Befund: Datenleck

Datenverkehr von Medizin-Apps auswerten

Jetzt sind Sie gefragt: Überprüfen Sie den Datenverkehr der von Ihnen genutzten Gesundheits-Apps und melden Sie uns Auffälligkeiten. Gemeinsam können wir für einen besseren Umgang mit sensiblen Gesundheitsdaten sorgen.

Von Ronald Eikenberg

Stellen Sie sich vor, Sie sitzen bei Ihrem Hausarzt und berichten ihm, dass Sie gerade Verdauungsprobleme plagen. Der Arzt greift daraufhin zum Telefonhörer und ruft eine Analysefirma in den USA an, um Ihr Leiden zu Protokoll zu geben. Danach meldet er auch noch Facebook, bei welcher Krankenkasse Sie sind. Unvorstellbar? Nicht in der digitalen Welt. Ein vergleichbares Verhalten hatten wir bei der Analyse der Health-App Ada beobachtet (siehe ct.de/yuea). Die App versteht sich als Gesundheitshelferin und versucht, von den Symptomen ihres Nutzers auf die ursächliche Erkrankung zu schließen – also ungefähr so wie ein Hausarzt.

In puncto Datenschutz könnten die Unterschiede jedoch nicht größer sein: Während Ihr Hausarzt an die ärztliche Schweigepflicht gebunden ist, hat Ada das anscheinend nicht so eng gesehen. Nachdem wir unsere Analyse in der vorherigen c't veröffentlichten, erreichten uns zahlreiche Leserzuschriften. Es drängt sich der Verdacht auf, dass dieser Fall nur die Spitze des Eisbergs ist.

Da es inzwischen unzählige Gesundheits-Apps gibt und deren Nutzung teilweise spezielle Zugänge voraussetzt, etwa die Mitgliedschaft bei einer bestimmten Krankenkasse, können wir unmöglich alle selbst untersuchen. Deshalb zeigen wir Ihnen in diesem Artikel, wie wir bei der Analyse der Ada-App vorgegangen sind, damit Sie die von Ihnen genutzten Apps ebenfalls untersuchen können. Wenn Sie etwas Auffälliges entdecken, geben Sie uns gern Bescheid – wir gehen der Sache nach.

Datenprobe nehmen

Um herauszufinden, welche Daten eine App ins Internet funkt, schneiden Sie am besten den Datenverkehr mit. Das ist unter Android besonders einfach, Sie können hier eine App wie tPacketCapture installieren und einen Mitschnitt erstellen. Diesen werten Sie anschließend bequem am Rechner mit der Analyse-Software Wireshark aus. Alternativ können Sie den Mitschnitt auch mit einer Fritzbox erstellen. Dann haben Sie auch den Traffic von iOS-Geräten auf dem Schirm.

Der Nachteil daran ist, dass Sie keinen verschlüsselten Datenverkehr einsehen können – und die meisten Apps kommunizieren inzwischen chiffriert. Sie sehen also, dass Daten übertragen werden und wohin, aber nicht, was verschickt wird. Einen vollständigen Einblick erhalten Sie mit Apps wie Packet Capture oder HttpCanary für Android, die sich auch in TLS/SSL-verschlüsselten Datenverkehr einklinken. Das klappt allerdings nur bis einschließlich Android 6, da Sie ansonsten das zur Entschlüsselung des Datenverkehrs nötige Zertifikat nicht installieren können. Unter neueren Android-Versionen benötigen Sie dazu Root-Rechte, welche aber dazu führen, dass manche Apps den Start verweigern. Vielleicht finden Sie ja noch ein altes Smartphone oder Tablet mit Android 6 in der Schublade, das Sie zur Traffic-Analyse nutzen können. Alternativ können Sie auch einen Android-Emulator einsetzen. iOS-Nutzer greifen am besten zu TLS/SSL-Proxies wie mitmproxy oder Burp, die auf einem Rechner gestartet werden. Wir haben unter ct.de/yuea einige Praxisartikel zusammengestellt, in denen wir die einzelnen Analyseverfahren detailliert erklären. Sie können die Artikel gratis abrufen.

Um der Health-App Ada auf die Finger zu schauen, haben wir Packet Capture auf einem Android-6-Smartphone installiert. Da wir uns nur für den Datenverkehr der Ada-App interessierten, wiesen wir Packet Capture an, ausschließlich deren Datenverkehr zu erfassen. Dazu starteten wir die selektive Aufzeichnung über den grünen Play Knopf mit der Ziffer 1, der sich oben rechts im Hauptbildschirm von Packet Capture befindet. Daraufhin öffneten wir die Ada-App und bedienten sie wie ein gewöhnlicher Nutzer: Zunächst legten wir mit Hilfe eines Facebook-Accounts ein Ada-Profil an, anschließend tippten wir die gesundheitlichen Beschwerden ein, um die möglichen Ursachen von Ada zu erfahren. Wir gaben vor, Kunde der Barmer-Krankenkasse zu sein und an Herzrasen zu leiden. Danach öffneten wir wieder das Analyse-Tool Packet Capture und konnten einen Blick auf die von Ada übertragenen Daten werfen.

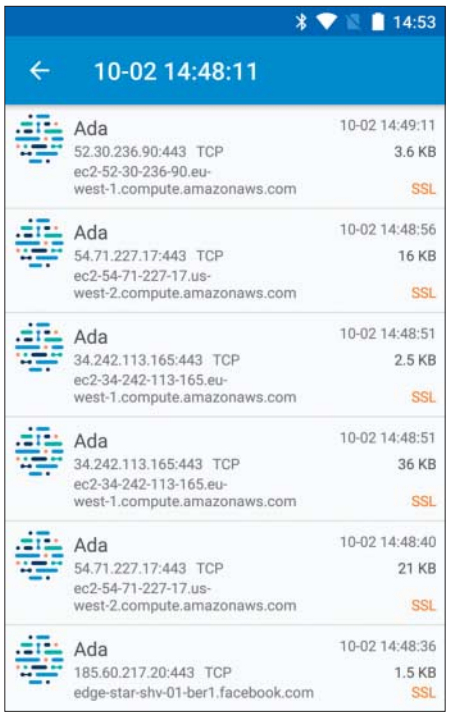
Laborbericht auswerten

Ada hatte laut einem der Protokolle mit den folgenden IP-Adressen über TLS/SSL (Port 443) kommuniziert:

```
185.60.217.20
54.71.227.17
34.242.113.165
52.30.236.90
```

Wer sich dahinter verbirgt, kann man anhand der Hostnamen erkennen, die Pa-

Was fehlt Ihnen denn? Der Nutzer unterhält sich mit Ada wie mit einem Hausarzt und gibt der App Details über seinen Gesundheitszustand preis.



Mit Packet Capture findet man schnell heraus, was Apps ins Internet funken – und wohin.

cket Capture in der Übersicht jeweils unter den IP-Adressen anzeigt:

```
185.60.217.20: edge-star-shv-01-ber1.facebook.com
54.71.227.17: ec2-54-71-227-17.us-west-2.compute.amazonaws.com
34.242.113.165: ec2-34-242-113-165.eu-west-1.compute.amazonaws.com
52.30.236.90: ec2-52-30-236-90.eu-west-1.compute.amazonaws.com
```

Die erste Adresse gehört anscheinend zu Facebook, die drei anderen zur Amazon Elastic Compute Cloud, die jedermann für seine Zwecke mieten kann. Die Amazon-Hostnamen unterscheiden sich im Detail, sie enthalten nämlich unterschiedliche Regionscodes (hier fett markiert), anhand derer man den Standort der Server ausmachen kann. „us-west-2“ steht laut Amazon für „USA West (Oregon)“, während „eu-west-1“ für „EU (Irland)“ steht.

Daten auf Reisen

Die Verbindung zu Facebook ist auf ersten Blick plausibel, schließlich hatten wir Facebook zur Anmeldung bei Ada genutzt. Hinter den IPs in der europäischen Amazon-Cloud steckt offenbar Ada selbst, wie die Detailansicht von Packet Capture zeigt. In den HTTP-Headerinformationen steht, dass die Ada-App bei den Verbindungen zu 34.242.113.165 den Host „prod-apigateway.adahealth.net“ angefragt hat. Beim Verbindungsaufbau mit 52.30.236.90 wollte Ada mit „prod-mh-26.adahealth.net“ sprechen. So weit, so unspektakulär – schließlich musste Ada die von uns eingetippten Daten ja irgendwie an sein Mutterschiff funken, um eine Meinung einzuholen.

Doch was ist mit den Datenpaketen, welche die App in die amerikanische Amazon-Wolke schickte? Bei den Verbindungen mit 54.71.227.17 hatte die App nach dem Host api.amplitude.com gefragt. Dahinter steckt der Analysedienst Amplitude mit Hauptsitz in San Francisco, Kalifornien. Das machte uns neugierig. Wir nahmen die an Amplitude verschickten Datenpakete unter die Lupe und entdeckten Erstaunliches: Denn Ada hatte nicht nur detaillierte Daten über unser Android-Smartphone an den US-Analysedienst geschickt, sondern auch konkrete Angaben, die den Nutzer und sogar dessen Gesundheit betreffen:

```
"query":"Herzrasen"
[...]
"profileSex":"MALE"
[...]
"profileAge":34
[...]
```

Laut den an den US-Dienst übertragenen Daten ist der Nutzer 34 Jahre alt, männlich und Kunde der Barmer-Krankenkasse. Zudem hatte der Nutzer nach „Herzrasen“ gesucht. Dass diese Daten notwendigerweise an den Hersteller übertragen wurden, ist die eine Sache, aber an das System einer Analysefirma mit Hauptsitz in San Francisco? An dieser Stelle könnte unsere Analyse eigentlich zu Ende sein, der Vollständigkeit halber schauten wir uns aber auch noch die Datenübertragung zu Facebook an. Es stellte sich heraus, dass die Ada-App die ausgewählte Krankenkasse auch an den Host graph.facebook.com gemeldet hatte. In einem anderen Mitschnitt konnten wir eine Übertragung von Geräteinformationen an ein System der Analysefirma Adjust beobachten. Auf deren Homepage wird man mit dem Slogan „Maximize the impact of your mobile marketing“ begrüßt.

Nachdem c’t den Anbieter der App mit dem Problem konfrontiert hatte, stritt dieser die Vorwürfe zunächst ab. Er veröffentlichte kurze Zeit später allerdings eine neue Version 2.49.1, in der die angemahnten Übertragungen nicht mehr auftauchten. Nachdem c’t schließlich ähnliche Übermittlungen beim Web-Interface von Ada aufdeckte, räumte der CSO und Mitbegründer von Ada Health, Dr. Martin Christian Hirsch, auf einer Podiumsdiskussion der Bundesärztekammer in Berlin Versäumnisse ein. Gegenüber c’t kündigte er an, die Datenschutzmängel abstellen zu wollen (siehe Seite 62).

Jetzt sind Sie am Zug!

Es deutet vieles daraufhin, dass Ada kein Einzelfall ist. Sie können aktiv dazu beitragen, Datenlecks aufzuspüren, die Sicherheit von Gesundheitsdaten zu verbessern und die Anbieter zum Umdenken zu bewegen. Überprüfen Sie auch die von Ihnen genutzten Health-Apps. Stoßen Sie dabei auf Auffälligkeiten wie Klartext-Datenübertragungen oder einen Informationsabfluss an Tracking-Firmen, teilen Sie dies gern mit uns! Am besten nutzen Sie dazu das Artikelforum unter ct.de/yuea.

Alternativ können Sie uns auch unter **ehealth@ct.de** kontaktieren. Wenn Sie uns anonym auf einen Missstand aufmerksam machen möchten, können Sie den Informanten-Briefkasten von heise Investigativ nutzen (siehe Kasten unten).

(rei@ct.de) c't

Analyse-Tools und Praxisartikel:
ct.de/yuea

heise Investigativ

Viele der c’t-Investigativ-Recherchen sind nur möglich dank Informationen, die Leser und Hinweisgeber direkt oder anonym an uns übermitteln.

Wenn Sie selbst Kenntnis von einem Missstand haben, von dem die Öffentlichkeit erfahren sollte, können Sie uns einen anonymen Hinweis oder brisantes Material zukommen lassen. Nutzen Sie dafür bitte unseren anonymen und sicheren Briefkasten.

https://heise.de/investigativ