28.07.2023 – 08:00 Uhr

Daten von Backups bestehen Sicherheitstest - fast

Bern (ots) -

Das neue Backup-Protokoll für Whatsapp-Nachrichten wurde einer umfassenden Sicherheitsanalyse durch ein Forschungsteam unterzogen. Eine dabei entdeckte Schwachstelle lässt sich durch ein starkes Passwort entschärfen.

Jeden Tag tauschen Menschen weltweit über hundert Milliarden Nachrichten auf dem Messenger-Dienst Whatsapp aus. Für die Vertraulichkeit soll dabei eine Ende-zu-Ende-Verschlüsselung sorgen. Beim automatischen Backup der Chats gab es allerdings bis vor kurzem nicht die gleiche Sicherheit - denn der persönliche Schlüssel zu den in der Cloud abgelegten Daten war der Firma bekannt. "Das Backup war gegenüber allen sicher, ausser gegenüber Whatsapp selbst", sagt die vom SNF geförderte Kryptografin Julia Hesse vom Forschungsinstitut IBM Research in Zürich.

Vielleicht auch deshalb führte der Messenger-Dienst Ende 2021 ein neues Backup-Protokoll ein, das Hesse nun gemeinsam mit Forschenden der ETH Zürich und der Bergischen Universität Wuppertal genau unter die Lupe genommen hat. Gemäss den Ergebnissen der Studie kann das Unternehmen selbst nun nicht mehr auf die Backups zugreifen.

Firmentresor ohne Firmenzugriff

Für die Analyse erstellte das Team ein formales Modell, das alle Anforderungen an ein sicheres Backup-System beschreibt - etwa die notwendige Länge der Schlüssel. Dieses ideale Modell verglichen sie dann mit dem tatsächlich eingesetzten Protokoll. Die Informationen dafür suchten sie sich aus verschiedenen Quellen zusammen, beispielsweise aus offiziellen von Whatsapp veröffentlichten Dokumenten und aus Befragungen von Mitarbeitenden, die das neue Backup-Protokoll entwickelt haben. "Wir mussten uns dabei auf die Angaben der Firma verlassen", so Hesse. "Ich sehe allerdings keine Motivation, hier nicht die Wahrheit zu sagen." Eine zusätzliche externe Sicherheitsüberprüfung sei ja eigentlich von Vorteil für das Unternehmen.

Beim neuen System liegt die Kopie des Schlüssels nicht mehr wie bisher bei der Firma, sondern auf einem eigenen, besonders sicheren Computer, auf den das Unternehmen keinen Zugriff hat und dessen Code nachträglich nicht geändert werden kann. Wenn eine Userin oder ein User das Smartphone verliert, kann sie oder er nun selbst durch ein Passwort auf den Schlüssel zugreifen und die eigenen Chats wiederherstellen. "Der Schlüssel ist gewissermassen in einer Truhe abgelegt, die nur durch das Passwort geöffnet werden kann", so Hesse.

Kostenloser Peer Review dank Transparenz

Ausserdem schützt das Protokoll das Backup vor sogenannten "Brute Force Angriffen", bei denen so lange Passwörter durchprobiert werden, bis das richtige gefunden ist. "Das System erlaubt selbst einem mächtigen Angreifer, der Server von Whatsapp unter Kontrolle bringt, nur zehn Versuche, dann wird der Schlüssel zerstört", so Hesse. Die Daten sind dann allerdings auch für die Nutzenden verloren.

Bei dieser Funktion entdeckten die Forschenden eine mögliche Schwachstelle: Eigentlich löscht das System alte Versionen des Backups, wenn eine neue Version erstellt wird - etwa beim Ändern des Passworts. "Ein Angriff von Whatsapp oder ausserhalb könnte dafür sorgen, dass die alten Versionen erhalten bleiben und so für jede noch existierende Version zehn zusätzliche Versuche möglich sind", so Hesse. Durch Wahl eines starken Passworts könne man dieses Hintertürchen aber schliessen. "Wenn man nicht seine Schweizer Postleitzahl, sondern mindestens acht Zeichen mit Sonderzeichen wählt, ist es egal, ob ein Angreifer zehn oder zweihundert Versuche hat."

Erhöht sich die Gefahr für potenzielle Angriffe nicht, wenn das Sicherheitsprotokoll inklusive möglicher Schlupflöcher detailliert publiziert wird, wie in dieser Studie geschehen? "In der Forschung ist man mittlerweile davon überzeugt, dass eine formale und öffentlich zugängliche Beschreibung des Protokolls die Sicherheit erhöht", so Hesse. So können andere Fachleute noch einmal alles genau anschauen oder neue Aspekte prüfen. "Das ist quasi ein kostenloser Peer Review Prozess, der sehr viel mehr wert ist, als wenn die Firma das Protokoll unter Verschluss halten würde."

G. T. Davies et al.: Security Analysis of the WhatsApp End-to-End Encrypted Backup Protocol. Crypto IACR (2023).

Der Text dieser News und weitere Informationen stehen auf der Webseite des Schweizerischen Nationalfonds zur Verfügung.

Pressekontakt:

Julia Hesse;
IBM Research Zürich;
Säumerstrasse 4;
8803 Rüschlikon;
Tel.: +41 43 538 72 79;
E-Mail: juliahesse2@gmail.com