

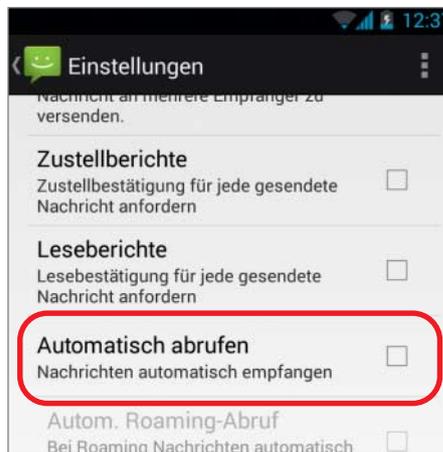
## Multimedia-Schnittstelle von Android unter Beschuss

Durch eine Reihe von Schwachstellen in der Multimedia-Schnittstelle Stagefright sollen sich 95 Prozent aller Android-Smartphones attackieren lassen – Version 2.2 bis 5.1.1 sind verwundbar. Auf diesem Weg können Angreifer etwa Schadcode ausführen und ein Smartphone in Dauerschleife zum Absturz bringen. Dafür muss der Angreifer lediglich eine MMS- oder Hangouts-Nachricht mit Exploit-Code an das Opfer schicken, berichtet der Sicherheitsforscher Joshua Drake von Zimperium zLabs. Für einen erfolgreichen Übergriff muss das Opfer die Nachricht nicht einmal öffnen und bekommt nichts vom Angriff mit. Je nachdem mit welchen Rechten der angegriffene Prozess ausgeführt wird, könne der Angreifer beispielsweise Audio und Video mitschneiden und so das Smartphone in eine Wanze verwandeln.

Zudem können Angreifer laut Trend Micro den Angriff auch über ein manipuliertes Video auf einer Webseite oder in einer App ausführen.

In den USA soll Google schon Updates für seine Nexus-Serie verteilen. Für welche weiteren Geräte die Patches zur Verfügung stehen, ist noch nicht bekannt. Der von der Android-Community entwickelte Abkömmling CyanogenMod ist den Entwicklern zufolge in den Versionen 11, 12 und 12.1 abgesichert.

Wer sich schützen will, kann in den Einstellungen alle Nachrichten von unbekanntenen Personen blocken. Zudem empfiehlt es sich, den automatischen Abruf von MMS-Nachrichten zu deaktivieren (siehe Bild). Das schützt allerdings nicht vor Hangouts-Kontakten oder Web-Seiten. Bei Hangouts kann man seit einem serverseitigen Update von



Um sich bis zum Erscheinen der Patches wenigstens etwas vor den Stagefright-Bugs abzusichern, deaktivieren Sie in den Nachrichten-Einstellungen den automatischen Abruf von Nachrichten.

Google einstellen, wer einen kontaktieren darf. (des@ct.de/rei@ct.de)

## Hacker steuern Jeep Cherokee fern

Im Uconnect-Infotainmentsystem von Fiat Chrysler soll eine kritische Schwachstelle klaffen, durch die ein Angreifer das damit ausgestattete Fahrzeug über das Internet fernsteuern und orten kann. Den Sicherheitsforschern Charlie Miller und Chris Valasek ist

es offenbar gelungen, über das Netz auf die Diagnose-Schnittstelle (CAN-Bus) eines Jeep Cherokee zuzugreifen.

Wer dieses Modell in Europa gekauft hat, muss sich anscheinend keine Sorgen machen. Gegenüber c't erklärte der Hersteller, dass auf

dem europäischen Markt keine von der Schwachstelle betroffenen Fahrzeuge verkauft werden. In den USA wurden hingegen 1,4 Millionen Fahrzeuge der Fiat-Chrysler-Gruppe zurückgerufen, um ein Update einzuspielen. (rei@ct.de)

## Kaspersky 2016 reduziert die Sammelwut von Internetseiten

Die aktuelle Generation der Kaspersky-Sicherheitssoftware für Windows beinhaltet eine neue Komponente mit dem Namen „Schutz vor Datensammlung“, die Web-Tracking-Dienste erkennt und auf Wunsch blockiert. Der Nutzer kann aber auch einzelne Webseiten vom Blockieren ausnehmen. Die Software unterteilt Tracker in unterschiedliche Kategorien. Damit ist es beispielsweise möglich, Social-Media-Tracker zu erlauben, aber Werbe-Anbieter zu blocken.

Das benötigte Plug-in funktioniert mit den aktuellen Browser-Versionen von Chrome, Firefox und Internet Explorer. Der in Windows 10 enthaltene neue Microsoft-Browser Edge bleibt außen vor, da er generell keine Plug-ins unterstützt.

Ebenfalls neu ist das Modul „Überwachung von Änderungen im Betriebssystem“, das den Nutzer vor unerwünschten Toolbars sowie

Plug-ins schützen soll und verhindern will, dass die Standard-Startseite und -Suchmaschine des Browsers überschrieben wird. Wenn die Software einen Prozess erkennt, der beispielsweise im Verlauf einer Freeware-Installation solche Modifikationen vornehmen möchte, warnt sie den Nutzer und ermöglicht ihm, die Änderungen zu verhindern.

Der Preis für Kaspersky Internet Security 2016 für ein Gerät und Jahr liegt bei 40 Euro. Kaspersky Anti-Virus verzichtet auf die genannten Erweiterungen und kostet wie gehabt 30 Euro. Darüber hinaus bietet Kaspersky eine Multi-Device-Version von Internet Security ab drei Geräten für 60 Euro an, die sich beliebig auf Windows-, Mac- und Android-Geräten verteilen lässt. Alle drei Versionen sollen am 1. September 2015 erscheinen. In den USA sind die neuen Versionen schon verfügbar. (rme@ct.de)



Neuerdings kann man mit Kasperskys Internet Security 2016 über den Punkt „Schutz vor Datensammlung“ auch Web-Tracking-Dienste blockieren.

## Sicherheits-Notizen

**Windows-Nutzer** sollten umgehend das Update MS15-078 einspielen, das eine kritische Lücke in vielen Windows-Versionen (Vista SP2 bis 8.1) stopft. Über die verwundbare Bibliothek ATMF.DLL können Angreifer Schadcode ausführen.

**OpenSSH** ist anfällig für Brute-force-Angriffe mit Wörterbüchern gängiger Passwörter, weil sich die Begrenzung der maximalen

Versuche pro Verbindung umgehen lässt. Admins sollten die Anmeldung auf Public-Key-Logins beschränken.

**WordPress 4.2.3** stopft unter anderem ein Sicherheitsloch, über das Angreifer mit bestimmten Rechten die gesamte Seite kompromittieren können.

Das Hacker-Forum **Darkode** wurde nach einer Polizeirazzia wiederbelebt und setzt

nun auf verschärfte Sicherheitsvorkehrungen.

In der Password Hashing Competition (PHC) hat sich der Algorithmus **Argon2** gegen 23 Mitbewerber durchgesetzt.

Das PHP-Skript **PHP File Manager** war fünf Jahre lang angreifbar. Mittlerweile hat der Hersteller das verwundbare Skript aus seinem Online-Shop entfernt.