Google: Mehr HTTPS, kaum Certificate Pinning

Der Anteil an HTTPS-Traffic am Datenverkehr im Internet ist deutlich gestiegen: Aus Googles jüngstem Transparenzbericht (siehe ct.de/yvmj) geht hervor, dass in Deutschland Ende Oktober 2017 inzwischen 71 Prozent der Webseiten, die Anwender mit Google Chrome aufrufen, die Transportverschlüsselung verwenden. Ein Jahr zuvor waren es noch 52 Prozent – ein Anstieg um mehr als ein Drittel.

Schlechter bestellt ist es um das HTTPS Public Key Pinning (HPKP), oft einfach „Certificate Pinning“ genannt. Es ist ein Verfahren, mit dem Google das Web ein Stück sicherer machen wollte. Setzen Website-Betreiber es ein, vergewissert sich der Browser, dass das Zertifikat stets als Folgezertifikat von derselben Zertifizierungsstelle kommt. Gibt sich ein Dritter mit einem missbräuchlich ausgestellten Zertifikat als der Webserver aus, schlägt der Browser Alarm.

Google plant nun, die Unterstützung für dynamisches Pinning mit Chrome 67 fallen zu lassen; statische Pins bleiben bis auf weiteres erhalten. Version 67 soll Ende Mai 2018 erscheinen. Die Verbreitung blieb weit hinter den Erwartungen zurück: Der britische Sicherheitsforscher Scott Helme hat ermittelt, dass im Jahr 2016 nur 375 Websites der „Alexa Top 1 Million Sites“ HPKP verwendeten – gerade mal eine von 2700.

HPKP gelangte zunehmend in die Kritik, weil es in der Praxis mitunter sperrig zu handhaben ist – immer wieder haben Website-Betreiber durch unachtsames Zertifikats-Handling ihre Besucher ausgesperrt. Als mittelfristige Alternative sieht Google sein eigenes Projekt Certificate Transparency (CT): Es soll CAs auf Dauer zwingen, sämtliche Zertifikatsausstellungen in einem manipulationssicheren, öffentlichen Protokoll zu hinterlegen. Das kann einen Missbrauch nicht technisch verhindern – Google setzt stattdessen auf Sicherheit durch Transparenz. *(ju@ct.de/ovw@ct.de)*

Transparenzbericht: ***ct.de/yvmj***

Sicherheits-Notizen

Anwender von **WordPress** sollten schleunigst auf Version 4.8.3 aktualisieren, um eine SQL-Injection-Lücke zu schließen, mit der Angreifer Webseiten übernehmen könnten.

Für **Oracle Fusion Middleware** steht ein Patch bereit, der eine kritische Lücke im Identity Manager schließt. Angreifer könnten sich über einen Default-Account via HTTP in verwundbare Systeme einloggen und sie übernehmen.

In Google **Chrome** und **Chromium** befindet sich in allen Versionen vor 62.0.3202.75 eine Lücke, die nichtautorisierten entfernten Angreifern das Ausführen beliebigen Programmcodes sowie DoS-Angriffe ermöglicht. Patches kommen wie gewohnt über die Update-Automatik der Browser.

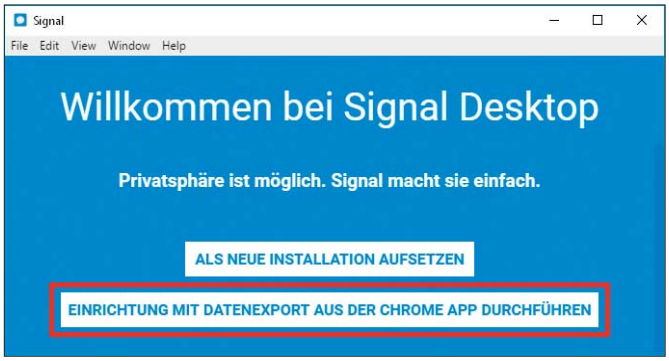
Desinfec’t 2017/18 ist da

Ab sofort ist das Sonderheft c’t wissen Desinfec’t 2017/18 am Kiosk und online für 9,90 Euro erhältlich. Auf der Heft-DVD befindet sich die brandneue Version des c’t-Sicherheitstools Desinfec’t 2017/18. Desinfec’t richtet sich an Windows-Nutzer, die mit dem Live-System vier Virenscanner von Avira, Eset, F-Secure und Sophos auf ein inaktives Windows loslassen können. Das Sicherheitstool wurde komplett überarbeitet, setzt nun auf Ubuntu 16.04.3 LTS und bietet standardmäßig einen schlankeren und flotteren Desktop als die Vorgänger. Alternativ gibt es das Heft auch als E-Paper inklusive Download-Code für 8,99 Euro. Wer möchte, bekommt die digitale Ausgabe auch auf einem USB-Stick, auf dem sich zusätzlich ein direkt startbares Desinfec’t befindet. Der Stick mit 16 GByte ist für 17,90 Euro ausschließlich online via shop.heise.de erhältlich. *(des@ct.de)*

Desktop-Clients für Signal

Die Entwickler des verschlüsselnden Messengers Signal haben Desktop-Clients veröffentlicht. Sie laufen auf Windows ab 7, macOS ab 10.9 und APT-fähigen Linux-Distributionen wie Ubuntu und Debian. Die Programme stehen auf signal.org zum Download bereit. Wie bei den Web- und Desktop-Clients für WhatsApp funktionieren die Signal-Programme nicht autark, sondern setzen Kontakt zu Signal auf dem Smartphone voraus.

Bislang war die einzige Möglichkeit, Signal auf dem Desktop zu nutzen, eine App für Googles Web-Browser Chrome – die passend zur Veröffentlichung des neuen Clients aber eingestellt wurde. Wer bislang die Chrome-App verwendet, kann aus ihr die Daten exportieren und während der Einrichtung des neuen Clients wieder importieren. *(dbe@ct.de)*



Wer Signal bislang als Chrome-App genutzt hat, kann die vorhandenen Daten in den neuen Desktop-Client importieren.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover