Original-URL des Artikels: http://www.golem.de/news/privacy-boxen-im-test-truegerische-privatheit-1604-120250.html **Veröffentlicht:** 13.04.2016 12:05 **Kurz-URL:** http://glm.io/120250

Privacy-Boxen im Test

Trügerische Privatheit

Der Wunsch nach Privatsphäre ist bei vielen Nutzern groß, Privacy-Boxen sollen dabei helfen. Wir haben uns vier aktuelle Modelle angeschaut - und sind nur von einem Gerät überzeugt.

In den vergangenen Jahren haben immer mehr Hersteller kleine Boxen auf den Markt gebracht, die einfache Privatsphäre oder mehr Sicherheit versprechen. Darunter gab es Crowdfunding-Katastrophen, betrügerische Anbieter und viele Missverständnisse. Grund genug für uns, aktuelle Geräte zu testen. Unsere Kandidaten sind die Upribox, der Eblocker, die Trutzbox und die Relaxbox.

Zugegeben, wir gehen mit einer gewissen Skepsis an die Sache ran. Wer einfache Lösungen verspricht, liegt meist nicht nur in der Politik daneben.

Zwei unserer Testgeräte, die Upribox und der Eblocker, basieren auf Bastelrechnern und damit recht einfacher Hardware. Die Trutzbox kommt im massiveren Metallgehäuse und bietet einen Mehrkernprozessor, wie er auch in Heimservern oder ähnlichen Geräten steckt. Die Relaxbox basiert auf dem Haplite und hat damit auch eher schwache Hardware. Alle Geräte versprechen mehr Privatsphäre für die Nutzer, mit unterschiedlichen Methoden. Einige bauen einen einfachen VPN-Tunnel auf, außerdem sind bei allen Geräten Technologien zur Ausfilterung von Werbung und Tracker-Netzwerken eingebaut.

Zwei der Geräte werben zudem mit einem Schutz vor Viren und Trojanern. Hier sind wir besonders skeptisch, denn ein solches Versprechen könnte Nutzer dazu bringen, leichtsinnig unsichere Webseiten anzuklicken, weil die verwendete Box ja einen Virenschutz bietet. Alle Geräte mit Virenschutz setzen auf Clam AV, der in der Vergangenheit häufiger für seine niedrige Erkennungsrate kritisiert wurde. Hinzu kommt, dass sich über den Sinn und Unsinn von Virenscannern sowieso trefflich streiten lässt. Weil die Boxen als Sicherheits- und Privatsphäre-Geräte verkauft werden, haben wir sie einigen Tests unterzogen. Bei allen Geräten prüften wir, ob es offene Ports, SSH-Zugänge ohne Passwort oder Ähnliches gab - das war nicht der Fall. Damit schnitten alle getesteten Geräte in diesem Punkt besser ab als frühere Kandidaten.

Upribox - das österreichische Bastelprojekt

Unser erstes Testgerät ist die Upribox - kurz für Usable Privacy Box. Der kleine weiße Kasten basiert auf einem Raspberry Pi 2 und einem 3D-gedruckten Gehäuse, außerdem wird ein WLAN-Stick von TP-Link mitgeliefert. Die Upribox hat zwei verschiedene Modi mit den Namen Silent Mode und Ninja Mode. Im Silent-Mode sollen Werbetracker und aufdringliche Werbung geblockt werden. Im Ninja-Mode wird die Verbindung komplett über Tor hergestellt. Außerdem gibt es die Möglichkeit, sich per VPN von außen mit der Box zu verbinden, um auch unterwegs die Funktionen der Upribox nutzen zu können.

Das Projekt wird von Markus Huber in Kooperation mit der Universität St. Pölten hergestellt. Im Jahr 2014 wurde die Entwicklung der Upribox mit 50.000 Euro Fördergeld aus dem Netidee-Projekt unterstützt. Der gesamte Code des Projekts liegt bei Github. Mit dem mitgelieferten USB-Stick werden zwei neue WLANs aufgespannt. Eines für den Silent Mode, ein weiteres für den Ninja Mode. Der verwendete Stick unterstützt den modernen AC-Modus noch nicht und ist daher in seiner Geschwindigkeit limitiert. Nutzer können das Gerät aber auch per Kabel in ihr Netzwerk einbinden und dann die IP-Adresse der Upribox als Proxy in den Browser eintragen, um diese Beschränkung zu umgehen.

In unserem Test war jedoch vermutlich ein anderer Faktor geschwindigkeitslimitierend. Im Silent Mode erreichten wir an verschiedenen Tagen Geschwindigkeiten von 3 bis 5 MBit pro Sekunde - an einer Internetleitung mit bis zu 100 MBit pro Sekunde, ohne nennenswerte weitere Belastungen. Das ist selbst für normales Surfen heutzutage etwas langsam, an Downloads will man gar nicht denken. Doch wie viel mehr Privatsphäre bietet das Gerät eigentlich, verglichen mit einem Browserplugin wie Ghostery? *"Eigentlich genauso viel"*, sagt Projektleiter Huber im Gespräch mit Golem.de. *"Mit der Upribox wollen wir vor allem Smartphone-Nutzer besser schützen. Auf dem Desktop haben Nutzer bereits viele Optionen, aber bei Smartphones ist die Situation noch schwierig."*

Technisch setzt die Upribox auf eine Manipulation der DNS-Anfragen. Bekannte Werbetracker werden anhand verschiedener Blacklists ausgefiltert. Eine Whitelist für einzelne Seiten kann nicht hinterlegt werden. Bei uns führte der Einsatz der Upribox im Silent-Modus zu einem harten Logout aus allen verwendeten Konten und zu jeder Menge Captchas in den darauffolgenden Tagen.

Keine volle Anonymisierung durch VPN

Eine Anonymisierung der IP-Adresse bietet die Upribox im Silent Mode nicht. Generell ist aber zu sagen, dass eine reine Verschleierung der IP-Adresse keine umfassende Anonymisierung bietet. Sie verschleiert zwar den eigenen (Netzwerk-)Standort vor einem Webseitenbetreiber. Fingerprinting und die Sammlung personenbezogener Daten können aber weiterhin durchgeführt werden, besonders, wenn Nutzer sich auf einer Webseite anmelden. Außerdem gibt es Forschungsarbeiten, mit deren Hilfe festgestellt werden kann, ob ein Nutzer sich in der Nähe der vorgegebenen IP-Adresse aufhält oder nicht. Auch Netflix blockiert Nutzer von VPN-Diensten immer häufiger.

Verbindung über Tor misslingt öfter

Eine Verbindung über Tor herzustellen, gelang im Test nicht immer. Obwohl wir den Ninja-Modus in der Konfigurationsoberfläche des Gerätes aktiviert hatten und uns in das aufgespannte WLAN einloggen konnten, bekamen wir zu mehreren Testzeitpunkten keine Verbindung ins Internet. Fehlermeldungen lagen uns nicht vor. Manchmal funktionierte die Verbindung - war aber auch dann sehr langsam. Für die meisten Anwendungsszenarien erscheint uns aber ohnehin die gezielte Verwendung eines Tor-Browsers deutlich sinnvoller. Wer den gesamten Traffic des Betriebssystems zeitweise über Tor leiten will, kann auch Live-Systeme wie Tails nutzen. Zu kaufen gibt es das Gerät noch nicht. *"Wer die Upribox jetzt haben will, muss selbst aktiv werden"*, sagt Huber. Den Code gibt es bei Github, ansonsten werden nur ein Raspberry Pi und ein kompatibler WLAN-Stick benötigt. Das Gerät soll es aber langfristig auch zu kaufen geben, Interessenten können sich in eine Warteliste eintragen. Das 3D-gedruckte Gehäuse soll deutlich stabiler und der WLAN-Stick in das Gehäuse integriert werden. Das ließe sich zum Beispiel mit einem Raspberry Pi 3 problemlos realisieren. Derzeit sieht die Kombination aus Stick und Gehäuse noch etwas merkwürdig aus.

Fazit: mit eigener Hardware gerne mal ausprobieren

Weil es das Gerät noch nicht zu kaufen gibt, könnten wir derzeit noch gar keine Kaufempfehlung geben. Wer einen Raspberry Pi und einen damit kompatiblen WLAN-Adapter zu Hause hat, kann die Upribox jedoch mit einfachen Mitteln selbst nachbauen und ausprobieren. Unserer Einschätzung nach dürfte der Haupteinsatzzweck des Gerätes, wie von Huber beschrieben, bei Smartphones liegen. Auch IT-affine Nutzer, die ihrer Familie einen einfachen Weg zur trackerfreien Nutzung des Webs ermöglichen wollen, könnten aktiv werden, sollten aber die geringe Geschwindigkeit beachten.

Der Eblocker: ein Gerät, das ganze Netzwerk zu übernehmen

Unser zweites Testgerät ist der Eblocker. Auch dieser kleine Kasten basiert auf einem Minirechner, in diesem Fall dem Banana Pi. Das Unternehmen Eblocker GmbH hat die Produktion des Gerätes in einer Crowdfunding-Kampagne finanziert. Wir konnten einen Prototyp testen.

Der Eblocker verspricht den Nutzern eine trackingfreie Nutzung des Internets, einen Schutz vor dynamischen Preisen auf Webseiten und verhaltensabhängiger Werbung. Zudem soll er die Erstellung von Nutzerprofilen verhindern. Die Installation des Gerätes verläuft unproblematisch. Anders als die anderen Geräte baut das Gerät kein eigenes WLAN auf, sondern nistet sich direkt im Netzwerk ein. Strom rein, Netzwerkkabel rein - fertig. Das ist einfach, führt im Test aber auch zu Problemen. Dazu später mehr. Alle Funktionen des Gerätes können über eine Weboberfläche eingestellt werden. Außerdem blendet der Eblocker nach der Aktivierung auf allen Webseiten ohne HTTPS-Verschlüsselung eine Javascript-Toolbar ein, die anzeigt, wie viele Tracker auf einer Seite blockiert wurden und bietet direkt im Browser weitere Konfigurationsmöglichkeiten. Uns ist nicht ganz wohl dabei, dass ein solches Gerät Manipulationen dieser Art vornimmt, auch wenn die Konfiguration dadurch natürlich vereinfacht wird. Bei Seiten mit HTTPS-Verschlüsselung funktioniert die Toolbar in der ersten getesteten Version noch nicht, weil keine Manipulation der übertragenen Daten durch das Gerät möglich war.

Im zweiten Schritt konnten wir ein Image mit SSL-Funktion testen. Das Feature ist sinnvoll umgesetzt: Jeder Eblocker bekommt sein eigenes lokal erstelltes Zertifikat, so dass Angriffe wie gegen Lenovo- oder Dell-Rechner im vergangenen Jahr nicht zu befürchten sind. Außerdem ist eine Liste an Domains hinterlegt, bei denen der Eblocker die Verbindung nicht aufmacht und die Verschlüsselung somit auch vor dem Eblocker bestehen bleibt. In der bestehenden Konfiguration sind das vor allem Onlinebanking-Seiten, Nutzer können aber weitere Domains einfach hinzufügen.

Anonymisierungsfunktion unglücklich gelöst

Die Anonymisierung finden wir etwas unglücklich gelöst. Nach der Beschreibung gingen wir davon aus, dass das Gerät direkt nach dem Einstecken die IP-Adresse verschleiert. Doch die Funktion muss erst über die Toolbar aktiviert werden. Die Surfgeschwindigkeit variiert je nach aktivem Exit-Node, denn die Verbindung wird über das Tor-Netzwerk hergestellt. Grundsätzlich werden nur Netzwerkanfragen auf Port 80 über Tor geroutet. Wer seine Mails über IMAP abfragt, verschleiert seinen Standort daher nicht. Wem es nur auf die Verschleierung des Standortes ankommt, kann in diesem Fall also auch den Tor-Browser nutzen. Später soll auch die Integration bestehender VPN-Netzwerke möglich sein, wie Geschäftsführer Christian Bennefeld im Gespräch mit Golem.de sagte. Dann wäre eine höhere Geschwindigkeit möglich, aber es fallen für einen leistungsfähigen VPN auch weitere Kosten an.

Interessant finden wir die Funktion, einer Webseite ein anderes Gerät als das eigentlich verwendete vorzutäuschen. Eblocker-Nutzer können so auf ihrem iPad so tun, als ob sie einen Windows-Rechner einsetzten. Das könnte helfen, wenn Webseiten ihre Preise für Apple-Nutzer nach oben korrigieren oder eher die teurere Alternative als Standard vorschlagen, wie es bereits in verschiedenen Fällen berichtet wurde. IT-affine Nutzer können den User-Agent ihres Browsers auch selbst oder mittels Plugins ändern, als Plug-und-Play-Lösung umgesetzt ist dieses Feature mit dem Eblocker aber für deutlich mehr Nutzer verfügbar.

Zero-Installation macht Probleme

Im Test hatten wir aber auch Probleme mit dem Gerät. Im Heimnetzwerk des Redakteurs installiert, übernahm das Gerät nach Anschluss an den Router alle Netzwerkverbindungen auf allen Geräten. Dieser Eifer ging uns zu weit. Auf einem Rechner funktionierte der VPN-Zugriff auf Citrix-Anwendungen einer Universität auf einmal nicht mehr richtig. Erst nachdem der Eblocker für das Gerät in der Weboberfläche deaktiviert wurde, ließ sich die Anwendung wieder problemlos nutzen.

In Foren berichten auch andere Nutzer von Netzwerkproblemen, die mit der Konfiguration zusammenhängen. So sollen innerhalb des Netzwerkes doppelte IPs vergeben worden sein, was zu Problemen führt. Erst ein vom Hersteller durchgeführtes Upgrade auf SNAT behob die Probleme.

Immerhin lässt sich die Konfiguration recht genau einstellen. Wer mehrere WLAN-Access-Points betreibt, kann den Eblocker für das gesamte WLAN aktivieren oder deaktivieren. Alternativ können die Funktionen für jeden Client einzeln zu- oder abgeschaltet werden.

Jugendschutz- und Multi-User-Funktionen kommen Ende des Jahres

In Vorbereitung, aber noch nicht fertig, ist die Family-Variante des Eblockers. Sie soll im vierten Quartal 2016 erscheinen und Jugendschutzfilter und Multi-User-Support bieten. Testen konnten wir diese Funktionen noch nicht.

Geschäftsführer Christian Bennefeld kommt selbst aus dem Tracker-Geschäft. Er ist Mitbegründer des Unternehmens Etracker, das nach eigenen Angaben einen datenschutzfreundlichen Tracker herstellt. Er hält nach wie vor 30 Prozent der Anteile, wie er im Gespräch mit Golem.de erzählt. Daher sei er auch auf dem Laufenden, was in der Tracker-Industrie vor sich gehe. Wer einen Eblocker erwerben möchte, kann zwischen zahlreichen Optionen wählen. Die von uns getesteten Funktionen gibt es in der "Pro" genannten Version. Die Family-Version kann bereits erworben werden, die fehlenden Funktionen sollen dann Ende des Jahres nachgeliefert werden. Die Geräte gibt es jeweils in einem weißen *"Design-Gehäuse"* und in der Standardversion, einem transparenten Plexiglaskasten, der den Blick auf die inneren Komponenten freigibt. Beide Varianten kosten gleich viel. Außerdem können Nutzer zwischen einem zunächst einjährigen Supportzeitraum oder einer lebenslangen Lizenz wählen. Die Preise variieren zwischen 199 und 399 Euro.

Es ist auch möglich, einen eigenen Banana oder Raspberry Pi zu verwenden und nur eine Lizenz zu kaufen. Die Preise beginnen bei 59 Euro für ein Jahr bis hin zu 299 Euro für die Lifetime-Familien-Lizenz. Ein Raspberry Pi 2 kostet rund 40 Euro, ein Banana Pi 2 etwas mehr. Bei beiden Varianten können Nutzer sparen, wenn sie die Hardware selbst kaufen und das Image auf eine Micro-SD-Karte flashen.

Eher für Einsteiger als für Powernutzer

Auch bei diesem Gerät gilt: Es ist vor allem geeignet, um weniger IT-affine Verwandte und Bekannte zu versorgen, die keine Browser-Plugins, keinen Tor-Browser und keinen VPN installieren wollen. Die Funktion zur Geräteverschleierung finden wir interessant und gut umgesetzt. Als alleiniges Kaufargument reicht uns das aber nicht.

Nutzer mit komplexeren Netzwerken müssen den Eblocker auf jeden Fall selbst konfigurieren, wenn sie komplexere Netzwerkanwendungen nutzen wollen. Die eigentlich nutzerfreundliche "Zero-Installation"-Funktion kann für erfahrene Anwender also zum Nachteil werden.

Trutzbox: mehr Heimserver als Privacy-Box

Die Trutzbox bietet im Vergleich zu den Wettbewerbern deutlich mehr Funktionen und setzt auch auf solidere Hardware. Die Box ist mehr Heimserver mit Privatsphäre-Funktionen als reine Privacy-Box. Das hat natürlich seinen Preis.

Im Gespräch mit Golem.de sagte Trutzbox-Geschäftsführer Herrmann Sauer: *"Wir wollen ein Mehr an Privatsphäre so einfach wie möglich machen."* Mit der Trutzbox wolle man ein möglichst vollständiges Paket für anonyme Kommunikation anbieten. Auf dem Gerät läuft eine Debian-Version, die nach Angaben von Sauer *"gehärtet"* wurde und auf der Version Jesse basiert. Außerdem sind zahlreiche Dienste wie VPN, Tor-Zugang und Mailserver vorkonfiguriert. Per Software-Update soll in den kommenden Wochen außerdem ein WebRTC-Dienst für Audio- und Videotelefonie nachgereicht werden. Wir konnten den Dienst im Gespräch mit Trutzbox-Geschäftsführer Sauer bereits ausprobieren. Die Übertragung des Bildschirminhaltes funktionierte dort ohne Probleme. Ist der Dienst aktiv, können Nutzer ohne weitere Software mit Freunden und Bekannten kommunizieren - und das über den eigenen Server. Technisch basiert das Gerät auf AMDs T40E-Zweikern-CPU aus der G-Serie mit einem Takt von 1 GHz, die auch in anspruchsvollen NAS-Systemen eingesetzt wird. Der CPU zur Seite stehen 2 GByte RAM und 16 GByte Speicher, der von einer Micro-SD-Karte kommt. Das Gerät bietet aber auch PCI-Express-Erweiterungsplätze. Die Hardware wird von dem schweizerischen Hersteller PC Engines unter dem Namen APU1D vermarktet.

Hochwertiges Gehäuse

Das Gerät ist in einem blauen Metallgehäuse verpackt, das sich deutlich hochwertiger anfühlt als die anderen Testgeräte. Alternativ gibt es das Gerät in Rot oder Schwarz. Auch die Netzwerkschnittstellen sind deutlich leistungsstärker: An der Rückseite befinden sich drei RJ45-Ports mit jeweils 1 GByte/s Durchsatz. Einer davon wird als Eingang genutzt, zwei stehen als Ausgang zum kabelgebundenen Anschluss von Rechnern zur Verfügung. Das Gehäuse bietet zwei USB-Anschlüsse, wobei einer durch den WLAN-Stick blockiert wird. Dazu gleich mehr. Der Hersteller macht keine Angaben über den verwendeten Standard, wir vermuten USB 2.0. Zu guter Letzt gibt es für Nostalgiker eine serielle Schnittstelle.

Es wird ein WLAN-USB-Stick mitgeliefert, über den die Box ein eigenes Netz aufspannen kann. Auch in diesem Fall empfinden wir das aber eher als Notlösung. Denn einerseits kann der USB-Stick wegen Platzproblemen nicht direkt an das Gehäuse angeschlossen werden, sondern muss über eine USB-Verlängerung angeschlossen werden - das sieht etwas komisch aus. Andererseits bietet der Stick auch in diesem Fall maximal N-WLAN-Geschwindigkeit und könnte daher zum Flaschenhals werden, gerade wenn NAS-Funktionen an dem Gerät genutzt werden. Für Nutzer mit einem bestehenden schnellen WLAN-Netzwerk dürfte es daher sinnvoller sein, das Gerät per Kabel mit dem Router zu verbinden und dann als Proxy im Browser einzutragen.

Gerät mit Updates kostet 299 Euro

Gemeinsam mit dem Gerät muss ein Update- und Service-Paket für mindestens ein Jahr erworben werden, was derzeit 299 Euro kostet. Nach Ablauf der Periode lassen sich die einzelnen Funktionen noch mit den Bordmitteln aktualisieren, wie Sauer verspricht. Der in die Trutzbox-Weboberfläche integrierte Updater funktioniert dann aber nicht mehr.

Die Installation des Gerätes verläuft unproblematisch. Im Lieferumfang findet sich eine detaillierte Anleitung mit den ersten Schritten, die sowohl die Einbindung des Gerätes ins Netzwerk als auch die Einrichtung der Funktionen über den Webbrowser erläutert und schematisch darstellt. Damit dürfte es auch für unerfahrene Nutzer kaum ein Problem sein, die Trutzbox in Betrieb zu nehmen.

Der Trutzbox-Hersteller Comidio bietet außerdem regelmäßig Webinare an, um Nutzern beim Umgang mit der Box behilflich zu sein. Die Teilnahme an diesen Webinaren ist im Service-Paket enthalten und verursacht keine weiteren Kosten.

SSL-Zertifikat wird lokal erzeugt

Während der Einrichtung muss der Nutzer ein Stammzertifikat in den Browser importieren, damit die Trutzbox den eingehenden Datenverkehr untersuchen kann. *"Das Zertifikat wird bei der Einrichtung des Gerätes auf dem Gerät lokal erstellt"*, sagt Geschäftsführer Sauer. *"Wir können also nicht selbst in die Verbindungen reinschauen."* Die Einrichtung muss für alle verwendeten Browser durchgeführt werden, sonst gibt es beim Aufrufen SSL-verschlüsselter Seiten Fehlermeldungen. Weil das Zertifikat individuell erstellt wird, sind Trutzbox-Geräte auch nicht für Angriffe wie bei Superfish oder dem von Dell vorinstallierten Root-Zertifikat anfällig.

Die in diesem Test wichtige Grundfunktion der Anonymisierung, beziehungsweise des Tracker- und Werbeblockers, erfüllt das Gerät. Zum Einsatz kommt einerseits Technik des deutschen VPN-Anbieters Jondonym, alternativ kann eine Verbindung über das Tor-Netzwerk hergestellt werden. Nutzer können das Gerät als Proxy benutzen und dann nur den Webtraffic über die Trutzbox filtern. Im transparenten Modus hingegen wird der gesamte Netzwerktraffic durch das Gerät geleitet. So können auch IoT-Geräte ohne eigene Konfigurationen gefiltert werden.

Proxys in Kaskaden

Die Daten werden über sogenannte Mixkaskaden versendet. Dabei werden mehrere Proxys hintereinandergeschaltet und zusätzlich die Daten unterschiedlicher Herkunft miteinander vermischt. Sie werden auch als Mixnetzwerk mit kaskadierenden Proxy-Servern bezeichnet. Jede Proxy-Station kennt nur den vorherigen Server, von dem die Daten kommen, und denjenigen Proxy-Server, an den die Daten weitergereicht werden. Zwischen jeder Station werden die Daten gesondert verschlüsselt.

Nutzer können die Funktionen der Trutzbox für verschiedene Seiten deaktivieren. Anders als beim Eblocker ist jedoch keine Blacklist von Seiten hinterlegt, bei denen das Gerät nicht in den SSL-Traffic hineinschaut.

Trutzbox bietet einen lokalen Mailserver

Darüber hinaus kann das Gerät als Mailserver verwendet werden. Mails zwischen verschiedenen Trutzbox-Nutzern werden Ende-zu-Ende verschlüsselt, ein zentraler Mailserver ist dabei nicht involviert. Stattdessen liegen alle notwendigen Informationen auf den jeweiligen Geräten der Nutzer vor. Nach Angaben der Herstellerfirma Comidio sind dabei auch die Metadaten verschlüsselt. Je nach verfügbarem Speicherplatz können prinzipiell beliebig viele

E-Mail-Accounts erstellt werden. Im Preis enthalten sind jedoch maximal fünf Trutzmail-Adressen, jede weitere kostet 12 Euro pro Jahr und kann nach Erwerb des Gerätes hinzugekauft werden.

Sollen Mails auch über das Internet ausgetauscht werden, muss das Gerät entweder eine feste IP-Adresse bekommen, was allerdings in den wenigsten Privathaushalten der Fall sein dürfte. Alternativ muss dann ein Dienst wie DynDNS genutzt werden, um das Gerät dauerhaft von außen ansprechen zu können. Eine detaillierte Anleitung zur Einrichtung dieser Funktion befindet sich im Online-Handbuch der Trutzbox. Auch die Trutzbox integriert den Virenscanner ClamAV, den Nutzer aber auch hier getrost ignorieren können. Einen zuverlässigen Schutz vor Viren und Trojanern bietet die Software nicht, daher sollte sie am besten ganz deaktiviert werden.

Bastelversion ist in Planung

Im Gespräch mit Golem.de sagte Comidio-Geschäftsführer Sauer, dass in Zukunft möglicherweise auch eine Bastelversion der Trutzbox angeboten werden könnte. Dann könnten Nutzer einen selbst angeschafften Raspberry Pi oder Banana Pi nutzen und müssten nur das Dienstleistungspaket erwerben. Hier müssten aber im Vergleich zur derzeitigen Lösung Abstriche bei der Leistung gemacht werden, mehrere parallele Videokonferenzen etwa dürften einen Bastelrechner überfordern. Wer aber nur die Anonymisierungsfunktionen nutzen will, für den könnte das eine interessante Lösung sein. Einen konkreten Zeitplan dafür gibt es aber bislang nicht.

Dank der leistungsfähigen Hardware und der sehr umfangreichen Dokumentation überzeugt uns das Gerät. Der Preis ist mit 299 Euro jedoch auch höher als bei den anderen Geräten - das liegt vor allem an der verwendeten Hardware. Nach Ablauf des ersten Jahres kosten die Trutz-Services 5 Euro im Monat. Wer alle Funktionen der Trutzbox tatsächlich nutzt, für den könnte sich eine Anschaffung lohnen. Wer sich dafür entscheidet, muss jedoch etwas Geduld mitbringen: Die Lieferzeit wird im Webshop mit drei bis vier Wochen angegeben.

Relaxbox

Die Relaxbox stammt von einem kleinen Berliner Startup, die erste Charge wurde über Crowdfunding finanziert. Das System soll die Privatsphäre der Nutzer verbessern und außerdem vor Viren schützen. Wir haben ein Vorabmodell aus dem Crowdfunding getestet, das in der Redaktion vorhanden war. Die Auslieferung der Serienmodelle soll Ende April beginnen.

Das Gerät basiert auf der Haplite-Plattform und dem damit ausgelieferten Router-OS der Firma Mikrotek, einem Linux-Derivat. Die Qualcomm-CPU taktet mit 650 MHz und bietet nur einen Kern. Der Arbeitsspeicher ist mit 32 MByte recht dürftig bemessen, der integrierte WLAN-Host funkt maximal mit N-WLAN-Geschwindigkeit. Die Relaxbox-Macher integrieren einen auf OpenVPN basierenden eigenen VPN-Dienst mit dem Virenscanner Clam AV sowie Googles Safe-Surf-API. So sollen Nutzer nicht nur vor der Identifizierung durch Webseitenbetreiber geschützt werden, sondern auch vor Viren und Trojanern.

Systembedingt kann dieser Virenschutz nur eingeschränkt funktionieren. Denn einerseits ist der Schutz nur auf Port 80 verfügbar - also beim normalen Websurfen - andererseits kann die Box mangels SSL-Zertifikat nicht in verschlüsselte Verbindungen hineinschauen. Darauf weist das System auch an verschiedenen Stellen hin. Unerfahrene Nutzer könnten sich trotzdem in falscher Sicherheit wähnen. Der Verzicht auf die Analyse von SSL-Verbindungen sei eine bewusste Design-Entscheidung, sagte der Pressesprecher des Unternehmens, Maximilian

Pohl, im Gespräch mit Golem.de: *"Wir wollen verschlüsselte Verbindungen gar nicht aufmachen können."* Auch die Integration von Googles Safe Browsing API bietet nur wenig zusätzlichen Schutz - und es gibt Probleme bei der Privatsphäre. Denn einerseits ist diese in moderne Webbrowser bereits integriert. Und andererseits überträgt eine frühere Version der API die aufgerufenen URLs im Klartext an Google. Erst mit der Version v3 der API werden die URLs vor der Übertragung gehasht.

Angaben zu VPN-Geschwindigkeit sind irreführend

Wenn die Relaxbox in den Handel kommt, wird es verschiedene Tarife geben: Free - damit werden maximal 1 MBit/s möglich. Im Basic-Tarif werden Surfgeschwindigkeiten von bis zu 10 MBit/s versprochen - für 6,99. Werbeblocker, Google Safe Browsing, Phishing-Schutz und Jugendschutzfilter sind jedoch erst im teuersten Tarif enthalten. Der Premium-Tarif kostet 10,99 im Monat und soll bis zu 30 MBit/s ermöglichen. Basic- und Premium-Tarif können auch ein Jahr im Voraus bezahlt werden, dann sinkt der Preis um einen beziehungsweise zwei Euro pro Monat.

Bereits beim Crowdfunding wurden verschiedene Stufen angeboten. Die VPN-Geschwindigkeit im teuersten Tarif wurde mit "Unbegrenzt" angegeben, was wir sehr missverständlich finden. Denn letztlich bedeutet das nur, dass die VPN-Geschwindigkeit vom Betreiber nicht künstlich gedrosselt wird. Darauf angesprochen sagt Pohl: *"Diese Angabe ist bei VPN-Betreibern Standard."*

Im Test ist die Geschwindigkeit des Crowdfunding-Modells noch sehr langsam. Mehr als 16 MBit erreichen wir zu keinem Zeitpunkt. Unser Tarif sollte aber eigentlich Geschwindigkeiten jenseits der 20 MBit ermöglichen. *"Die Geschwindigkeit ist eines der Dinge, die wir in Zukunft verbessern wollen"*, sagt Pohl. Mit den Crowdfunding-Nutzern habe man jetzt zahlreiche Erfahrungen gemacht, die in die weitere Entwicklung der Box fließen.

Ende April sollen die Crowdfunding-Nutzer ein Update erhalten, mit dem dann auch die Geschwindigkeit merklich verbessert werden soll. Im derzeit mit dem Gerät ausgelieferten Mini-Handbuch finden sich noch fehlerhafte URLs, die eigentlich auf AGB und Datenschutzbestimmungen verweisen sollen. Hier sollte noch einmal nachgebessert werden.

Die Werbeblocker-Funktionen waren bei unserem Gerät noch nicht aktiv. Tatsächlich betrachten die Macher das Feature auch eher als Addon, wie sie im Gespräch sagten. Für die Werbefreiheit soll im Endprodukt der Dienst Privoxy genutzt werden. Wir werden dann noch einmal Erfahrungen nachtragen.

Uns überzeugt das Gerät nicht. Neben dem Anschaffungspreis kommen vor allem mit dem Premium-Tarif recht hohe Kosten auf die Nutzer zu. Der Mehrwert gegenüber einem reinen VPN-Dienst ist dabei recht gering.

Fazit: Wir sind nicht überzeugt

Hat sich unsere ursprüngliche Skepsis nach der Befassung mit den Geräten gelegt? Nicht unbedingt. Bei den getesteten Geräten haben wir zwar keine peinlichen Sicherheitslücken wie offene SSH- oder Telnet-Ports gefunden.

Doch der Mehrwert der meisten Geräte ist relativ gering. Eine bloße Verschleierung der IP-Adresse bietet eben nicht, wie oft angenommen, eine komplette Anonymisierung, sondern lediglich eine Standortverschleierung. Ein guter VPN kann also vor Abmahnungen schützen, nicht aber vor Fingerprinting oder einer gezielten Überwachung. Wer damit zufrieden ist, kann

also einfach einen VPN nutzen. Mit einer Privacy-Box ließe sich ein solch leistungsfähiger VPN mit der Familie teilen. Doch bis auf die Trutzbox war die Verbindungsgeschwindigkeit über VPN sehr langsam. Wenn dann jemand in der Familie Netflix schauen will, müsste dafür der VPN ausgeschaltet - oder das Netzwerk gewechselt werden. Damit ist das fast so kompliziert, wie jeweils einen eigenen VPN-Zugang einzurichten.

Die Virenschutzfunktionen der Geräte sind aus unserer Sicht irreführend und weitgehend nutzlos. Sie sollten deaktiviert werden, um Sicherheitslücken durch Sicherheitssoftware zu vermeiden. Die eigene Sicherheit lässt sich deutlich besser erhöhen, indem unnötige Sicherheitslücken wie Flash- oder Java-Plugins vom Rechner entfernt werden. Googles Safe-Browsing-Funktion ist in ihrer aktuellen Version in gängigen Browsern vorhanden. Auch hier besteht also kein akuter Bedarf.

Die Trutzbox, die Relaxbox und die Upribox bauen jeweils eigene WLAN-Netzwerke auf, die dann privates Surfen gewährleisten sollen. Das ist einerseits praktisch, weil Nutzer die Funktionen zielgenau nutzen können, wenn sie beim Surfen ein Mehr an Privatsphäre wollen. Andererseits sind die verwendeten WLAN-Sticks nicht so schnell wie moderne Router, auch die Reichweite ist deutlich geringer. Mit ein bisschen Konfiguration lassen sich die Geräte aber auch in bestehende Netzwerke eingliedern.

Die Upribox ist derzeit noch ein Bastelprojekt mit einigen interessanten Features. Das Gerät erfordert wenig Konfiguration und ist eine solide Basis zum Experimentieren. Aus unserer Sicht ist die Box vor allem geeignet, um weniger IT-affine Freunde und Verwandte mit mehr Privatsphäre auszustatten. An der Geschwindigkeit muss aber noch gearbeitet werden.

Die Konfiguration des Eblockers ist sehr einfach, führte im Test aber auch zu Problemen mit komplexeren Netzwerkanwendungen. Die Anonymisierung über das Tor-Netzwerk muss erst zugeschaltet werden, was letztlich sinnvoll ist, wir aber etwas verwirrend fanden. Weil Tor beim Eblocker nur Port 80 anonymisiert, kann letztlich auch ein Tor-Browser verwendet werden, der zudem extra gehärtet ist und von Haus aus zahlreiche Privatsphäre-Features mitbringt. Interessant fanden wir die Funktion, den User-Agent mit einem Klick umzustellen.

Die Trutzbox liefert Hardware mit Leistungsreserven und ein vollständiges Debian-System, dafür kostet das Gerät aber auch etwas mehr. Nutzer können mit etwas Erfahrung selbst NAS-Funktionen umsetzen oder Dienste wie Owncloud installieren. Außerdem bietet das Gerät einen eigenen Mailserver und bald auch einen WebRTC-Server, den wir bereits ausprobieren konnten. Wer den vollen Umfang des Gerätes nutzt, für den könnte sich die Anschaffung lohnen. Grundsätzlich sollten sich alle .deb-Pakete installieren lassen.

Die Relaxbox war in unserem Test noch deutlich zu langsam, Surfvergnügen kam so nicht auf. Der Mehrwert gegenüber einem guten VPN ist gering, gerade weil einige VPN-Dienste auch ohne extra Hardware Werbeblocker und Virenschutz implementieren. Es bleibt abzuwarten, ob das Update für die Verkaufsversion die Probleme behebt. (hg)

Verwandte Artikel:
Datenweitergabe an Regierung: Reddits Kanarienvogel hat ausgezwitschert
(01.04.2016, http://glm.io/120093)
EU-Parlament: Schrödingers Datenschutz beschlossen
(14.04.2016, http://glm.io/120330)
Microsoft: Edge folgt Chrome im Kampf gegen Flash-Werbung
(08.04.2016, http://glm.io/120226)
Adblock Plus: Deutschlands heimliche Werbemacht
(04.07.2013, http://glm.io/100198)

Kostenfreie SSL-Zertifikate: Let's Encrypt ist nicht mehr Beta
(14.04.2016, http://glm.io/120322)
