> „Logs“ können die Log-Files der TrutzMail Prozesse angezeigt werden. Vier Voraussetzungen müssen erfüllt sein, um eine TrutzMail verschlüsselt und signiert an einen Empfänger zu schicken:

- Empfänger-Mail-Adresse muss existieren
- Absender TrutzMail Zertifikat ist gültig
- Empfänger TrutzMail Zertifikat ist gültig
- Empfänger TrutzBox ist eingeschaltet und am Netz

Abhängig davon welche dieser Voraussetzungen nicht erfüllt ist, werden entsprechende Informationen entweder direkt im MailClient, im TrutzBox-Mail-Status 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**)

TrutzRTC – Echtzeit Kommunikation (Real-Time-Communication)

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, basieren auf zentralen Kommunikations-Servern, die von Anbietern betrieben werden und somit zumindest die Möglichkeit einer Überwachung darstellen könnten.

Firmen oder auch Privat-Anwender nutzen allerdings gerne kostenlose Dienste wie WhatsApp oder Skype, bei denen sie teilweise in den AGBs sogar zustimmen, dass die Kommunikationsdaten ausgewertet werden.

Somit gibt es 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[200]. 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.

Somit war von Anfang an klar, dass die TrutzBox auch für Echtzeit Kommunikation eine sichere und anonyme Alternative anbieten muss.

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.

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

TrutzRTC XMPP-Server

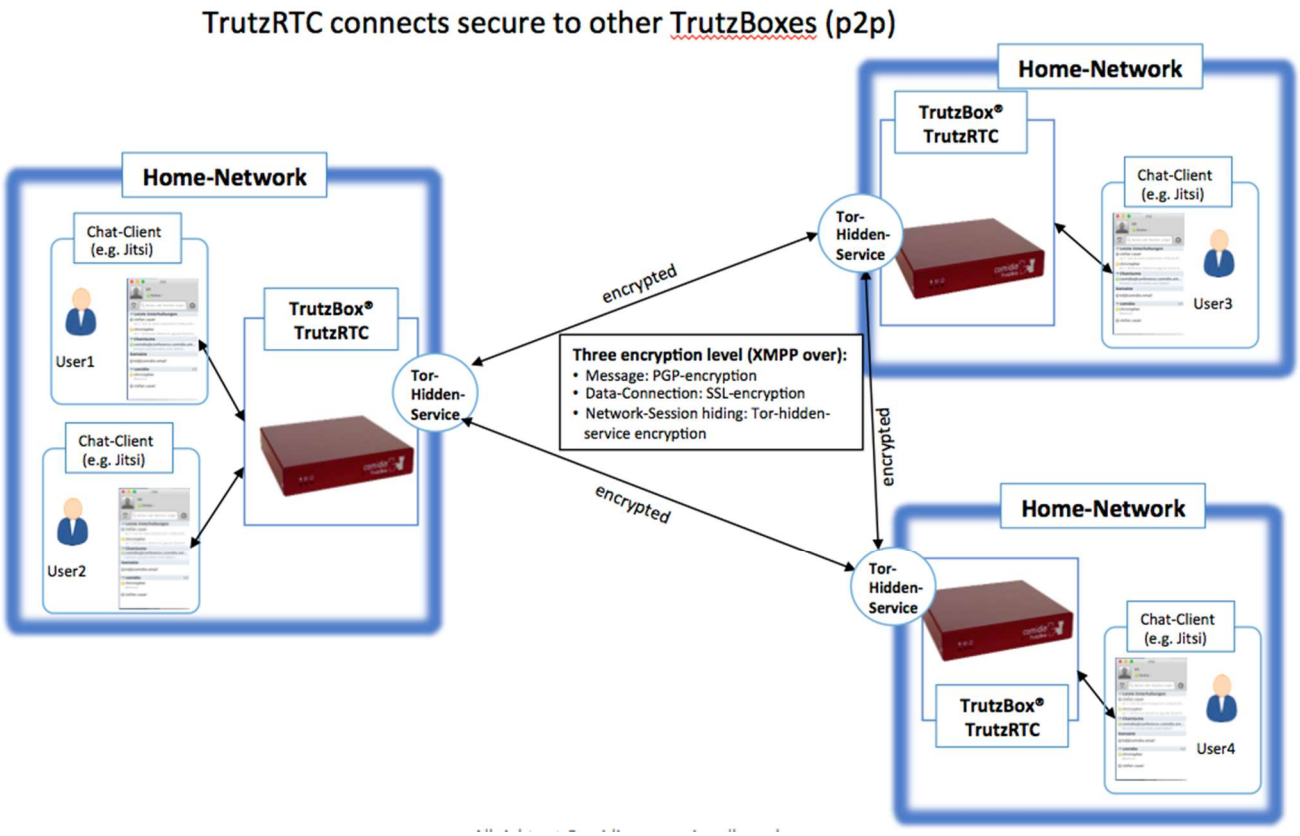
Das XMPP (Extensible Messaging and Presence Protocol), auf Deutsch „erweiterbares Nachrichten- und Anwesenheits-Protokoll“, ist ein Internet-Standard zum Austausch von Nachrichten (Chat). Es basiert auf der vor vielen Jahren entwickelten Jabber-Software und funktioniert ähnlich wie E-Mail. Ein XMPP-Server 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 Kommunikations-partners) 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 werden, 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 Messaging verwendet werden:



(© 2015 Comidio GmbH)

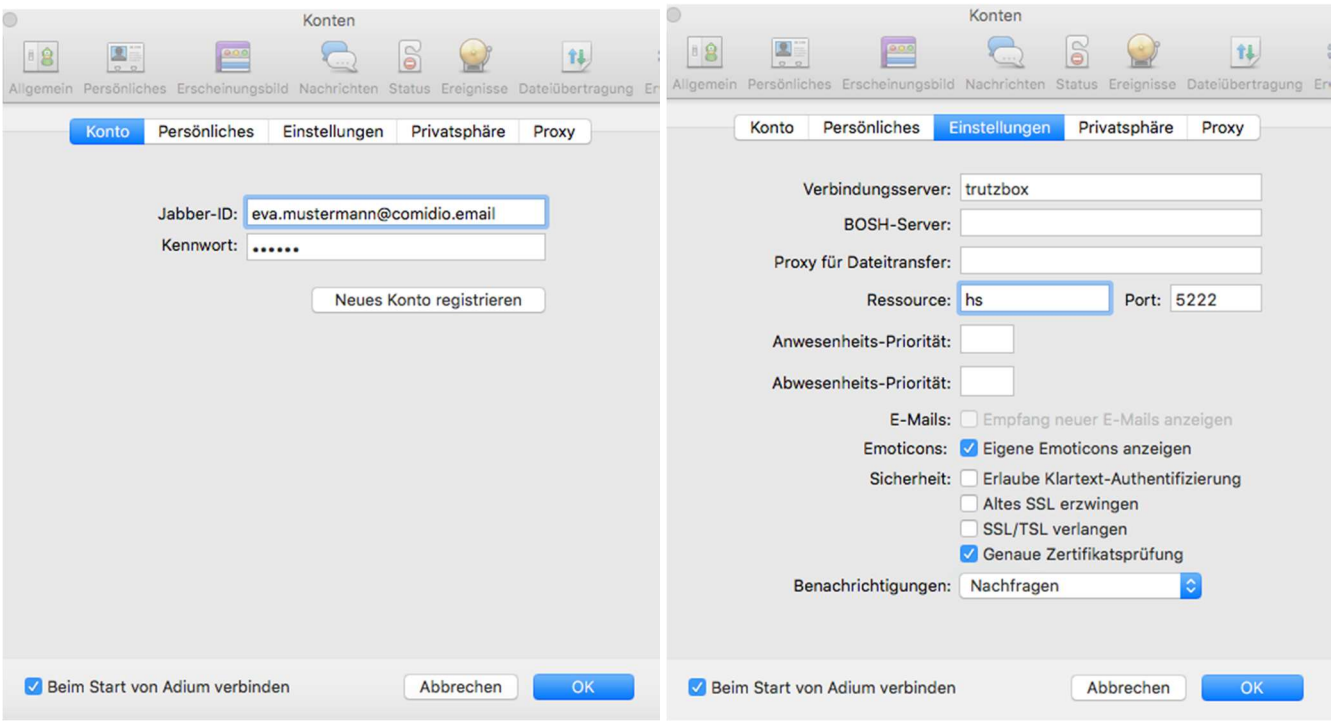
Um den XMPP-Server nutzen zu können, wird auf dem Endgerät ein XMPP-fähiges Programm benötigt. Chat-Programme, die das XMPP-Protokoll unterstützen, sind für alle gängigen Betriebssysteme mit unterschiedlichem Funktionsumfang verfügbar. Diese Links geben einen guten Überblick über verfügbare XMPP-Clients:

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

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 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[201]), allerdings derzeit nur für Kommunikations-Teilnehmer, die auf der gleichen TrutzBox angemeldet sind.
- Audio-/Video-Kommunikation: Telefongespräche (Jingle RTP Sessions, optional mit ZRTP Verschlüsselung[202]),
- 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
- OTR (Off-the-Record Messaging)[203]: inoffizielle; vertrauliche, nicht für die Öffentlichkeit bestimmte Nachrichtenübermittlung. Im Gegensatz zur normalen PGP-Verschlüsselung, ist mit OTR später nicht

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

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

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

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

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 oder dem sicheren Netzwerk der TrutzBox (Transparentmode) verbunden ist.

Um sich auch von unterwegs mit dem XMPP-Server auf der TrutzBox zu verbinden sollte der TrutzBox „Fernzugriff“ genutzt werden

Dazu, wie unter „Fernzugriff“ beschrieben, den TrutzBox Fernzugriff einrichten und den TrutzRTC Benutzer unter „Benutzer verwalten“ auf der TrutzBox für den Fernzugriff berechtigen. 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.

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[204] (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.

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 alle Teilnehmer einen Client im Einsatz haben, der den gleichen Audio-/Video-Codex unterstützen. 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. WebRTC[205] 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.

Um eine Video-Konferenz zu starten, muss lediglich mit einem WebRTC fähigen Browser die TrutzBox auf Port 9082 aufgerufen werden. Am Ende des Links wird einfach ein Raum-Name angehängt:

z.B.: https://trutzbox:9082/raumname

Beim gewählten Raumnamen dürfen keine Sonderzeichen verwendet werden!

Damit verbindet sich der Browser mit dem Raum “raumname”. 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.

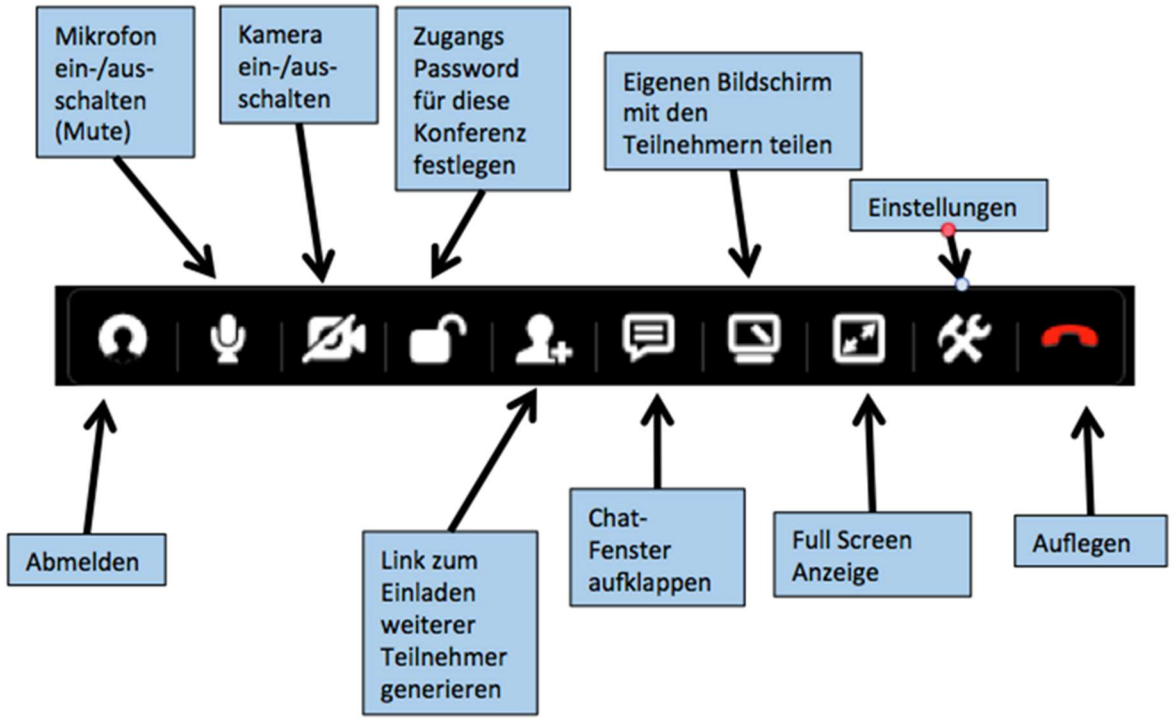
[204] https://de.wikipedia.org/wiki/ZRTP

[205] http://webrtc.org/

- 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 als Benutzer 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.

Bildschirm Inhalt übertragen (Screen-Sharing)

Mit ist es möglich, den eigenen Bildschirminhalt mit den Konferenzteilnehmern zu teilen.

Allerdings haben alle Browser eine eingebaute Sicherheitseinstellung, die verhindert, dass eine Software den Bildschirminhalt auslesen kann. Aus diesem Grund muss dem Browser zunächst mitgeteilt werden, dass die TrutzBox den Bildschirminhalt auslesen darf.

Bei **Chrome** ist es dazu notwendig, dass dieses Feature schon beim Aufruf deaktiviert wird. Dazu bitte auf dem

- **Mac**: chrome in der console mit diesem Befehl starten:
  open -a 'Google Chrome' --args '--enable-usermedia-screen-capturing'
- Unter **Windows** muss entsprechend Chrome mit den gleichen Parametern gestartet werden:
  https://github.com/muaz-khan/WebRTC-Experiment/tree/master/Pluginfree-Screen-Sharing

Bei **Firefox** muss dazu, nachdem Firefox gestartet wurde, durch Eingabe des Befehls *about:config* eine interne Konfiguration umgestellt werden. Danach nach *allowed* suchen und durch doppelclick auf den Parameter „media.getusermedia.screensharing.allowed_domains“ die Domain trutzbox in der Liste der erlaubten Domains hinzufügen.

Sicherheit und Anonymität bei der Nutzung des Konferenz-Servers

Der Konferenz-Server befindet sich auf der TrutzBox und nimmt keinerlei Verbindung zu einem anderen Server im Internet auf. Der WebRTC Browser verbindet 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. Niemand, der den Internet-Datenverkehr überwacht, ist in der Lage, Gespräche oder den Video-Stream zu entschlüsseln.

Leistungsgrenzen des Konferenz-Servers

Der TrutzRTC Konferenz-Server basiert auf der Open-Source Software Jitsi-Video-Bridge[206][207]. Obwohl dieser Konferenz-Server sehr leistungsfähig ist und auch die TrutzBox Hardware sehr leistungsstark ist, sind nicht unbegrenzt viele Teilnehmer möglich. Die Anzahl der Teilnehmer ist 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 bis ca 800 KBit/s jeweils benötigt. Somit werden wahrscheinlich bei normalen 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.

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 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.

[206] https://de.wikipedia.org/wiki/Jitsi

[207] https://jitsi.org/Projects/JitsiVideobridge

Dazu müssen allerdings auf dem Internet-Router diese zwei Ports geöffnet und an die TrutzBox weitergeleitet werden:

- TCP-9082
- UDP-9083

Mit dem Link „https://externe-ip-adresse:9082/raumname“ kann dann im Internet der Raum beigetreten werden.

Da sich bei den meisten Home-Internet Anbindungen einmal täglich die externe IP-Adresse ändert, ist es ratsam, auch hier einen DynDNS Service zu nutzen.

Eine weitere Möglichkeit, den richtigen externen Link für die Teilnahme an einer Konferenz zu ermitteln wurde in den TrutzBox XMPP-Server eingebaut. Übermitteln Sie im XMPP-Chat das Symbol „#“ mit einem Raumnamen an eine Person übermittelt, dann wird dieser „Befehl“ in den externen Link zum Konferenz-Server umgewandelt. Somit wird aus:

#meinraum

z.B. diese Adresse: https://188.107.13.86:9082/meinraum

die der Chat-Teilnehmer direkt anklicken kann um somit an der Videokonferenz teilnehmen zu können.

Interne TrutzRTC Architektur

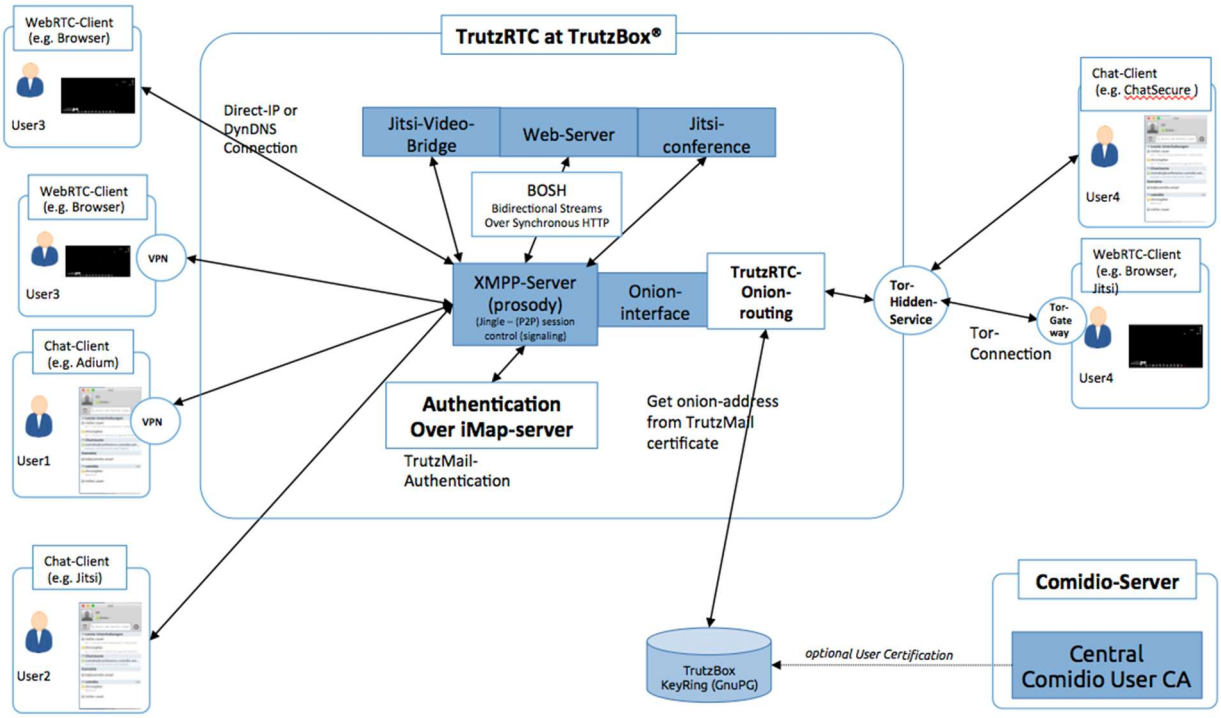
Zum besseren Verständnis hier eine Beschreibung der internen TrutzRTC Architektur. Kern der TrutzRTC Implementierung bildet der XMPP-Server „prosody“[208],[209]. Prosody ist ein weit verbreiteter Open-Source XMPP-Server, der sich vor allem durch seinen Ressourcen schonenden Betrieb und seine umfangreiche Erweiterbarkeit auszeichnet.

Um über die TrutzMail Adresse den XMPP-Server 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 TrutzBox 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.

[208] https://prosody.im/

[209] https://de.wikipedia.org/wiki/Prosody



(© 2015 Comidio GmbH)

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:

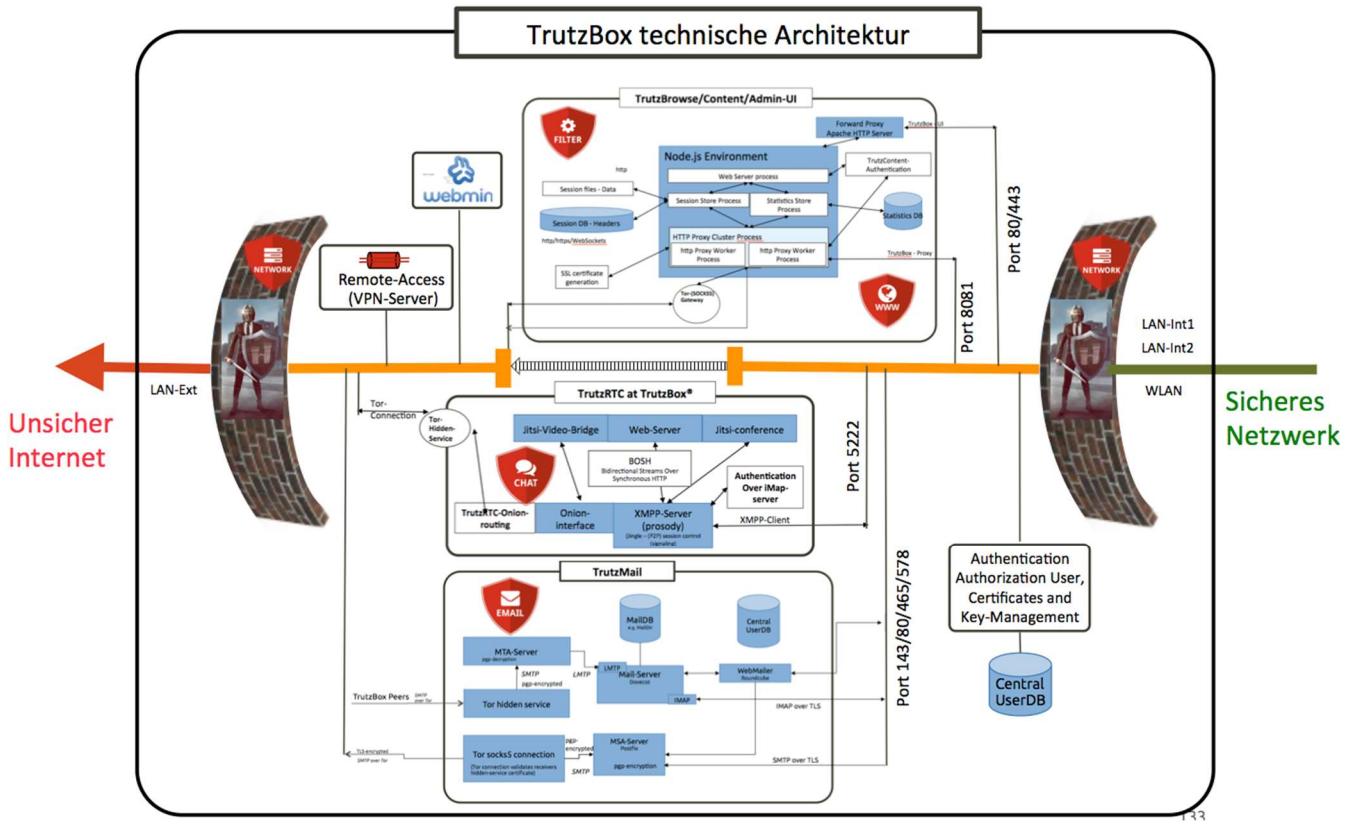
- TrutzBox Netzwerk
- Firewall
- Virenscanner
- Host Intrusion Detection System
- Abgesichertes Betriebssystem
- VPN–Zugriff auf die TrutzBox® über das Internet (Fernzugriff)

Des Weiteren sind für zukünftige TrutzBox® Releases in Planung:

- Network Intrusion Detection System bzw. DPI als Deep Packet Inspection (basierend auf Snort)
- Intrusion Prevention System (Kombination aus Snort, Firewall, Webfrontend und Logikmodul)

TrutzBox® Netzwerk

Die TrutzBox fungiert 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 Hoch fahren 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 geändert werden.

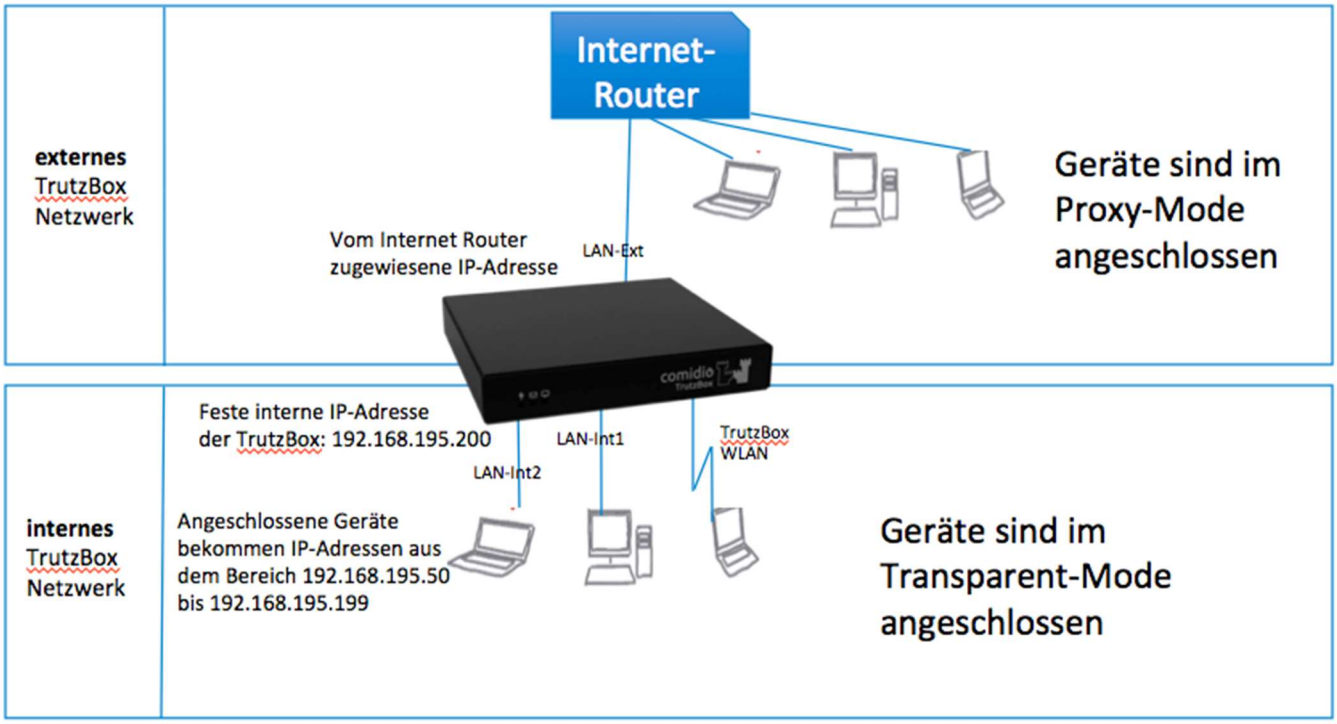
Das TrutzBox interne (sichere) Netzwerk

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. 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® 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. Die IP-Adresse der TrutzBox® bezieht sie beim Starten vom Internet-Router.



(© 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

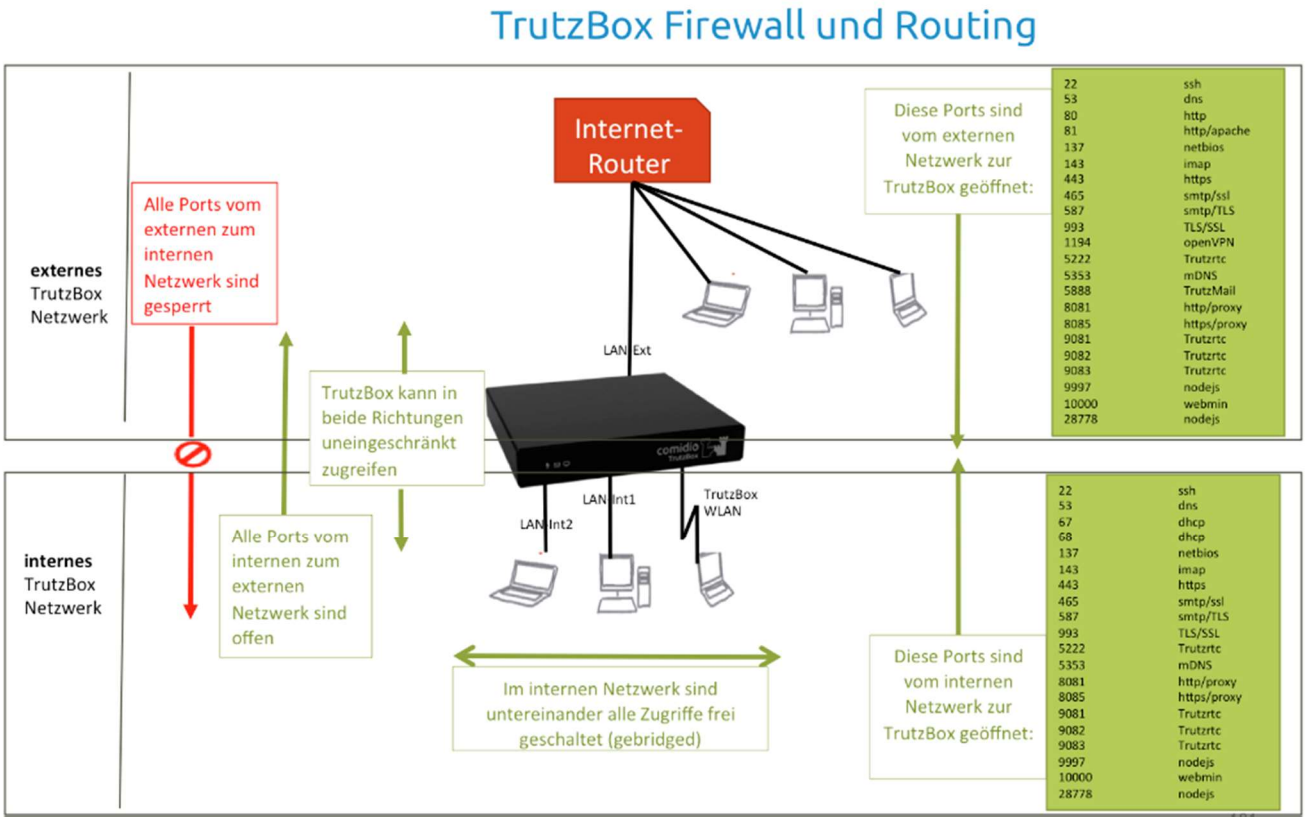
Firewall

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 unkontrollierten 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 gebridgt, 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.



(© 2017 Comidio GmbH)

Der TrutzBox® Administrator kann nach Bedarf weitere Ports öffnen.

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.

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. Es besteht aus einem eingebundenen Virenscanner sowie der Firewall selbst, die die Kommunikation zur TrutzBox® unterbinden kann. DPI wird in einer späteren TrutzBox® Version zur Verfügung stehen.

Durch all diese Maßnahmen bietet die TrutzBox® einen zusätzlichen Schutz vor Netzwerkangriffen.

Schutz vor Viren

Es kann z.B. sein, dass sich auf irgendeinem Gerät im internen Netzwerk des Internet-Nutzers, noch bevor die TrutzBox® installiert wird, eine Schad-Software eingerichtet hat. Oder auf einem PC eine Software per CD installiert wird, die einen Schädling enthält.

Oder dass der Nutzer einen verseuchten USB-Stick in ein Gerät steckt, der von einem kriminellen Hacker zuvor manipuliert wurde. Diese Viren werden, sofern sie über die TrutzBox® laufen, von der TrutzBox® erkannt und notfalls unschädlich gemacht.

Die eingesetzte Antiviren-Software bietet Schutz für die folgenden Bereiche:

- Schutz der TrutzBox® selbst vor Virenbefall
- Schutz vor Viren, die über E-Mail verteilt werden (TrutzMail)
- Schutz vor Viren, die über einen Web-Zugriff verteilt werden (TrutzBrowse) (noch nicht implementiert)
- Schutz vor Viren, die über das Netzwerk verteilt werden

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.

Sollte es dennoch einen Virenbefall geben, wird durch den Einsatz der Software ClamAV die TrutzBox® ständig auf Virenbefall überprüft und im Fall eines Angriffs wird der Virus erkannt und entfernt.

Schutz vor Viren, die über E-Mail verteilt werden:

ClamAV bietet auch die Möglichkeit, einen Virenschutz gegenüber allen von der TrutzBox® empfangenen E-Mails, einzubinden.

Diese E-Mails und ggf. deren Anhänge werden auf Viren überprüft und bei verdächtigen Inhalten in einen Quarantäne-Ordner verschoben.

Schutz vor Viren die über einen Web Zugriff verteilt werden:

ClamAV bietet die Möglichkeit einen Virenschutz in die TrutzBrowse Funktionalität einzubinden, um Webzugriffe auf Webseiten zu überprüfen. Diese Funktion ist derzeit noch nicht implementiert.

Zusätzlich empfiehlt Comidio, möglichst auf allen Internet-Geräten zusätzlich eine aktuelle Virenschutz-Software zu installieren.

Fernzugriff - VPN - Virtual Private Network

VPN bedeutet virtual private network. Ein VPN verbindet ein privates Netzwerk (Heimnetzwerk) mit einem unsicheren Netzwerk (das Internet). Es ermöglicht einem Computer über ein öffentliches Netzwerk Daten auszutauschen, als wäre der Computer direkt mit dem Heimnetzwerk verbunden. Über einen solchen VPN Zugang können TrutzBox® Nutzer die gesamte TrutzBox® Funktionalität von außerhalb des Heimnetzwerks nutzen, z.B. von unterwegs mit dem Smartphone.

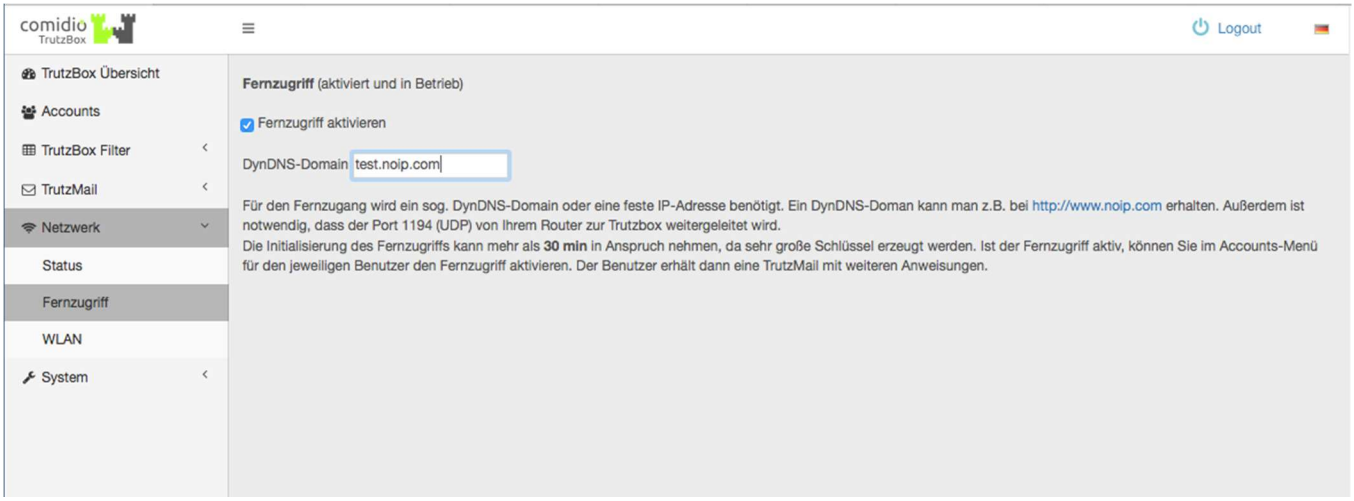
Dadurch bietet dieser Zugang die gleiche Funktionalität, Sicherheit und Kontrollmechanismen wie aus dem privaten Netzwerk zu Hause. Eine VPN Verbindung wird erreicht, indem eine virtuelle Punkt-zu-Punkt Verbindung mit entsprechender Verschlüsselung aufgebaut wird.

Mit VPN ist es dem TrutzBox® Besitzer auch möglich, anderen (z.B. Freunden oder Verwandten) Zugriff auf seine TrutzBox® zu geben und diese mitzubenutzen. Die TrutzBox® ermöglicht diese Mitbenutzung zwar, aber Comidio empfiehlt das ausdrücklich nicht, da der Administrator der TrutzBox® in der Lage ist, 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 von unterwegs, z.B. Hotel, auf die TrutzBox® zu Hause zugreifen zu können, muss diese zunächst über eine Adresse erreichbar sein. Da sich allerdings in der Regel die öffentliche IP Adresse, die der Internet-Service-Provider vergibt, täglich ändern kann, muss zunächst eine Dynamische-DNS-Adresse bei einem beliebigen Provider für Dynamische-DNS-Adressen eingerichtet werden (z.B. bei spdns.eu). Des Weiteren muss der Internet-Router für den externen Zugriff auf UDP-Port 1194 geöffnet werden, damit die TrutzBox von außen über das VPN-Protokoll erreichbar wird.

Die eingesetzte VPN Lösung auf der TrutzBox® (VPN-Server) basiert auf OpenVPN. Um VPN (Fernzugriff) nutzen zu können, muss dieser zunächst unter Netzwerk -> Fernzugriff aktiviert werden. Dazu wird ein zusätzlicher, sehr sicherer Schlüssel auf der TrutzBox® generiert, was sehr lange dauern kann (bis zu 30 Min.). Hier muss zuvor auch die DynDNS-Adresse des Internet-Anschlusses eingetragen werden.



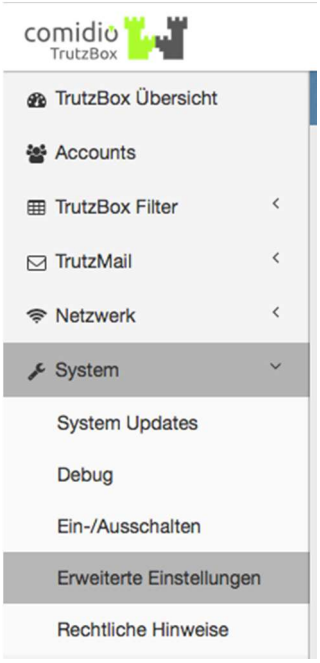
Nach der Fernzugriff-Aktivierung steht für jeden eingerichteten TrutzBox® Benutzer, der eine TrutzMail Adresse hat, unter dem Menüpunkt „Benutzer Verwalten“ eine neue Option „Fernzugriff“ zur Verfügung. Wird diese aktiviert, generiert die TrutzBox® ein „TrutzVPN-Certificate” für diese E-Mail-Adresse und speichert dieses in Form eines Open-VPN Konfigurations-Files (email-adresse.ovpn) ab. Dieses Konfigurations-File kann, nach Installation des OpenVPN Programms, auf den mobilen Devices importiert werden. Danach kann unterwegs von einem beliebigen Internet-Anschluss auf die TrutzBox® zu Hause zugegriffen und alle Funktionen genutzt werden. Eine Liste von VPN-Clients ist hier zu finden: https://de.wikipedia.org/wiki/OpenVPN#Frontends.

Erweiterte Einstellungen (Webmin)

Einige sehr betriebsystemnahe Funktionen, wie alle TrutzBase Funktionen, können mit dem Werkzeug „Webmin“ bedient werden. Webmin wird standardmäßig auf der TrutzBox® ausgeliefert und mit dem Menüpunkt System->Erweiterte Einstellungen aufgerufen.

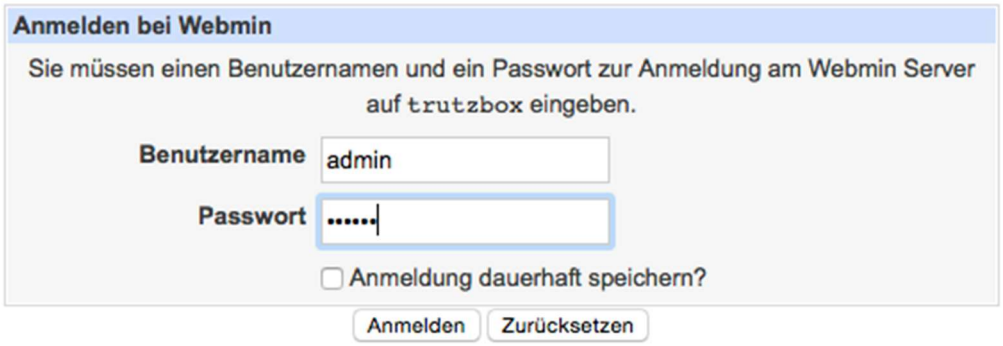
Wichtig: Webmin sollte nur von erfahrenen Linux Administratoren benutzt werden, da es mit diesem Werkzeug möglich ist, die Konfiguration der TrutzBox derart zu verstellen, dass diese nicht mehr nutzbar ist!

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!

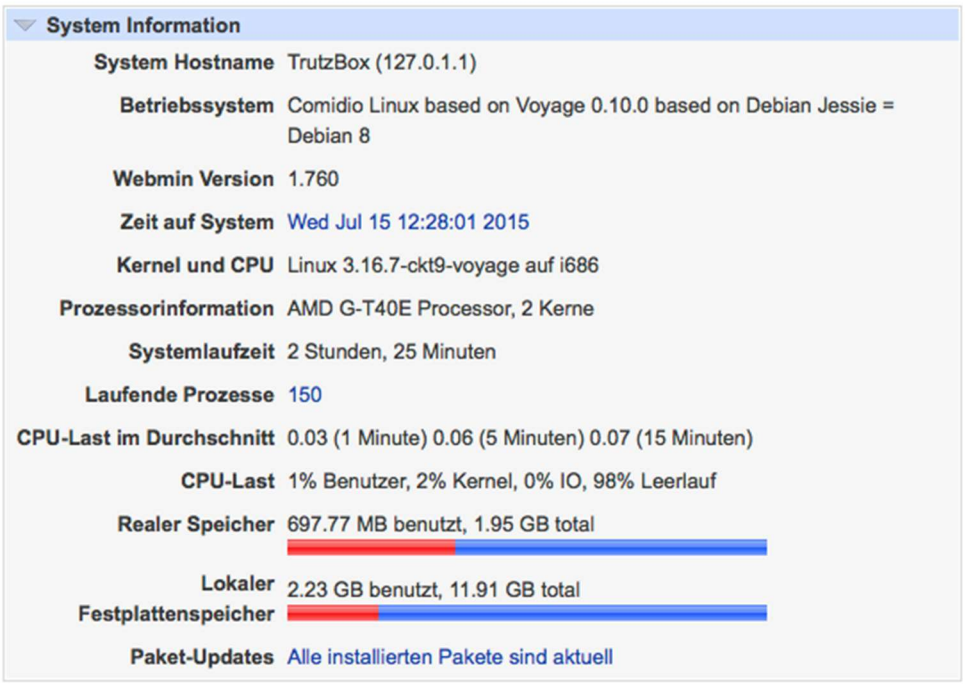


Da es sich bei Webmin[210] um ein eigenständiges Tool handelt, ist es notwendig, sich zunächst neu einzuloggen. Dazu bitte als Benutzernamen „admin“ und das TrutzBox® Administrator Passwort eingeben.

[210] http://doxfer.webmin.com/Webmin/Main_Page

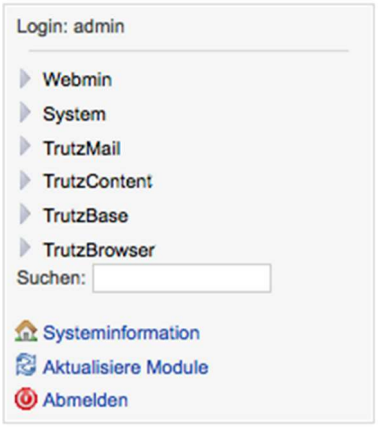


Nach dem Anmelden zeigt Webmin eine zusammengefasste Übersicht der Systeminformationen an:



Evtl. ausstehende Updates der TrutzBox® können direkt mit dem Link nach „Paket-Updates“ verwaltet 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)[211]. 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[212] (Linux), das von Comidio besonders abgesichert wurde.

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, Virenscanner und TrutzBrowse Blacklists aktuell halten zu können, wurde das Standard „Debian Package Manager“ (dpkg) verwendet.

Für den Notfall steht auch der Menüpunkt „Reset auf Werkseinstellung“ zur Verfügung. Hier werden alle Nutzerdaten und Einstellungen gelöscht und das Betriebssystem auf die Version des Auslieferungszustands gesetzt. Danach muss die TrutzBox® durch „update“ auf einen aktuellen Softwarestand gebracht werden.

TrutzBox® auf Werkseinstellungen 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 „System“ -> „System-Updates und –Reset“ die Möglichkeit, die TrutzBox in den gleichen Zustand zu versetzen wie bei Auslieferung.

Bitte beachten Sie, dass dabei alle Einstellungen und Daten auf der TrutzBox gelöscht werden. Also auch evtl. noch gespeicherte E-Mails werden dabei gelöscht.

Bei diesem Zurücksetzen auf Werkseinstellungen wird nach dem Neustart zunächst die aktuell aktive Partition sicher gelöscht. Somit sollte man bei einem Verkauf der TrutzBox zunächst einen solchen Reset durchführen. Danach wird eine komplette Sicherheitskopie der TrutzBox Software bei Auslieferungsstand, über die aktive Partition kopiert. Das kann längere Zeit dauern.

[211] http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

[212] http://linux.voyage.hk

Danach 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.

TrutzMail Adressen bleiben erhalten 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 Festplatte),
- geringer Stromverbrauch,
- neben WLAN auch noch mindesten 2 LAN-Anschlüsse mit schnellen 1Gbit,
- geringer Kühl- und Platzbedarf, mechanisch stabil, sodass weitere Geräte darauf gestapelt werden können und
- für Privatpersonen bezahlbar.

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.

Die technischen Daten des Boards:

- CPU: AMD Embedded G series GX-412TC, 1 GHz quad Jaguar core with 64 bit and AES-NI support, 32K data + 32K instruction cache per core, shared 2MB L2 cache.
- DRAM: 2 GByte DDR3-1333 DRAM, with optional ECC support
- Storage: Boot from SD card (internal sdhci controller), external USB, m-SATA SSD or conventional SATA SSD / HDD
- Power: About 6 to 10W of 12V DC power depending on CPU load. Connect to 2.5 mm DC jack (centre positive) or optional internal header
- I/O: DB9 serial port, 2 USB 3.0 external + + 2 USB 2.0 internal, three front panel LEDs, pushbutton
- 2 miniPCI express (one with SIM socket for 3G modem)
- Connectivity: 3 Gigabit Ethernet channels using Intel i211AT NICs, DB9 serial port for serial console, LPC bus, GPIO header, I2C bus, COM2 (3.3V RXD/TXD).
- Board size: 6 x 6" (152.4 x 152.4 mm)

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.

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 die SD-Karte 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).
- Pseudonymisierung der Client-IP-Adresse mit der man sich im Internet bewegt: nicht nur durch Tor sondern auch JonDonym zu ermöglichen. JonDoNym hat einige Vorteile gegenüber Tor: https://www.anonym-surfen.de/help/services_tor.html
- 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.

