Security Awareness

Privatsphäre im Internet und Konfiguration eines Pi-hole in einem Heimnetzwerk

Markus Becht

12. Juli 2020

Abstract

Dieses Paper behandelt die Konfiguration eines Pi-holes im Heimnetzwerk zum Schutz der Privatsphäre im Internet. Es wird darauf eingegangen wie Werbung zur Manipulation und Bewertung von Menschen dient. Anschließend werden Maßnahmen zum Schutz vor Tracking beschrieben. Der Einsatz von Ad Blockern und VPNs schützt die Privatsphäre. Im Praxisbeispiel wird auf die Konfigruation eines Pi-holes im Heimnetzwerk eingegangen, damit Werbung zentral auf jedem Gerät gefiltert und blockiert wird.

Einleitung

Am 20.03.2020 wurde in Bayern aufgrund der COVID-19-Pandemie eine Ausgangsbeschränkung verhängt. Zur Eindämmung des Coronavirus wurde viel über die Corona-Warn-App diskutiert. Die App soll durch Übertragung von Standortdaten von Smartphones zur schnellen Nachverfolgung von Infektionsketten dienen. Das klare Ziel dabei ist, dass Menschen die mit infizierten Personen in Kontakt gekommen sind, schnell zu benachrichtigen, damit sie sich testen lassen können und sich bei einem positiven Testergebnis in Quarantäne begeben können. So könnten Infektionsketten schneller identifiziert und unterbrochen werden. Kritik an den GPS-Daten des Mobilfunks findet sich darin, dass die Standortdaten viel zu ungenau für den Infektionsradius sind. Die Menschen können sich in U-Bahnen und mehrstöckigen Häusern nicht nur nebeneinander, sondern auch übereinander aufhalten. Die Standortdaten erfassen auch nicht geteilte Standorte, wenn sich Menschen nebeneinander befinden, aber durch eine Wand getrennt sind. Als Lösung kommt die Bluetooth-Technologie in betracht, deren eigentliche Schwäche in diesem Fall zu einer Stärke wird. Mit der geringen Reichweite von bis zu 10 Metern können Handydaten der Menschen ausgetauscht werden, denen man zu nahe gekommen ist. Durch den Austausch der Daten entstehen Zweifel am Datenschutz. Beim Datenaustausch werden Aufenthaltsorte der Personen veröffentlicht, was

zur Preisgabe sensibler Informationen führt. Was folgte, war eine deutschlandweite Diskussion, ob die Corona-Tracking-App einen massiven Eingriff in die Grundrechte bedeutet. Durch die aufgekommene Diskussion stellt sich die Frage, wie man die Privatsphäre im Internet schützen kann. Ziel dieser Arbeit ist es mit einfachen Möglichkeiten Zuhause werbefrei im Internet surfen zu können.

Im ersten Abschnitt des Papers werden die Grundlagen zum Thema Tracking erläutert. Im Hauptteil wird am Praxisbeispiel die Konfiguration eines Pi-Holes gezeigt. Zum Schluss wird noch ein Ausblick und eine Conclusion zum Thema abgegeben.

Anonymität im Internet

In diesem Paper geht es nicht darum, welche Werbung angezeigt wird, sondern wie die „Werbung“ genutzt wird, um Aktivitäten im Internet zu beobachten. Diese Informationen werden gesammelt, um Menschen auszuspionieren und manipulieren zu können. Das Sammeln der Informationen wird mit sogenannten Tracking-programmen bzw. Verfolgerprogrammen realisiert. [6]
Manipulation durch Werbung wird verwendet, um an Zielgruppen angepasste Werbung zu erhalten. Die Werbung könnte so geschalten sein, dass verfolgt werden kann, wie etwas angeschaut wird oder welchen Preis die Ware hat. Anschließend tauchen immer wieder Vorschläge zu ähnlichen Produkten mit ähnlichen Preisen auf. Manipulation kann auch im Bereich Wahlen und Meinungen eingesetzt werden. Hier kann durch Tracking herausgefunden werden, wie ein Mensch tickt. Dieser erhält dann bevorzugt Nachrichten und Werbung zu diesen Meinungen und Charaktereigenschaften, was Menschen beeinflussen kann. [8]
Neben der Manipulation können die gesammelten Daten auch zur Bewertung der Menschen dienen. Aufgrund des Surfverhaltens können Informationen z. B. zur Bewertung des Gesundheitszustandes oder der Kreditwürdigkeit bestimmt werden.
Um Manipulationen und Bewertungen durch Werbung zu entgehen, ist es wichtig keine digitalen Fußspuren im Internet zu hinterlassen. Dadurch können keine Informationen gesammelt werden. In diesem Bericht wird Werbung als Synonym für Trackersoftware bzw. Verfolgerprogramme verwendet.

Ein erster Schritt zum Schutz der Privatsphäre ist die Nutzung eines Browser-Plugins. Ad Blocker wie μBlock Origin sind effizient bei der Eliminierung von Werbung und Trackerprogrammen. Sie filtern und blockieren Webinhalte und schützen so die Privatsphäre. Obwohl μBlock Origin für die gängigen Browser wie Chrome, Firefox und Safari installiert werden kann, können diese nicht auf Smart-TVs oder internetfähige Receiver installiert werden. [7] Soll auch auf diesen Geräten das Tracking eliminiert werden, wird eine übergeordnete Lösung benötigt. Diese Lösung bietet die Konfiguration eines Pi-holes im Heimnetzwerk.

Es ist wichtig zu verstehen, wie die Datenübertragung im Netzwerk funktioniert.
Durch den Aufruf einer Internetseite im Browser sendet der PC die Internetadresse an einen Domain Name Service (DNS). Der DNS wandelt den Namen in die IP-Adresse um. Danach findet erst der Datenaustausch zwischen Computer und Webserver statt.
Ist auf der Internetseite Trackersoftware eingebunden, müssen diese Tracker nachgeladen werden. D. h. die Namen der Tracker

werden an einen DNS geschickt und in IP-Adressen aufgelöst. Anschließend werden die Tracker nachgeladen und der Computer kommuniziert mit dem Tracker.

Die Idee hinter der Konfiguration eines Pi-holes ist den DNS zu konfigurieren. Er erkennt, ob die eingehende Adresse eine Trackingadresse ist oder nicht. Falls es eine Trackingadresse ist, wird diese gefiltert und blockiert. Dadurch kann verhindert werden, dass Werbung auf dem Computer angezeigt wird.

In jedem Heimnetzwerk gibt es einen DNS-Server, den alle internetfähigen Geräte mitgeteilt bekommen. Erst dann kann Datenaustausch stattfinden. In den meisten Fällen ist der DNS-Server gleichzeitig der Router im Heimnetzwerk. Die Idee der Implementierung eines Pi-holes ist die Ergänzung eines weiteren DNS-Service, der alle Anfragen bekommt und prüft, ob die Adressen blockiert werden sollen oder die Anfragen weitergeleitet werden können. Der Ablauf nach Konfiguration des Service ist wie folgt: Das Gerät möchte eine Internetseite aufrufen. Der Name der Seite wird an den DNS-Server gesendet und dieser liefert die IP-Adresse zurück. Nach der Konfiguration des Pi-holes versucht das Gerät den DNS-Server zu erreichen und wird auf das Pi-hole umgeleitet. Dort findet die Überprüfung der Adresse statt, sodass Werbung gefiltert und blockiert wird und der Rest der Seite normal genutzt werden kann. Sobald der Router so konfiguriert ist, dass die Namensauflösung auf dem Raspberry Pi erfolgt, muss der DNS-Server nicht auf allen Geräten einzeln hinterlegt werden Alle Anfragen der Geräte im Netzwerk werden automatisch an das Pi-hole umgeleitet. Somit können auch Smart-TVs, Internetradios und weitere netzwerkfähigen Geräte vor Tracking geschützt werden.

Eine weitere Möglichkeit zum Schutz vor Tracking ist der Einsatz von Virtual Private Networks (VPNs). Sie werden verwendet um die Daten bei der Kommunikation zu verschlüsseln. Die meisten Router bieten die Funktion zur kostenlosen Konfiguration eines VPNs. Sobald man außer Haus ist, kann sich das Genutzte Geräte mit dem VPN des Routers im Heimnetzwerk verbinden. Beim Aufruf einer Internetseite wird zunächst eine verschlüsselte Verbindung mit dem Router im Heimnetzwerk aufgebaut. Da auf diesen Router eine DNS-Umleitung zum Pi-hole konfiguriert ist, werden die Daten über den Raspberry Pi geleitet und gefiltert. So lässt sich das Tracking auch für unterwegs verhindern.

Konfiguration des Pi-holes auf einem Raspberry Pi

Für die Installation des Pi-holes wird ein Gerät mit 512 MB Arbeitsspeicher und ein entsprechendes Unix-Betriebssystem benötigt. [4] Da die Installation des Pi-holes nicht viel Speicherplatz benötigt, kann das Pi-hole auf nahezu jedem Raspberry Pi mit einer Micro SD-Speicherkarte installiert werden. Im Folgenden wird ein Raspberry Pi 3B+ mit einer 32 GB SD-Speicherkarte zur Installation und Konfiguration verwendet.
Bevor die Installation des Pi-holes durchgeführt werden kann, muss zunächst das Betriebssystem für den Raspberry Pi auf die SD-Karte installiert werden. Dafür wurde das aktuellste von der Raspberry Pi-Organisation bereitgestellte Raspberry Pi OS (32-bit) Lite Betriebssystem vom Mai 2020 auf einem Windows 10-Laptop mit SD-Speicherkarten-Slot heruntergeladen. [5]

Mittels ETCHER wurde das Betriebssystem-Image auf die SD-Karte übertragen. [1] Damit kein Monitor zur Konfiguration des Raspberry Pis benötigt wird, muss SSH aktiviert werden. Dabei wurde ins Boot-Verzeichnis der SD-Karte eine leere Datei ohne Dateiendung mit dem Namen „ssh“ erstellt. Anschließend konnte die SD-Karte in den Raspberry Pi eingesetzt und der Pi mit einem USB-Netzteil gestartet werden. Um die IP-Adresse des Raspberry Pis zu erhalten, wurde sich mit der FRITZ!BOX 6591 CABLE von AVM verbunden und dort nach dem Hostnamen „raspberrypi“ gefiltert. So heißt der Raspberry Pi standardmäßig. Ebenso ist der Benutzername „pi“ und das Passwort „raspberry“ voreingestellt. Damit der Raspberry Pi bei einem Neustart nicht jedes Mal eine neue IP-Adresse erhält, wurde dem Gerät über die FRITZ!BOX eine feste IP-Adresse zugewiesen, die der Raspberry Pi beim nächsten Neustart erhält.
Als nächstes konnte die Grundkonfiguration des Raspberry Pis durchgeführt werden, nachdem man sich mit Hilfe der Powershell auf den Raspberry Pi aufgeschalten hatte. Damit der Service SSH immer automatisch beim Booten des Raspberry Pis gestartet wird, wurde auf der Konsole folgender Befehl ausgeführt:

```
sudo update-rc.d ssh defaults
```

Die Grundkonfiguration erfolgt durch den Aufruf eines Konfigurationstools mit dem Befehl:

```
sudo raspi-config
```

Hier können verschiedene Optionen gewählt werden und dadurch kann z. B. das Standardpasswort des Benutzers, der Hostname, die Bootoptionen, Sprache, Zeitzone, Tastaturlayout und vieles mehr auf die entsprechenden Wünsche eingestellt werden. Nachdem zum Schluss die Software des Rasperry Pis aktualisiert wurde, kann der Raspberry Pi neu gestartet werden.
Die Installation des Pi-holes erfolgt mit folgendem Befehl: [3]

```
curl -sSL https://install.pi-hole.net | bash
```

Die Installation kann je nach Raspberry Pi und Internetverbindung einige Minuten dauern. Nach der Installation der Software startet ein Einrichtungsassistent automatisch.
Zunächst muss ein DNS-Anbier ausgewählt werden, welcher die Webanfragen auflöst. Hier kann man sich aus einer Reihe von vorgeschlagenen Anbietern entscheiden oder einen eigenen Anbieter eintragen. Aus den vorgeschlagenen Anbietern wurde der DNS-Server von CLOUDFLARE gewählt, da er einer der schnellsten DNS-Server weltweit ist. Dadurch das CLOUDFLARE keine IP-Adressen speichert und alle Logdateien nach 24 Stunden löscht, bietet der DNS-Dienstleister viel Schutz für die Privatsphäre. [9]
Anschließend werden einige Listen, die zur Filterung der Werbung im Internet verwendet werden, vom Assistenten vorgeschlagen. Nach Abschluss der Konfiguration können weitere Listen zur Webfilterung hinzugefügt werden. Alle von Pi-hole vorgeschlagenen Listen sollten zur Filterung verwendet werden.
Es sollte auch keine Änderung beim Filtern von IPv4- und IPv6-Adressen erfolgen. Diese sind beide standardmäßig aktiviert.
Nachdem in der Grundkonfiguration bereits die IP-Adresse des Raspberry Pis festgelegt wurde, können die Netzwerkeinstellungen bestätigt werden.
Anschließend können Einstellungen getroffen werden, ob auf dem

Raspberry Pi die DNS-Anfragen gespeichert werden und wie diese angezeigt werden. Lebt man nun in einer WG mit mehreren Personen im Haushalt sollten die Abfragen nicht gespeichert werden oder zumindest anonymisiert abgelegt werden. Im besten Fall sollten die Abfragen nicht aufgezeichnet werden. Die Personen sollten zumindest darüber informiert werden, wenn sich für die Variante der Speicherung der Log-Dateien entschieden wird.
Wenn die Daten geloggt werden, kann man interessante Erkenntnisse erlangen, wohin z. B. der Smart-TV oder ein mit dem Internet verbundener Receiver kommuniziert. Für den Anfang kann es daher sinnvoll sein, die Abfragen in die Logs zu speichern. Spätestens nachdem man den Netzwerkverkehr der Geräte analysiert hat, sollte die Funktion abgeschaltet werden.
Sobald die Einrichtung des Pi-holes abgeschlossen ist, wird ein Passwort für den Admin-Zugang zur Pi-hole Weboberfläche angezeigt. Dieses wird für den späteren Login an der Weboberfläche benötigt.
Im letzten Schritt der Konfiguration eines Pi-holes im Heimnetzwerk muss der Raspberry Pi als DNS-Server im Heimnetzwerk eingerichtet werden. Hier gibt es zwei Optionen: [2]

- DNS-Server auf der FRITZ!Box eintragen
- DNS-Server auf jedem Gerät eintragen

Da der Raspberry Pi im Heimnetzwerk als DNS-Server dienen soll, ist es am sinnvollsten die IPv4- und IPv6-Adressen des Raspberry Pis direkt an der FRITZ!Box einzutragen. Dadurch werden alle ausgehenden und eingehenden DNS-Anfragen automatisch an den Raspberry Pi weitergeleitet. Das Pi-hole filtert die Werbung.
Gibt es Geräte im Heimnetzwerk bei denen keine Werbung gefiltert werden soll oder ist die Funktion zur Einrichtung eines DNS-Servers auf dem Router im Heimnetzwerk nicht möglich, kann alternativ auf jedem einzelnen Gerät der DNS-Server manuell eingetragen werden. Wie das Funktioniert hängt von dem jeweiligen Betriebssystem ab. Diese Option ist nicht zu empfehlen, da viele Vorteile durch die Konfiguration des Pi-holes verloren gehen. In manchen Fällen gibt es keine andere Möglichkeit als den DNS-Server manuell an jedem netzwerkfähigen Gerät einzutragen. Manche Netzanbieter konfigurieren ihre Router so, dass kein DNS-Server eingetragen werden kann. Kauft man einen Router direkt bei einem solchen Anbieter gibt es keine Möglichkeit einen DNS-Server auf dem Gerät einzutragen und so eine automatische Weiterleitung an den Raspberry Pi zu konfigurieren. In diesem Fall bleibt nur die alternative Möglichkeit zur Eintragung des DNS-Servers auf jedem einzelnen Gerät.

Conclusion

Durch die Installation von Ad Blockern kann die Privatsphäre beim Surfen im Internet geschützt werden. Für den Schutz vor Werbung aller Geräte im Heimnetzwerk muss eine Weiterleitung des DNS-Servers auf den konfigurierten Raspberry Pi erfolgen. So werden alle Geräte, die mit dem Internet kommunizieren zentral vor Trackingsoftware geschützt, ohne jedes einzelne Gerät manuell konfigurieren zu müssen. Für zusätzlichen Schutz können beide Varianten genutzt werden. Die Ad Blocker und das Pi-hole arbeiten mit unterschiedlichen Datenbasen und ergänzen sich daher sehr gut. Durch den Einsatz von VPNs können die Daten nicht nur verschlüsselt werden, sondern die Funktion bi-

etet bei richtiger Konfiguration auch die Möglichkeit unterwegs Werbung zu filtern.

Index

Literatur

[1] Balena, Hrsg. *balenaEtcher - Flash OS images to SD cards & USB drives*. 2020. URL: https://www.balena.io/etcher/.

[2] Boris Hofferbert. „Pi-Hole auf dem Raspberry Pi einrichten - so geht's“. In: *heise Online* (3.4.2019). URL: https://www.heise.de/tipps-tricks/Pi-Hole-auf-dem-Raspberry-Pi-einrichten-so-geht-s-4358553.html.

[3] Pi-hole LLC, Hrsg. *Installation - Pi-hole documentation*. 2020. URL: https://docs.pi-hole.net/main/basic-install/.

[4] Pi-hole LLC, Hrsg. *Prerequisites*. 2020. URL: https://docs.pi-hole.net/main/prerequisites/.

[5] Raspberry Pi Foundation, Hrsg. *Download Raspberry Pi OS for Raspberry Pi*. 2020. URL: https://www.raspberrypi.org/downloads/raspberry-pi-os/.

[6] Jan Schallaböck. „Was ist und wie funktioniert Webtracking?“ In: *iRights - Kreativität und Urheberrecht in der digitalen Welt* (18.12.2019). URL: https://irights.info/artikel/was-ist-und-wie-funktioniert-webtracking/23386.

[7] *uBlock - A Fast and Efficient Ad Blocker. Easy on CPU and Memory*. 2020-07-12T09:02:01.000Z. URL: https://ublock.org/.

[8] *Werbung und Manipulation - wissenschaft.de*. 2020-07-12T08:32:51.000Z. URL: https://www.wissenschaft.de/gesellschaft-psychologie/werbung-und-manipulation/.

[9] Tilman Wittenhorst. „1.1.1.1: Cloudflare bietet datenschutzfreundlichen und schnellen DNS-Dienst“. In: *heise Online* (25.11.2018). URL: https://www.heise.de/newsticker/meldung/1-1-1-1-Cloudflare-bietet-datenschutzfreundlichen-und-schnellen-DNS-Dienst-4009673.html.