Alexander Spier

Am offenen Herzen

Android aufbohren mit Xposed

Mit dem Xposed Framework kann sich jeder sein persönliches Android fürs Smartphone und Tablet basteln. So bekommen Sie die volle Kontrolle über Ihr Android und die eigenen Daten, ohne das Gerät mit alternativen Android-Versionen wie CyanogenMod zu flashen und alles neu zu installieren. Die Rückkehr zum Originalzustand ist schnell erledigt.

Alternative Android-ROMs sind an sich eine feine Sache. Sie helfen zum Beispiel beim Stromsparen, erlauben mehr Privatsphäre und lassen sich dem eigenen Geschmack umfangreich anpassen. Doch nicht für jedes Smartphone gibt es ein schönes und gut angepasstes ROM, die Installation erfordert viel Arbeit, und längst nicht jeden Zusatz braucht man dann im Alltag tatsächlich.

Das Xposed Framework ist da weniger umständlich: Es erlaubt, das bereits vorhandene Android vom Gerätehersteller an die eigenen Bedürfnisse anzupassen und einzelne Apps gezielt zu beeinflussen, und zwar zur Laufzeit, ohne dass die Software selbst dauerhaft verändert wird. Die meisten Änderungen wird man daher auch schnell wieder los: Deaktiviert oder löscht man Xposed, verhält sich das System wieder wie zuvor.

Es ist sogar auf den vielen exotischen Smartphones und Tablets einsetzbar, die gar nicht erst mit einem alternativen Android-ROM und einer aktiven Entwicklergemeinde gesegnet sind. Denn Treiber-Hickhack und das Warten auf angepasste Versionen für jedes Modell entfallen mit Xposed. Ob eine ARM- oder x86-CPU im Gerät stecken, ist egal.

Bisher läuft die Software mit Android bis Version 4.4 stabil, das daher hier im Mittelpunkt steht. Für Android 5 und die neue ART-Laufzeitumgebung gibt es erst eine frühe Alpha-Version, die in einigen Punkten abweicht und für den alltäglichen Einsatz noch nicht taugt. Für alte Geräte mit Android 2.3 (Gingerbread) gibt es Portierungen, allerdings nicht vom Xposed-Entwickler.

Das Xposed Framework selbst ist nur eine Grundlage, die Funktionen werden durch separate Module nachgerüstet. Diese kommen wie andere Android-Apps im APK-Format. Sie können über den Xposed Installer und teilweise den Play Store abgerufen werden. Solche Module schränken zum Beispiel bequem Zugriffsrechte für Programme ein, ändern das Aussehen der Oberfläche, bringen der Android-Mail-App PGP-Verschlüsselung bei oder erweitern die Möglichkeiten der Kamera-Software. Braucht man eine Anpassung nicht mehr, deaktiviert man das Modul einfach.

Um an die Android-Systeminnereien zu gelangen, benötigt eine App Root-Rechte, daran kommt auch Xposed nicht vorbei. Sie zu erlangen ist je nach Gerät unterschiedlich aufwendig, aber prinzipiell bei fast jedem Modell möglich [1]. Anleitungen und Tools findet man auch in einschlägigen Entwicklerforen wie xda-developers.com. Ein Backup persönlicher Daten vor dem Rooten und der Installation von Xposed ist ratsam. Denn bei beiden Aktionen besteht ein gewisses Risiko, dass das System danach nicht mehr startet und nur mühsam wieder lauffähig gemacht werden kann. Zudem muss man sich bewusst sein, dass viele Hersteller einmal gerooteten Geräten die Garantie verweigern.

Da Apps mit Root-Zugriff nahezu unbeschränkt im System schalten und walten könnten, benötigt man eine App, die diese Rechte selektiv gewährt. Viele Root-Tools installieren gleich das empfehlenswerte SuperSU, das es auch im Play Store gibt. Fordert eine App Root-Rechte an, kann man sie ihr damit dauerhaft oder nur vorübergehend gewähren.

Nun angelt man sich von der Entwicklerseite die APK-Datei für den Xposed Installer in der neusten stabilen Version (aktuell 2.6.1) und erlaubt in den Android-Einstellungen die Installation von Apps aus unbekannten Quellen. Beim ersten Start des Installers gewährt man ihm Superuser-Rechte. Hier passiert die eigentliche Einrichtung von Xposed: Hinter dem Menüpunkt „Framework" befindet sich der Button zum Installieren der nötigen Dateien, nach einem Android-Neustart ist das Xposed Framework aktiv. Die komplette Prozedur muss man nur einmal hinter sich bringen. Bei System-Updates reicht es, das Framework über den Installer erneut zu installieren, solange der Root-Zugriff weiter besteht.

Fallstricke

Auf populären Geräten wie dem Galaxy S5 und dem Nexus 4 hatten wir mit der Einrichtung der stabilen Version keine Probleme. Stark veränderte Android-Versionen und exotische Hardware bringen Xposed manchmal aus dem Tritt. So warnt die Software explizit vor Boot-Schleifen, also einem Hängenbleiben des Systems beim Start. Das gilt insbesondere für die mit Android 5 kompatible Alpha-Version 3.0.

Aus einer Boot-Schleife kann man sich unter Umständen befreien, indem man während der Startanimation alle Hardwaretasten einmal ausprobiert. Vibriert bei einer Taste das Gerät, gilt es, diese rasch vier weitere Male zu drücken, um Xposed zu deaktivieren – auch hilfreich, wenn man sich mit einem Modul selbst ausgesperrt hat. Über den herkömmlichen Recovery-Modus von Android kann das Smartphone nur komplett zurückgesetzt werden. Hilfreich ist es daher, vor dem Rooten noch ein Custom Recovery wie ClockworkMod oder TWRP zu flashen, die deutlich mehr Rettungsmöglichkeiten bieten. So kann man einfach eine Zip-Datei aufs Gerät flashen, die Xposed wieder entfernt. Diese Datei erstellt Xposed automatisch auf der SD-Karte und sie steht auch als Download bereit.

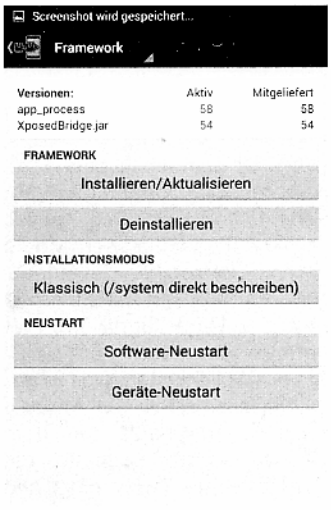
Auf einigen Geräten scheitert die Einrichtung von Xposed, wenn der System-Ordner schreibgeschützt ist. Mit Hilfe eines Custom Recovery klappt es eventuell trotzdem, dazu müssen Sie in den Xposed-Einstellungen den Installationsmodus von „Klassisch" auf „Recovery" ändern. Wahlweise flasht Xposed die Dateien automatisch beim Start, andernfalls spielen Sie es manuell im Recovery-Modus ein.

Probleme gibt es auch, wenn andere Tools an den gleichen Stellen einhaken wie Xposed oder eines seiner Module. So vertragen sich einige Launcher und Apps zum Rechtemanagement nicht mit den entsprechenden Xposed-Modulen. Programme

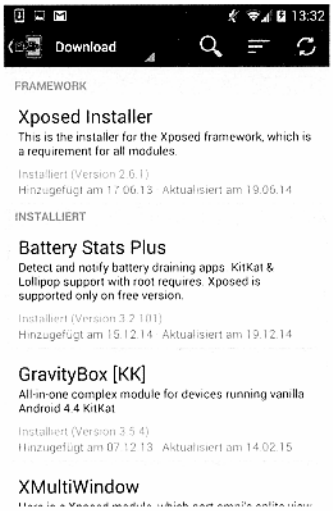
Xposed, ART und Android 5

Google setzt seit einiger Zeit auf eine neue Android-Runtime namens ART, was Xposed noch einige Probleme bereitet. Bei Android 4.4 ist sie nur optional, seit Android 5 jedoch der Standard. Auf keinen Fall sollte man unter Android 4.4 die Runtime von Dalvik auf die neuere ART umstellen, denn damit kommt Xposed nicht zurecht – stattdessen landet man in einer Boot-Schleife.

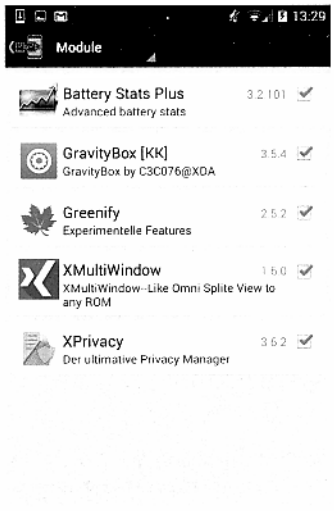
Auch auf Android 5 ist Xposed erst seit Kurzem als zu ART kompatible Alpha-Version verfügbar. Die Umstellung nötigt dem Xposed-Entwickler tiefgreifende Änderungen ab: Die Alpha-Version von Xposed tauscht diverse Systemkomponenten aus und deaktiviert einige Optimierungen von ART, um die gleichen Funktionen wie bisher bereitzustellen. Lohn der Mühe ist Abwärtskompatibilität für die Modul-Entwickler; die meisten Xposed-Module werden deshalb später auch auf Android 5 laufen. Noch hakt es jedoch an vielen Stellen, bis zu einer stabilen Version für Android Lollipop wird noch etwas Zeit vergehen.



Das Einspielen des Framework ins Systemverzeichnis übernimmt der Xposed Installer.



Xposed ist erst mit Modulen nützlich, die im Installer direkt heruntergeladen werden.



Die Xposed-Module müssen nach der Installation aktiviert werden.

Neugierigen Apps gewöhnt man mit XPrivacy die Schnüffelei ab.

die ebenfalls systemnahe Funktionen verändern, sollte man also möglichst nicht parallel zu Xposed installieren. Manche Herstelleroberflächen wie HTC Sense vertragen sich ebenfalls nicht mit allen Modulen.

Hunderte Module

Über 500 Module listet der Xposed Installer unter „Downloads" mittlerweile auf, die meisten davon mit ausführlichen Infos und Links zu den Entwicklerseiten. Nicht alle Module sind für jedes Gerät und jede Android-Version geeignet, daher lohnt ein genauer Blick auf die Beschreibung. Zum Herunterladen scrollt man in der App-Detailansicht einmal nach rechts. Auch ältere Versionen stehen hier bereit, falls ein Update Probleme macht. Das Modul-Repository gibt es auch als Webseite, von der die Module als APK-Datei geladen werden können.

Die Installation läuft wie bei herkömmlichen Apps ab. Danach müssen die Erweiterungen noch unter „Module" aktiviert und das Gerät neu gestartet werden. Um sie zu deaktivieren, geht man genauso vor. Deinstalliert werden die Module wie andere Programme in der App-Übersicht. Es ist also nicht möglich, dem System heimlich Module unterzuschieben.

Einige Apps bringen eigene Xposed-Module mit, die es nicht in der Sammlung gibt. Das Energiespartool Greenify etwa nutzt Xposed, um auch Systemdienste einbremsen zu können, auf die es sonst keinen Zugriff hat. Die Modul-Installation läuft dabei genauso ab, das Modul muss von Hand in Xposed aktiviert werden.

Unter den Hunderten Modulen gibt es eine Menge interessante und teils auf sehr spezifische Probleme zugeschnittene. Ausprobieren lohnt sich, denn dauerhaft kaputtmachen kann man dabei wenig – wenn man die Hinweise der Autoren beachtet und die Finger von den Android-Systemdiensten lässt. Mit einigen Modulen kann man sich durchaus vom System aussperren, wenn man die Warnungen ignoriert.

Privat mit XPrivacy

Das mächtige XPrivacy-Modul erlaubt es, die Berechtigungen für einzelne Apps sehr genau zu steuern und so unerwünschte Zugriffe auf Funktionen und private Daten zu verhindern. Dabei greift die Software falls möglich nicht direkt ins Android-Rechtemanagement ein und entzieht Apps keine Berechtigungen. Denn darauf reagieren viele Apps allergisch und stürzen einfach ab. Stattdessen füttert XPrivacy die Apps mit falschen Daten, wenn sie auf sensible Informationen und gesperrte Funktionen zugreifen. So sehen Facebook, WhatsApp und Co. auf Wunsch nur leere Kontaktlisten, falsche Ortsangaben oder zufällige IDs. Die dabei übergebenen Daten lassen sich anpassen. Die Version für 5 Euro erlaubt es sogar, einzelne Kontakte gezielt freizugeben. Am Beispiel von WhatsApp haben wir das Vorgehen auf S. 154 aufgedröselt.

In der Grundeinstellung verhindert XPrivacy den Zugriff auf Daten, die Rückschlüsse auf den Nutzer zulassen. Greift eine App zum ersten Mal auf eine Kategorie zu, fragt das Modul, ob das erlaubt oder blockiert werden soll. Auch eine temporäre Freigabe ist möglich. Rot hinterlegte Kategorien sind für das reibungslose Funktionieren der App meistens erforderlich. Blockiert man sie, kassiert man mitunter einen Absturz. Schränkt man Dinge wie den Internet-Zugriff ein, arbeitet die App noch, man darf sich nur nicht wundern, wenn keine Daten abgerufen werden. Die Abfragen muss man bei jeder frisch installierten App über sich ergehen lassen.

Ändern lassen sich die Freigaben für jede installierte App auch in XPrivacy direkt. In der Grundeinstellung gibt es für jede blockbare Funktion zwei Kästchen. Ist im linken ein Haken gesetzt, wird sie blockiert. Steht im rechten Kästchen ein Fragezeichen, wird vor dem Zugriff nach Erlaubnis gefragt. Die Einstellungen sind entweder für eine komplette Kategorie möglich oder nach Antippen des rot hinterlegten Pfeils links daneben äußerst kleinteilig für einzelne Android-Befehle. Ausgefüllte Boxen zeigen an, dass nur einzelne Unterpunkte beschränkt sind. Zusätzlich ist in der Übersicht vermerkt, ob und wann eine Funktion zuletzt verwendet wurde. Um die kritische Webview-Sicherheitslücke unter Android 4.3 und früher einzudämmen, beschränkt man „Anzeigen (mittels Browser)". XPrivacy selbst warnt allerdings davor, dass eine böswillige App diese Einstellung umgehen kann.

Die Hilfe ist zwar umfangreich, trotzdem wird aber nicht immer klar, welche Funktion da gerade eingeschränkt wird. In der Regel reicht es, die Oberkategorien einzuschränken. Rot markierte Unterpunkte sperrt XPrivacy nicht automatisch, da sie kritisch für das Funktionieren der jeweiligen App sind. Will man sich nicht selber durch die Kategorien und Google-Dokumente schlagen oder die Folgen ausprobieren, helfen Profile. Dafür werden von Nutzern hochgeladene Einstellungen ausgewertet und die Mehrheit entscheidet, welche Rechte erlaubt und verweigert werden. Die Crowd-Profile stehen nur in der Bezahl-Version zur Verfügung, anschauen kann man sich die Mehrheitsentscheidungen kostenlos im Netz.

Um mit Xposed auch vorinstallierte Apps und Dienste zu beeinflussen, muss man in den Einstellungen den Experten-Modus und die entsprechende Funktion aktivieren. Sich versehentlich vom System auszusperren ist dann aber leicht ohne Weiteres möglich. Einen Performance-Verlust durch XPrivacy konnten wir übrigens nicht beobachten, trotz der Eingriffe liefen Apps und System so schnell wie zuvor. (asp@ct.de)

Literatur

[1] Hannes A. Czerulla, Freiheit für Android, Rooting für Android-Smartphones und -Tablets, c't 2/15, S. 82

c't Xposed, Root-Hilfen und Module: ct.de/y74e

Holger Bleich, Alexander Spier

Kontaktkontrolle

Adressbuch-Zugriff von WhatsApp einschränken

WhatsApp greift nach allen Kontakten in Smartphone-Adressbüchern und überträgt sie zu seinen Servern. Während iPhone- und Windows-Phone-Nutzer diese Datenschieberei nur ganz oder gar nicht verweigern können, erlaubt Android zumindest berufliche von privaten Kontakten zu trennen.

Nach der Installation und bei jedem Neustart sichtet der Mobil-Messenger WhatsApp alle im Handy gespeicherten Kontakte und gleicht sie mit seinen Servern ab. Findet der Server die Mobilfunknummer eines anderen WhatsApp-Nutzers, überträgt er diesen Kontakt in die App. Dieser Scan bedeutet, dass jeder Kontakt im Smartphone auf dem Server von WhatsApp landet – ob man will oder nicht.

Eine Menge Geheimnisträger dürften damit unbewusst vertrauliche Kontakte in die WhatsApp- respektive Facebook-Cloud pumpen. Man denke etwa an den Informanten eines Journalisten, dem er absolute Diskretion garantiert hat, an Mandanten eines Anwalts oder Patienten eines Psychiaters. Hat man diesen Personen Vertraulichkeit zugesichert, handelt man sogar rechtswidrig, wenn man deren Kontaktdaten an Dritte überträgt.

Wenn Sie Ihr Handy beruflich und privat nutzen, sind alle Kontakte für Apps mit entsprechenden Rechten zugänglich. Zwar können Android und Windows Phone mehrere voneinander abgeschottete Adressbücher pflegen. Doch für Apps wie WhatsApp taugt dies nicht als Einschränkung – sie erhalten stets vollen Zugriff auf alle Adressbücher.

Viele Unternehmen zwingen ihre Mitarbeiter daher, ihr Handy mit MDM-Software (Mobile Device Management) zu versehen. Derlei (meist recht teure) Lösungen schränken den Zugriff auf vertrauliche Daten ein oder schaffen voreinander versteckte Bereiche auf demselben Gerät [1]. Für Betriebe mit wenigen Mitarbeitern ist MDM allerdings Overkill. Meist lautet die einzige Lösung, beruflich und privat verschiedene Geräte zu nutzen und auf dem beruflichen kein WhatsApp zu installieren. Das läuft jedoch dem „Bring your own Device"-Gedanken zuwider und ist schlicht unpraktisch.

Mini-MDM mit Android 5

Wir haben nach Möglichkeiten gesucht, unter Android, iOS und Windows Phone Apps den Zugriff auf das zentrale Adressbuch zu verweigern. Unter iOS oder Windows Phone lassen sich WhatsApp einzelne Kontakte nicht vorenthalten, nur eine Komplettsperre ist möglich. Ohne Adressbuchzugriff taugt WhatsApp aber nur zum Empfangen und zum Antworten auf eingegangene Nachrichten. Neue Kontakte anschreiben kann man so nicht.

Eine Möglichkeit ist es, vertrauliche Telefonnummern, Termine und Mail-Adressen getrennt vom System in einem eigenen Container aufzubewahren. Der Exchange-Client Touchdown synchronisiert Daten beispielsweise nicht mit dem System-Adressbuch, sondern bewahrt sie unzugänglich für andere Programme in einem eigenen Ordner auf. Das bedeutet allerdings auch Komfortverzicht, denn die Adressen können nur in der App genutzt werden.

Android sieht nicht einmal die Möglichkeit vor, einer App den Adressbuch-Zugriff zu verweigern. Mit Android 5 hat Google jedoch die auf den Tablets schon länger vorhandene Benutzerverwaltung auf Smartphones eingeführt. So ist es möglich, beispielsweise einen geschäftlichen und einen privaten Nutzer anzulegen. Der Kontaktzugriff von WhatsApp bleibt auf die Daten des jeweils aktiven Nutzers beschränkt. Solange man auf dem vertraulichen Konto kein WhatsApp installiert, bleiben diese Kontakte im Adressbuch verschont. Unseren Tests zufolge gibt es für angelegte Nutzer und deren Apps tatsächlich keine Möglichkeit, in den Kontakten der anderen Nutzer herumzuschnüffeln.

Damit WhatsApp Kontakte nicht findet, unterbindet man den Zugriff beim ersten Start.

In XPrivacy kann man in der Detailansicht für WhatsApp gezielt Kontakte freigeben.

Selektive Zugriffssperre

Für Android 4.4 haben wir ebenfalls eine Lösung gefunden, doch die ist nur mit einem gerooteten Smartphone, dem auf Seite 152 vorgestellten Xposed Framework und dessen Modul XPrivacy umsetzbar. Die Einrichtung von Xposed macht Arbeit und der Root-Zugriff eröffnet zudem Angreifern prinzipiell mehr Möglichkeiten, weil er das Sicherheitsmodell von Android teilweise unterläuft. Mit dem XPrivacy-Modul lassen sich die Zugriffsrechte jeder einzelnen App fein granuliert steuern, also auch jene von WhatsApp. XPrivacy erlaubt es, WhatsApp selektiv Kontakte aus dem Android-Adressbuch vorzuenthalten. Nötig ist dafür die Pro-Variante für 5 Euro.

Sie sollten zunächst WhatsApp installieren, sich aber noch nicht anmelden. Stattdessen rufen Sie in XPrivacy die Optionen für WhatsApp auf. Dort ist der Zugriff aufs Adressbuch per Voreinstellung zunächst gesperrt und auf Nachfragen beim Zugriff eingestellt.

Setzen Sie das linke Einschränkungs-Häkchen bei der Ressource „Kontakte" und lassen das rechte Kästchen leer. Damit sperren Sie erst einmal den Zugriff auf alle Kontakte und füttern WhatsApp mit einer leeren Liste. Über das Kontextmenü („Kontakte für Zugriff freigeben") haben Sie nun die Möglichkeit, eine Positivliste zu erstellen, die Sie später jederzeit ergänzen können. Wählen Sie dazu die (unpassend übersetzte) Liste „Alle Einstellungen" und haken dort die gewünschten Kontakte an. Nur Ihre Auswahl bekommt WhatsApp künftig zu sehen. Dass die Positivliste aktiv ist, erkennen Sie am eingekreisten „W" (für Whitelist) in der Rechte-Übersicht.

Jetzt können Sie XPrivacy verlassen und die Installation von WhatsApp abschließen. Eventuell auftauchende Rechte-Nachfragen von XPrivacy beantworten Sie für Kontakte mit „Blockieren". WhatsApp wird so nur die erlaubten Kontakte zum Server schicken. (hob@ct.de)

Literatur

[1] René Peinl, Peter Schüler, Teile und herrsche, Berufliche und private Daten auf Smartphones und Tablets trennen, c't 1/14, S. 172 c't

Ronald Eikenberg, Jörg Wirtgen

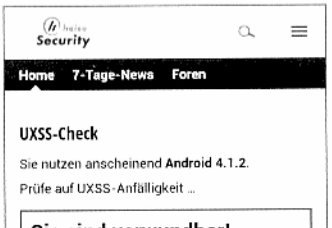
Surf-Versicherung für Android

Jelly Bean und älter trotz Schwachstellen sicher nutzen

Wer eine ältere Android-Version als 4.4 nutzt, muss mit Sicherheitslücken im Browser leben, die Google nicht schließen will – und selbst die existierenden Sicherheits-Patches kommen nicht auf allen Geräten an. Bevor die Lücken von Cyber-Ganoven ausgenutzt werden, sollten Sie daher auf Ihrem Smartphone und Tablet ein paar Vorsichtsmaßnahmen ergreifen.

Auf fast der Hälfte der aktuell genutzten Android-Geräte läuft noch Jelly Bean (Android 4.1 bis 4.3), auf über 10 Prozent eine noch ältere Version – und in vielen davon klaffen Sicherheitslöcher. Zwar hat Google bislang stets passende Patches entwickelt, doch die landen nur bei den Herstellern, die es dann oft versäumen, sie den Nutzern in Firmware-Updates zur Verfügung zu stellen. Ob und welche Lücken im eigenen Gerät klaffen, kann man nur mit großem Aufwand herausfinden.

Künftig spitzt sich die Lage für Nutzer alter Android-Versionen weiter zu: Google ließ durchblicken, künftig keine Sicherheits-Patches für den bis Android 4.3 genutzten Browser mehr zu entwickeln. Damit stirbt die letzte Hoffnung, dass neu entdeckte Lücken jemals geschlossen werden. Googles Entscheidung betrifft nicht nur den Browser, sondern das gesamte System: Seine sogenannte WebView-Komponente kommt in unzähligen Apps zum Einsatz, die dadurch ebenfalls angreifbar sind. Browser und WebView kann man bis Jelly Bean nur per Firmware-Update auf den aktuellen Stand bringen.



Mit dem Android-Check auf heise security finden Sie heraus, wie sicher Ihr Android-Gerät beim Surfen ist (siehe c't-Link).

Smartphone als Wanze

Würde es ein Angreifer darauf anlegen, ein Android-Gerät zu kompromittieren, hätte er reichlich Möglichkeiten. So bringt etwa das frei verfügbare Pentesting-Tool Metasploit inzwischen elf Module mit, die verschiedene Android-Lücken ausnützen. Je älter die Android-Version, desto größer die Auswahl. Mit Metasploit haben wir mit überschaubarem Aufwand eine Webseite gebaut, die ein ansurfendes Jelly-Bean-Smartphone in eine Abhörwanze verwandelt – ohne dass der Nutzer etwas davon mitbekommt. Nach der Infektion konnten wir über das Netz unter anderem Kamera und Mikrofon anzapfen, die GPS-Koordinaten abrufen und auf Dateien zugreifen. Schuld ist eine Lücke in einer Browser-Schnittstelle, durch die Webseiten beliebige Java-Befehle auf dem Android-Gerät ausführen können.

Durch eine Lücke jüngeren Datums in Android bis 4.3 kann ein Angreifer eine essenzielle Schutzfunktion des Browsers austricksen, die sogenannte Same-Origin-Policy. Sie bewirkt, dass eine Website nicht auf Inhalte einer anderen Website zugreifen darf. Lädt etwa eine böswillige Seite in einem IFrame das Webmail-Interface von web.de, bekommt sie normalerweise keinen Zugriff auf den Inhalt des IFrames mit dem Mail-Posteingang. Bei den betroffenen Android-Versionen kann ein Angreifer jedoch die Same-Origin-Policy mit wenigen Zeilen JavaScript-Code umgehen und so auf persönliche Daten seines Opfers zugreifen. Auch das konnten wir nachvollziehen. Diese Angriffsform bezeichnet man als Universal-Cross-Site-Scripting (UXSS).

Der Sicherheitsexperte Tod Beardsley von Rapid7 hat den Angriff kürzlich auf die Spitze getrieben, indem er UXSS mit einer Lücke in Googles Play Store kombinierte. Seine Demoseite steuerte die Web-Ausgabe von Google Play fern. Sie lud zuerst die Produktseite einer beliebigen App und klickte anschließend auf den Kaufen-Button. Kurze Zeit später wurde die App auf dem Gerät des Webseitenbesuchers installiert und gestartet – vollautomatisch und ganz ohne Nutzerinteraktion. Google hat die verwundbaren Browser-Versionen kurz darauf aus der Web-Version des Stores ausgesperrt. Damit wird zwar die automatische App-Installation verhindert, die Wurzel des Übels – die UXSS-Lücke – existiert jedoch weiterhin.

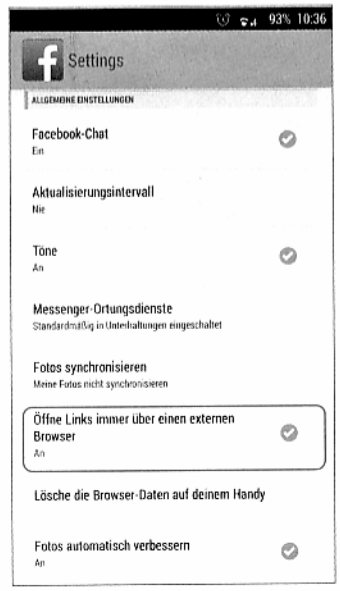
Immerhin war es nur möglich, Apps aus dem Play Store zu laden – die weitaus gefährlicheren Apps aus fremden Quellen lassen sich weiterhin nicht ohne Bestätigung des Nutzers installieren.

So schützen Sie sich

Die einzige wasserdichte Lösung ist der Umstieg auf Android 4.4 oder 5. Dort kommt eine WebView-Komponente auf Chrome-Basis zum Einsatz, die weniger Fehler aufweist und Updates automatisch über den Play Store bekommt – unabhängig vom Betriebssystem. Wenn der Gerätehersteller eine Aktualisierung auf Android 4.4 anbietet, sollten Sie die also aufspielen und sind fertig; weiter brauchen Sie nicht zu lesen. Sie fangen sich damit allerdings Einschränkungen beim Zugriff auf die SD-Karte ein [1].

Lässt Sie der Hersteller bei 4.3 oder älter hängen, können Sie überprüfen, ob er zumindest für den oben beschrieben UXSS-Bug einen Patch in die Firmware integriert hat. Wir haben dazu eine harmlose Testseite entwickelt (siehe c't-Link am Ende des Artikels), welche die UXSS-Lücke tatsächlich ausnutzt – gelingt das, ist die Wahrscheinlichkeit groß, dass der Hersteller auch andere Patches vernachlässigt hat. Sie sollten also vom Schlimmsten ausgehen.

Gibt es kein offizielles Update auf 4.4 oder neuer, kann ein CustomROM mit Android 4.4 eine Lösung sein; also ein selbst aufgespieltes Alternativ-Android. Für viele Geräte gibt es CustomROMs, eine gute Anlaufstelle ist CyanogenMod. Das ist aber nichts, was man mal eben schnell einspielt, sondern eine grundlegende Entscheidung. Selbst wenn alles glattgeht, müssen Sie Ihr Gerät dazu rooten sowie alle Apps und Einstellungen neu installieren. Sie verlieren meist auch die Hersteller-Garantie und müssen auf jene Apps des Herstellers verzichten,



Apps wie Facebook oder RSS-Reader nutzen einen eigenen, wahrscheinlich ebenfalls verwundbaren Browser. Einige lassen sich so einstellen, dass sie stattdessen den externen Browser aufrufen.

Maßnahmen bei Android bis 4.3

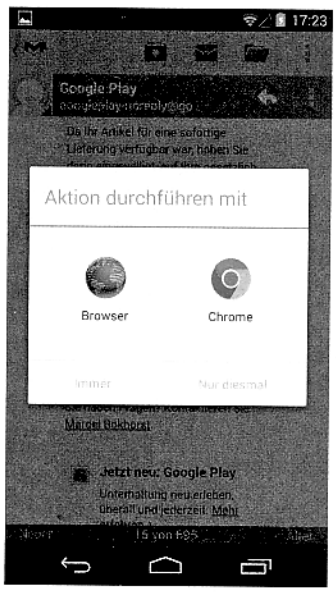
- Installieren Sie Firefox, Chrome oder Dolphin Browser.
- Stellen Sie browsende Apps wie Facebook so ein, dass sie den externen Browser nutzen. Alternativ: Nutzen Sie solche Dienste im Browser statt per App.
- Verzichten Sie auf Apps mit Werbebannern.
- Surfen Sie in öffentlichen WLANs per VPN oder bleiben Sie stattdessen im Mobilfunknetz.

die er nicht auch im Play Store anbietet. Beides ist bei älteren Geräten kein großer Verlust. [2]

Browsen ohne WebView

Wenn Sie kein 4.4 bekommen, müssen Sie mit den Lücken leben. Da es bisher noch keine echten Angriffe gibt, sondern nur Proof-of-Concepts, bleibt das ein geringes Risiko. Einige Vorsichtsmaßnahmen sind aber angebracht. Installieren Sie zuerst einen Browser mit eigenem Renderer, zum Beispiel Chrome, Firefox oder Dolphin Browser. Damit sind Sie nicht mehr angreifbar, solange Sie diesen Browser benutzen.

Viele beliebte Browser-Apps wie CM Browser, Maxthon oder Mercury haben keine eigene Browser-Engine, sondern rufen die WebView-Komponente auf. Sie bieten auf verwundbaren Geräten daher keine Abhilfe. Überprüfen Sie im Zweifelsfall über unsere Testseite, welche Engine zum Einsatz kommt. Die Seite zeigt einen Text wie „AppleWebKit/534.40" an. Rufen Sie unseren Test zuerst mit dem Standard-Browser und dann der Alternative auf, um festzustellen, ob Letztere eine andere oder zumindest neuere Engine einsetzt.



Tippen Sie in einer Mail auf einen Link, wählen Sie Chrome und bestätigen Sie dieses Fenster mit „Immer". Dann haben Sie den unverwundbaren Browser als Standard eingestellt.

Nach der Installation des Browsers sollten Sie ihn aus einer anderen App aufrufen, am einfachsten durch Antippen eines Links in einer Mail. Dann fragt Android nach, welcher Browser standardmäßig aufgerufen wird – wählen Sie dort den neuen aus und bestätigen Sie „immer". Fehlt die Frage, hatten Sie vielleicht schon mal einen anderen installiert. Das Zurücksetzen so einer Default-Zuordnung löst Android recht umständlich: Suchen Sie in Einstellungen/Apps den startenden, als Standard eingestellten Browser (zu finden im Reiter „Alle"), tippen Sie darauf und dann auf den Knopf „Standardeinstellung zurücksetzen" unter „Standardmäßig starten". Danach kommt die Auswahlbox beim nächsten Antippen eines Links wieder.

Einige Apps bieten einen internen Browser zum Anzeigen von Websites und nutzen dazu vermutlich den kaputten WebView. Dazu gehören beispielsweise die Facebook-App und einige News- und RSS-Reader. Um darüber nicht angreifbar zu sein: Versuchen Sie, die App so einzustellen, dass sie einen externen Browser aufruft. Bei Facebook geht das über die „App-Einstellungen" in dem unübersichtlich langen Menü, das sich beim Tippen des grauen Menüknopfs öffnet.

Hat die App keine solche Einstellung, sollten Sie mit ihr keine externen Links mehr aufrufen. Vielleicht können Sie sogar ganz auf die App verzichten und den entsprechenden Dienst nur noch per Mobil-Browser nutzen.

WebView woanders

Die meisten Apps, die Werbebanner einblenden, dürften dafür ebenfalls den WebView nutzen. Angriffe auf die Server, die solche Banner verbreiten, finden tatsächlich statt, bisher zielen sie auf Windows-Lücken. Auf diese Weise wurden auch schon renommierte Seiten mit böswilligen Werbebannern unterminiert. Es reicht also nicht, dem Seitenanbieter oder – im Fall von Android – dem App-Anbieter zu trauen, denn der Angriff findet möglicherweise außerhalb seines Einflussbereichs statt. Die einfachste Lösung ist, auf werbefinanzierte Apps zu verzichten oder die Bezahlversion zu kaufen.

Der WebView kommt auch zu vielen anderen Gelegenheiten in Apps zum Einsatz. Beispielsweise zeigen einige Apps ihre Versionshistorie oder Nutzungsbedingungen an, indem sie eine Website vom Anbieter aufrufen; andere laden als Hauptzweck Webinhalte nach. Auf den ersten Blick ist das ungefährlich, doch zwei Szenarien sind denkbar: Erstens könnte der Server des Anbieters gehackt werden und Schadcode ausliefern. Zweitens können Angreifer den Datenverkehr in öffentlichen WLANs manipulieren.

Gegen das Mithorchen hilft eine Maßnahme, die bei Benutzung kritischer Apps in öffentlichen WLANs sowieso eine Überlegung wert ist: Gehen Sie nur per VPN online. Richten Sie sich also entweder zu Hause einen VPN-Zugang ein (nicht ganz trivial), fragen Sie die IT-Abteilung Ihres Arbeitgebers oder schauen Sie sich bei kommerziellen VPN-Anbietern um [3]. Eine weitere Lösung wäre, die potenziell kritischen WLANs zu vermeiden und per Mobilfunk ins Internet zu gehen. Gegen gehackte Anbieterserver hilft beides nicht.

Rooten hilft wenig

Reparieren lässt sich die WebView-Lücke nach unserem Wissen nicht. Selbst auf gerooteten Geräten ist uns keine Lösung bekannt, WebView zu fixen oder notfalls ganz lahmzulegen.

Nach dem Rooten kann man jedoch Adblocker wie das Xposed-Modul MinMinGuard oder AdAway installieren, die vor korrumpierten Werbebannern schützen können. Das Xposed-Modul Xprivacy widmet sich zwar unter „Anzeigen (mittels Browser)" dem WebView, verhindert aber hauptsächlich die Übertragung privater Daten wie dem UserAgent-String. Das Abschalten oder Absichern von WebView gelingt damit nicht. Somit erzeugen diese Tools oder auch Xposed-Firewalls ein eher trügerisches Gefühl der Sicherheit, ohne das Problem wirklich zu lösen. (jow@ct.de)

Wenn das Auswahlfenster nicht erscheint, ist schon ein Browser als Standard ausgewählt – möglicherweise der verwundbare. Das können Sie in den App-Infos überprüfen und zurückstellen.

Literatur

[1] Jörg Wirtgen, Beschreiben verboten, Einschränkungen beim Zugriff auf SD-Karten unter Android 4.4 und 5.0, c't 3/15, S. 150

[2] Hannes Czerulla, Freiheit für Android, Rooting für Android-Smartphones und -Tablets, c't 2/15, S. 82

[3] Urs Mansmann, Sonne, Strand und Internet, Im Urlaub sicher und günstig online gehen, c't 15/14, S. 76

c't Testen Sie Ihren Browser: ct.de/yhue