Mehr Privatsphäre mit Fritzboxen

FritzOS 7.20 schützt VoIP-Telefonie, WLAN und Surf-Daten

Bild: Andreas Martini

Lange Zeit war lediglich bekannt, wie vielfältig die Privatsphäre von Nutzern ausgespäht werden kann. Nun mehren sich aber die Gegenmittel. In aktuellen Fritzboxen lassen sich drei wichtige besonders einfach aktivieren.

Von Dušan Živadinović

Seine Privatsphäre muss man selbst verteidigen, Konzerne und der Staat haben daran naturgemäß kein Interesse. Das ist soweit nichts Neues. Wie Sie Ihre PCs, Smartphones und andere Geräte ohne viel Aufwand konfigurieren, damit sie einen minimalen Fußabdruck im Internet hinterlassen, haben wir beispielsweise in c't 13/2020 zusammengefasst.

Doch für manche Lücken materialisieren sich die Gegenmittel nur verzögert. Beispielsweise ist die Telefonie per Voice over IP seit jeher ungeschützt. Obwohl erste Verschlüsselungen schon Anfang der 2000er-Jahre spezifiziert worden sind, ließen Provider, Telefon-, Tk-Anlagen- und Routerhersteller sie fast zwei Jahrzehnte lang links liegen. Derweil haben Messenger mit VoIP-Funktion davon profitiert. Signal, Wire, WhatsApp, iMessage und andere verschlüsseln Ende-zu-Ende und der Nutzer muss nicht einen Finger dafür rühren.

VoIP-Telefonie schützen

Höchste Zeit also, dass mit der Telekom ein großer Player im Markt wenigstens eine der vielen Methoden aufgreift und Routerhersteller wie AVM, Lancom oder Bintec-elmeg mitzieht. Denn Messenger sind nicht interoperabel und heute noch weniger verbreitet als Festnetztelefone.

Doch übliche VoIP-Gespräche, die auch grenzüberschreitend laufen können, lassen sich leicht massenhaft abhören, auch von fremden Nachrichtendiensten. Nicht zu vergessen die blank in den Hausverteilern zusammenlaufenden Telefonkabel: An Hausverteilern, die oft unbeachtet in Kellern stehen oder gar außen an Gebäuden, können Angreifer mit Notebook und DSL-Analysator oft unbehelligt alles mitschneiden, was über die DSL-Leitungen ins Internet geht. Und es soll ja Firmen geben, in denen man sich Passwörter oder auch Kreditkartendaten telefonisch durchgibt.

Die Geräteentwickler haben es allerdings nicht immer leicht, die Spezifikationen zur VoIP-Verschlüsselung umzusetzen. An manchen Stellen sind die Schriften zu knapp oder sie überlassen die genaue Implementierung dem Gespür der Programmierer. Das geht nicht immer gut und so haben wir auch für die Fritzbox Verbesserungsvorschläge. Unterm Strich muss man aber sagen: Der Einstieg in die VoIP-Verschlüsselung ist gelungen, auch wenn der hiesige Branchenprimus AVM zu wünschen übrig gelassen hat. Einzelheiten dazu finden Sie im Beitrag ab Seite 18.

WLAN absichern

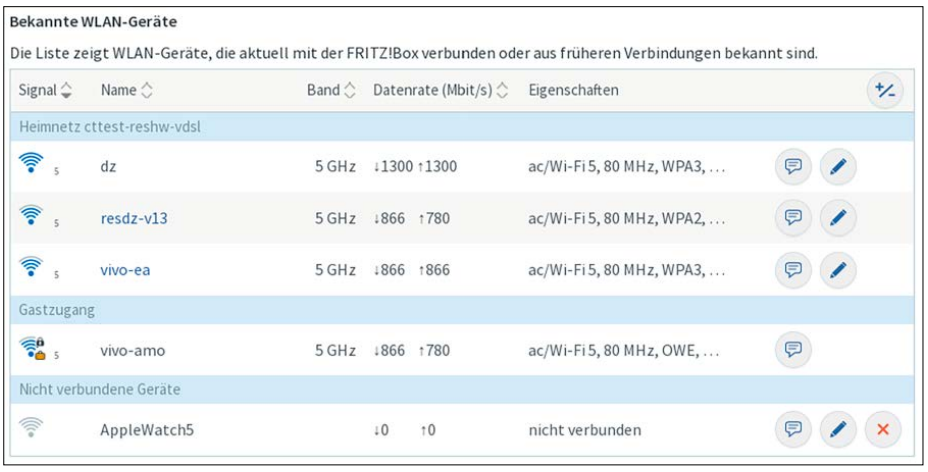
Manche Sicherheitstechnik bekommt im Laufe der Zeit Risse. Bei der WLAN-Verschlüsselung kennt man das schon zur Genüge: Mit WEP und WPA sind schon zwei Methoden gekommen und (hoffentlich rückstandslos) gegangen. Nun sollte man für die dritte Methode, das aktuelle WPA2, den Abschied einläuten.

Zwar ist WPA2 nicht so grundlegend löchrig wie die WLAN-Steinzeittechnik WEP: WPA2-geschützte Funknetze lassen sich bisher nur über hartnäckiges Ausprobieren knacken (Brute Force). Aber Hochrechnungen, laut denen ein erwürfeltes 16-stelliges Passwort dem stumpfen Ausprobieren rund 19 Billionen Jahre lang standhalten soll, sind nun mal Hochrechnungen. Zudem gehen sie von aktuellen Methoden und aktueller Hardware aus. Doch WPA2 fehlt der Vertraulichkeitsschutz Perfect Forward Secrecy (PFS). Deshalb muss eine Attacke nicht zur Laufzeit des angegriffenen WLANs abgeschlossen sein, sondern kann auch aufgezeichnete Daten aufdecken. Falls man in einigen Jahren Quanten-Computer darauf ansetzen kann, sind Angreifer vermutlich weit schneller am Ziel als heute prognostiziert.

Je eher Sie auf das bereits verfügbare WPA3 umsteigen desto besser. Die neue WLAN-Verschlüsselung ist zwar beileibe nicht perfekt. Aber zum Beispiel ist anders als bei WPA2 für jede Passworteingabe ein neuer Verbindungsversuch erforderlich, sodass sich automatisierte Brute-Force-Angriffe auf eine WLAN-Basis derart in die Länge ziehen, dass sie aussichtslos sind. Zudem werten die Basisstationen zu viele misslungene Einbuchungsversuche als Angriffe und zögern ihre Antworten dann hinaus. Was WPA3 im Detail bringt, wie Sie es in Fritzboxen aktivieren und wie aktuelle Geräte im Test abschneiden, lesen Sie ab Seite 26.

DNS-Leckage stopfen

Für manche Privatsphären-Lecks müssen Gegenmittel komplett neu entwickelt und implementiert werden. Dazu zählt die



Stellt man aktuelle Fritzboxen auf das moderne WPA3 um, erhöht das die Sicherheit erheblich. WLAN-Clients, die sich nicht aufrüsten lassen, können weiterhin WPA2 verwenden.

Verschlüsselung der Kommunikation mit DNS-Resolvern, den „Telefonbüchern des Internet“. Denn alle Geräte sprechen Server im Internet anhand ihrer IP-Adresse an, die sie von Resolvern hauptsächlich im Klartext abfragen. Als die Technik Mitte der 1980er-Jahre entstand, hatte kein Entwickler auf dem Zettel, dass man anhand von DNS-Anfragen Nutzerprofile erstellen könnte. Auch kam später manche DNS-Erweiterung hinzu, die anderen Zwecken dienen sollte, aber nebenbei User-Tracking ermöglicht.

Dazu zählt insbesondere die Methode, mit der Provider die Betreiber von Content Delivery Networks (CDNs) informieren, wo auf der Welt sich der anfragende Client befindet (Geolocation). Damit können sie den Client zum nächstgelegenen Rechenzentrum leiten, was die Paketlaufzeit verkürzt (EDNS0-Option: edns-client-subnet, ECS). Große Content-Anbieter wie Apple, Microsoft oder Netflix nutzen CDNs, um Weitverkehrsstrecken zu entlasten. Daher ist ECS grundsätzlich von Vorteil.

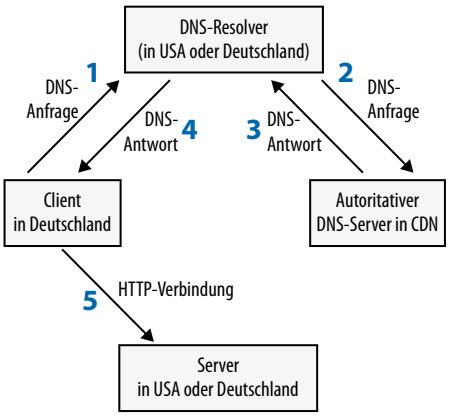
Aber um Kinderschutzfilter zu implementieren, markieren Provider DNS-Anfragen vor der Weiterleitung – und auf den Strecken zu den Root-Server und zum autoritativen Server können die Anfragen Dritte lesen (zum Beispiel am weltgrößten Internet-Drehkreuz DE-CIX in Frankfurt). Auch dagegen ist erst mal nichts einzuwenden. Man kann zum Markieren Hashes nutzen oder andere Merkmale, die keinem User direkt zugeordnet werden können.

User-Tracking geschenkt

Doch manche Provider nutzen die MAC-Adresse, den Usernamen oder andere Daten, die eine Identifizierung (Fingerprinting) hinter einem Router leicht machen. Wenn Lauscher diese Daten mit dem HTTP(S)-Verkehr korrelieren, sehen sie, welche Seiten Sie sich in der Freizeit ansehen und welche, wenn Sie beruflich aktiv sind.

Anhand solcher tageszeit- und wochentagabhängigen Profile lässt sich ein User sowohl auf Desktop- als auch auf Mobilgeräten identifizieren. So lässt sich grob ableiten, wo sich ein User gerade befindet (zu Hause oder unterwegs). Einzelheiten dazu finden Sie über ct.de/yxkt im RFC 7626 sowie in einem Vortrag der Sicherheitsspezialistin Sara Dickinson.

Die Internet Engineering Task Force kommentiert die Situation so: Die weitaus meisten Webseiten sind zwar öffentlich (anonyme Alkoholiker, BitTorrent-Tracker, Suchmaschinen, Beratungsseiten etc.), aber die Daten darüber, wer welche Webseiten besucht, sollten weder öffentlich sein noch gesammelt werden können. Daher entwickelte die Organisation Verschlüsselungsmethoden für DNS-Abfragen: DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT). Beide schützen die Privatsphäre nur bis zum Resolver und verhindern den Datenabfluss über die ECS-Technik nicht. Aber wer einen nicht-protokollierenden Resolver nutzt, kann einer Resolver-Petze entgehen. AVM baut in seine Fritzboxen DoT ein. Wie man die Technik aktiviert und wie gut sie im Test funktionierte, lesen Sie ab Seite 22.



Vom konfigurierten DNS-Resolver hängt wesentlich ab, welches Rechenzentrum etwa einen angefragten Netflix-Stream liefert und damit auch die Länge der Übertragungsstrecke. Leider plappern manche Resolver private Daten aus.

Jedoch ist AVM nicht der erste Hersteller, der DoT in Routern integriert. Beispielsweise bringt das Router-Betriebssystem pfSense DoT seit 2018 mit. Auch die Turris-Router der tschechischen Registry CZ.NIC, das freie Routerbetriebssystem OpenWrt und die Firewall-Distribution IPFire können DNS-Anfragen verschlüsseln.

Was DoT nicht macht

DoT ist ein wichtiger Baustein beim Schutz der Privatsphäre, aber nur einer von vielen. Die Technik verschlüsselt nur die Strecke vom Client zum Resolver. Der Resolver löst den Namen der angefragten Domain weiterhin im Klartext auf (er kommuniziert unverschlüsselt mit DNS-Root-Servern und autoritativen Servern).

Wer also den Verkehr eines Resolvers langfristig erfasst, kann im Datenstrom der vielen Nutzer, die diesen Resolver verwenden, vermutlich unterschiedliche Profile erkennen. Fachleute meinen, es sei nicht Privacy-relevant, ob zum Beispiel irgendein Telekom-Kunde die Webseite der Deutschen Aids-Hilfe besuchen wollte. Trotzdem gibt es Pläne, die restliche DNS-Kommunikation abzusichern.

DNS-Ratschläge

Über die DNS-Verschlüsselung hinaus hilft eine Handvoll einfacher Faustregeln, die Privatsphäre zu verbessern.

Meiden Sie kommerzielle VPN-Dienste. VPN-Anbieter betreiben eigene DNS-Server, um Kunden den Zugang zu Diensten zu ermöglichen, die ihnen das Geo-Blocking normalerweise vorenthält. Jedoch verrät man dabei seine Internet-Ziele dem VPN-Betreiber. Prinzipiell kann er diese Kenntnisse zu Geld machen, etwa durch Verkauf von Profilen an Werbetreibende.

Welchen DNS-Server Ihr aktuelles Gerät gerade benutzt (Smartphone, PC, Tablet, Smart-TV), verrät beispielsweise die Testseite Browserleaks (siehe ct.de/yxkt). Dort stehen im Bereich „DNS Leak Test“ die IP-Adressen der genutzten DNS-Resolver. Vor allem VPN-Anbieter unterhalten Webdienste zur DNS-Analyse, darunter „DNS leak test“ oder „Perfect Privacy“. Damit lässt sich prüfen, welche DNS-Informationen Streaming-Anbietern wie Netflix vorliegen, um etwa länderspezifische Zugänge zu ihren Videoangeboten durchzusetzen.

Prüfen Sie ab und zu, welchen Resolver Ihre Geräte befragen, denn es gab schon etliche Attacken auf Router, um darin den DNS-Server umzubiegen. Angreifer können so mitlesen, wer was tut oder DNS-Anfragen auf Werbeseiten umlenken, die für sie lukrativ sind – oder gleich Malware wie Erpressungstrojaner in den Browser schleusen.

Um Attacken auf Router möglichst kleine Angriffsflächen zu bieten, halten Sie deren Firmware aktuell. Sichern Sie das Webinterface mit einem individuellen, möglichst langen Passwort aus Groß-, Kleinbuchstaben und Sonderzeichen, schalten Sie Zugriffe aus dem Internet auf das Webinterface ab, nutzen Sie für die Fernwartung ein VPN. Verwenden Sie für das WLAN ein anderes, gleichfalls langes Passwort. Verweisen Sie Geräte von Besuchern ins Gastnetz. Bleibt uns noch eins für Ihre Internet-Surf-Unternehmungen zu wünschen: Mast- und Schotbruch!

(dz@ct.de) **ct**

Weitere Infos: ***ct.de/yxkt***