Sicherheitsmängel in Gesundheits-App Vivy

Bereits fünf Tage nach dem Start der elektronischen Gesundheitsakte Vivy haben Sicherheitsforscher der Firma Modzero Mängel darin entdeckt.

Eine Funktion, mit der Patienten ad hoc Dokumente mit ihrem Arzt teilen können, sei konzeptionell **nicht ausreichend geschützt** gewesen. Das Problem: Der Arzt erhält für den Abruf der Dokumente vom Vivy-Server eine URL, die ein Angreifer jedoch erraten könnte. Für den Arzt bestimmte Dokumente seien damit für Dritte lesbar gewesen, bis der Arzt sie herunterlädt. Selbst wenn der Arzt schneller gewesen wäre, hätten Angreifer immer noch Metadaten des Patienten sowie den Arztnamen einsehen können. Die Dokumenten-URLs schickte die App zudem an vier Drittanbieter in den USA und Singapur.

Modzero monierte überdies Schwächen in der Ende-zu-Ende-Verschlüsselung. Sie chiffriert die Kommunikation zwischen der Smartphone-App des Patienten und dem Browser des Arztes. Wäre es einem Angreifer gelungen, unbemerkt die Vivy-Server zu kompromittieren, hätte er die Web-App auf der Arztseite manipulieren können. Hinzu kam ein Cross-Site-Scripting-Fehler. Diesen hätten ein Patient oder sein unbemerkt manipuliertes Smartphone ebenfalls dazu missbrauchen können, Code im Browser des Arztes auszuführen.

Vivy hat die Lücken nach einer vertraulichen Meldung am 21. September umgehend geschlossen. In einer eigenen Mitteilung spricht das Unternehmen von „hypothetischen Angriffsvektoren“ mit „vielen spezifischen Annahmen“. Für einen Großteil der Angriffe sei es erforderlich gewesen, den Computer des Arztes oder die Smartphone-Installation des Patienten zu manipulieren. *(mon@ct.de)*

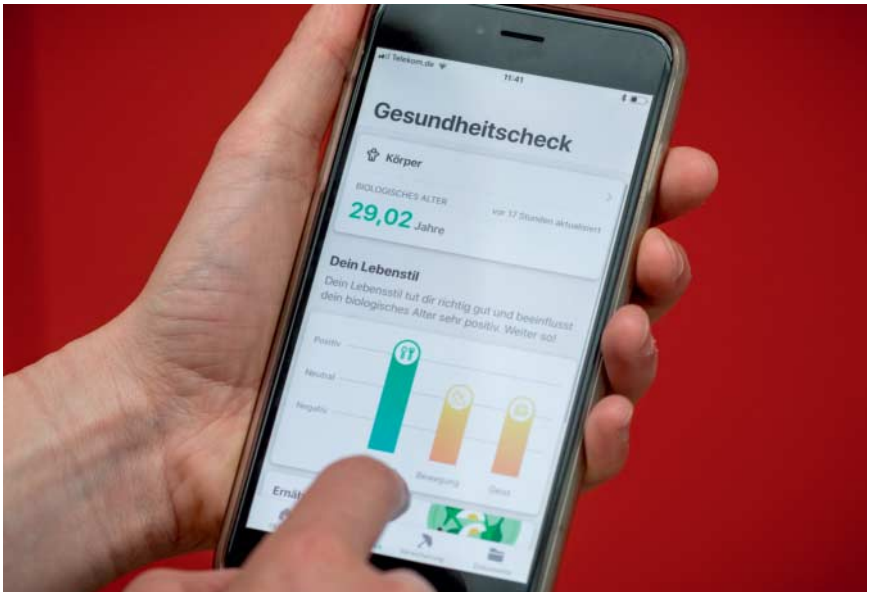


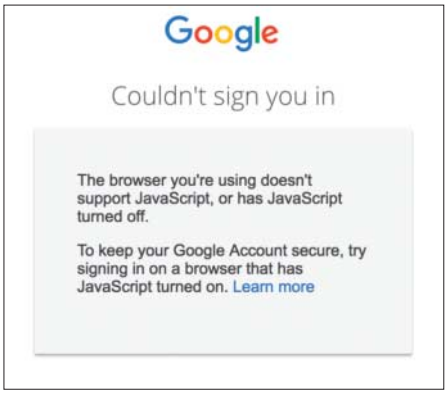
Bild: dpa, Michael Kappeler

In der App Vivy hätten Angreifer Patientendaten einsehen können.

Google-Log-in nur noch mit JavaScript

Google will die Accounts seiner Nutzer künftig besser schützen. Bereits beim **Browser-Log-in** wird nun geprüft, ob alles mit rechten Dingen zugeht: „Wir führen eine Risikobewertung durch und erlauben die Anmeldung nur, wenn nichts verdächtig erscheint“, teilte der Konzern mit. Ohne aktiviertes JavaScript funktioniert diese Sicherheitsmaßnahme allerdings nicht.

Den meisten Google-Kunden wird das egal sein, denn die große Mehrheit surft mit aktiviertem JavaScript durchs Netz. Nur „eine kleine Minderheit“ entscheide sich dafür, die Skriptsprache lieber abgeschaltet zu lassen, erklärte Google – und verwies auf 0,1 Prozent der Nutzer, die ohne JavaScript unterwegs sind. Diese Anwender müssen JavaScript zumindest für den Log-in einschalten. Ein alternatives Anmeldeverfahren gibt es nicht. *(dbe@ct.de)*



Ohne aktiviertes JavaScript ist kein Log-in im Browser möglich.

Aus 1&1 wird 1&1 Ionos

1&1 bündelt seine **Webhosting- und Cloud-Angebote** unter der neuen internationalen Dachmarke „1&1 Ionos“. Das neue Unternehmen integriert die Produkte des vor einem Jahr von 1&1 zugekauften Cloud-Anbieters ProfitBricks und will sich auch als Plattform-Anbieter im PaaS-Segment etablieren.

1&1 Ionos soll insbesondere kleine und mittelständische Unternehmen ansprechen, denn hier liege das größte Wachstumspotenzial im Hosting- und Cloud-Markt, erläuterte 1&1-Marketing- und Vertriebsvorstand Christian Böing. Böing ist gleichzeitig Chef des Webhosters Strato, der wie 1&1 Teil des United-Internet-Konzerns ist. Strato und andere auf nationalen Märkten eingeführte Marken sollen weiter bestehen bleiben. *(hob@ct.de)*