Mehr Sicherheit für Krypto-Messenger

Nutzer der verschlüsselnden Messenger-App Threema können ihren Account ab sofort löschen lassen. Dazu muss man im Vorfeld ein Widerrufskennwort festlegen. Gibt man es auf einer speziellen Webseite der Entwickler ein (siehe c't-Link), wird der Account unwiederbringlich zerstört und verschwindet auch aus den Adressbüchern der Threema-Kontakte. So kann man zum Beispiel sicherstellen, dass der Account nicht missbraucht wird, etwa nachdem das Smartphone geklaut wurde. Die Entwickler haben bislang erst die Android- und die iOS-Version mit der neuen Funktion ausgestattet. Windows-Phone-Nutzer sind noch außen vor.

Auch Telegram kennt neue Tricks, die den Accountmissbrauch erschweren sollen. Der Messenger zeigt nun an, wie viele Sitzungen aktuell mit einem Account geöffnet sind. Entdeckt man dabei eine Sitzung von einer verdächtigen IP-Adresse, kann man sie gezielt schließen. Darüber hinaus können Telegram-Nutzer ihren Account nun per Zwei-Faktor-Authentifizierung schützen. Standardmäßig verschickt der Dienst ein Einmalpasswort per SMS, über das man bei der Einrichtung beweist, auch tatsächlich der legitime Besitzer der Rufnummer zu sein. Weiteren Schutz bietet nun ein dauerhaft gültiges Passwort, das man beim Einrichten eingeben muss. Telegram gibt es für alle wichtigen Mobil- und Desktop-Betriebssysteme

Wer statt über das Internet lieber verschlüsselt per SMS kommuniziert, kann dazu die kostenlose Android-App SMSSecure nutzen. Der Fork des Krypto-Messengers TextSecure bringt die SMS-Verschlüsselung, die aus dem TextSecure-Projekt entfernt wurde, wieder zurück aufs Smartphone. (rei@ct.de)

Mit einem Widerrufspasswort können Threema-Nutzer ihren Account jederzeit löschen –, auch wenn sie keinen Zugriff mehr auf ihr Smartphone haben.

c't Threema, Telegram, SMSSecure: ct.de/yay6

TrueCrypt ohne Hintertüren

Die letzte Version 7.1a des Verschlüsselungsprogramms TrueCrypt ist sicher und kann bedenkenlos weiter genutzt werden. Zu diesem Ergebnis kam das Open Crypto Audit Project (OCAP) nach einer Analyse des Quellcodes. Das Projekt hat ein umfangreiches Audit durchgeführt und nun den abschließenden Bericht dazu veröffentlicht.

TrueCrypt war im Rahmen der Snowden-Enthüllungen ins Interesse der Forschergemeinde gerückt. Diese hatte Spenden gesammelt, um den Quellcode auf Hintertüren und Programmierfehler durchsuchen zu lassen. Das in diesem Zusammenhang geschaffene OCAP hatte zunächst Bootloader und Windows-Kerneltreiber des Programms untersucht und keine gravierenden Mängel entdeckt. Nun ist der zweite und letzte Teil des Audits abgeschlossen.

Die Forscher fanden zwar keine gravierenden Mängel im TrueCrypt-Quellcode, die gegen den Einsatz sprechen würden. Sie machten jedoch vier Schwächen aus, von denen sie eine als ernsthafter einstufen. Dabei geht es um die Generierung von Zufallszahlen zur Schlüsselerzeugung in der Windows-Version. Unter sehr unwahrscheinlichen Umständen sei es möglich, dass das Windows-Crypto-API nicht sauber aufgerufen werde, ohne dass dies von TrueCrypt bemerkt werde. In diesen Fällen generiere TrueCrypt unsichere Schlüssel zur Festplattenverschlüsselung. (hob@ct.de)

DNS-Server plaudern Geheimnisse aus

Wie ein Scan der Webseite Internetwache.org zeigt, sind viele DNS-Server zu lasch konfiguriert und geben dadurch mehr preis, als sie sollten: Angreifer bekommen Einsicht in alle Hosts in einer Domain – und somit eine Liste möglicher Angriffsziele.

Wenn DNS-Server ihren Datenbestand untereinander austauschen (Zonentransfer), nutzen sie das sogenannte AXFR-Verfahren (Asynchronous Xfer Full Range). Typischerweise dürfen nur ausgewählte Systeme solche Zonentransfers anfordern. Laut Internetwache gibt es jedoch viele DNS-Server, die das generell erlauben. Ein Angreifer erhält so wertvolle Informationen über mögliche Opfer. Prekär wird die Lage spätestens dann, wenn der Domaininhaber unzureichend gesicherte Dienste betreibt – in dem Glauben, dass die Adresse schon niemand erraten wird.

Internetwache.org hat eine Million Websites auf das Problem untersucht und konnte in über 130 000 Fällen den Zonentransfer anstoßen und Informationen zu über 70 000 Domains abrufen. Bedenkt man, dass das Datenleck AXFR bereits seit Jahrzehnten bekannt ist und auch ausgenutzt wird, ist das schon peinlich. Wer selbst überprüfen möchte, ob sein DNS-Server zu freizügig konfiguriert ist, findet über den c't-Link eine Anleitung und ein Tool. (rei@ct.de)

c't DNS-Server checken: ct.de/yay6

Root-Lücke in OS X

Eine Sicherheitslücke in Apples OS X kann dazu missbraucht werden, Befehle mit Admin-Rechten auszuführen –, auch wenn man das entsprechende Passwort nicht kennt. Entdeckt hat sie der Sicherheitsexperte Emil Kvarnhammar, der das Problem im Oktober an Apple meldete.

Mit dem Update auf OS X 10.10.3 hat Apple die Lücke für OS X 10.10.x („Yosemite") geschlossen, will sie wohl aber aufgrund der nötigen weitreichenden Änderungen nicht auf ältere Versionen des Betriebssystems zurückportieren. Kvarnhammar hat Angriffscode bereitgestellt, der nach seinen Angaben mindestens auf OS X 10.7.5, 10.8.2, 10.9.5 und 10.10.2 funktioniert. (fab@ct.de)

PIN-Briefe geben Geheimnisse preis

Das etwa beim Versand von Kreditkarten-PINs eingesetzte Sicherheitspapier Hydalam soll sich mit überschaubarem Aufwand austricksen lassen. Silvan Reiser beschreibt in seinem Blog, wie es ihm gelang, die von einer Kreditkartenfirma zugestellte PIN abzulesen, ohne das Sicherheitssiegel zu beschädigen. Er durchleuchtete den PIN-Brief mit einem Blitz und fotografierte das Resultat. Anschließend bearbeitete er die Raw-Datei mit Photoshop, woraufhin die PIN klar sichtbar wurde. Er gibt an, das ursprüngliche Bild mit einem Differenzbild überlagert und Letzteres anschließend verschoben zu haben. Den genauen Ablauf demonstriert er in einem YouTube-Clip.

Eigentlich soll die PIN erst sichtbar sein, wenn man eine Papierschicht von dem geschützten Bereich abgezogen hat. Dies lässt sich nicht wieder rückgängig machen und ist deshalb ein Indikator dafür, ob die PIN auf dem Transportweg eingesehen wurde. Dass man den Sichtschutzfolien nicht bedingungslos trauen kann, zeigt auch eine fast zehn Jahre alte Untersuchung der University of Cambridge. Damals gelang es in den Forschern, alle untersuchten PIN-Briefe auszulesen, ohne das Siegel zu beschädigen.(rei@ct.de)

c't Video: ct.de/yay6

Cyber-Angreifer legen TV-Kanäle lahm

Einer Hackergruppe ist es gelungen, den Sendebetrieb des französischen Fernsehsenders TV5 Monde am 8. April für mehrere Stunden lahmzulegen. Zeitgleich verbreiteten die Täter über die Website des Senders und dessen Facebook-Seite islamistische Drohungen. Wie genau der Angriff stattgefunden hat, war bei Redaktionsschluss noch unklar. Zumindest für Teile ihres Angriffs könnten sie Passwörter und Zugangsmöglichkeiten genutzt haben, die in Fernsehberichten einsehbar waren. In mindestens zwei Fällen sind Beiträge aus der TV5-Redaktion gesendet worden, in denen Passwörter klar lesbar waren.

Nach dem Angriff waren drei französische Minister zur Sendezentrale gekommen, um sich zu informieren. Neben Kultusministerin Fleur Pellerin waren auch Außenminister Laurent Fabius und Innenminister Bernard Cazeneuve vor Ort. Der erklärte, dass Ermittlungen eingeleitet seien, und verwies darauf, dass man mehr Mittel für den Kampf gegen Cyberkriminalität bereitstellen will. (mho@ct.de)