Nutzlose Passwörter

Gesundheitsdaten zweier populärer Apps waren jahrelang ohne Prüfung abrufbar

Die Backend-Server der beiden Gesundheits-Apps „Sanitas Health Coach“ und „HealthForYou“ der Hans Dinslage GmbH gaben jahrelang Gesundheitsdaten preis. Betroffen sein könnten über 1,5 Millionen Nutzer.

Von Hartmut Gieselmann

Smarte Fieberthermometer, Waagen, Blutdruck- und Pulsmessgeräte bekommt man inzwischen selbst beim Discounter für ein paar Euro. So auch von Silvercrest, einer Hausmarke von Lidl. Der Aktivitätssensor „SAS 88“ für 27,99 Euro sowie das Thermometer „SFT 81“ für 24,99 Euro geben ihre Messdaten beispielsweise an die kostenlose App „HealthForYou“ weiter. Entwickelt wurde sie von der Hans Dinslage GmbH, einer Tochter der Beurer GmbH aus Ulm.

Neben HealthForYou bietet Hans Dinslage auch die App „Sanitas Health Coach“ für Android und iOS an, die beispielsweise Daten von der Bluetooth-Waage SBF 70 sammelt. Beide Apps sind überaus populär: Laut Googles Play Store wurden allein die Android-Versionen zusammen über 1,5 Millionen mal heruntergeladen.

Anwender können bei beiden Apps Nutzerkonten anlegen und eine Reihe persönlicher Daten übermitteln, darunter Name, Geburtsdatum, Größe, Geschlecht und Mailadresse. Kombiniert werden die Infos mit Messprotokollen der per Bluetooth gekoppelten Geräte: Gewicht, Blutdruck, Puls, Sauerstoffgehalt im Blut, Körpertemperatur, Schlafdauer, gegangene Schritte und getrunkene Wassermenge. Die Apps laden die Informationen in die Server-Cloud der Hans Dinslage GmbH. Gespeichert werden sie laut Hersteller in zwei deutschen Rechenzentren des Dienstleisters Dynamic 1001. Wer sich mit dem Konto von einem anderen Smartphone oder Browser anmeldet, kann die Daten herunterladen und neue Messwerte aufspielen.

Das ist praktisch, um seine Fitness- und Gewichtsfortschritte über einen längeren Zeitraum zu beobachten. Doch leider konnten jahrelang auch Dritte die Daten abrufen. Dazu mussten sie die Mail-Adresse des Nutzers wissen oder erraten und beim Server eine gezielte Anfrage stellen (HTTPS POST Request). Der plauderte drauflos, ohne ein vom Nutzer angegebenes Passwort zu prüfen. Mehr noch: Der Server verriet auch den Hashwert und Salt des echten Nutzerpassworts. Mit Mailadresse und Passwort-Hash konnte sich ein Angreifer anschließend ein API-Token ausstellen lassen, das uneingeschränkten Zugriff auf das Konto ermöglichte.

Bild: Beurer

Die betroffene App „HealthForYou“ wird oft mit smarten Gesundheits-Gadgets der Marke Silvercrest des Discounters Lidl gekoppelt.

Lücke seit 2015

Gefunden hat die kritische Sicherheitslücke Nick Decker von der Trovent Security GmbH in Bochum. Vier Tage lang analysierte er die Android-Apps und ihren Datenverkehr mit den Backend-Servern, bevor er die fehlerhafte Informationsherausgabe des Servers erkannte und Alarm schlug. Trovent setzte Hans Dinslage und Beurer am 28. April in Kenntnis, woraufhin der App-Hersteller die Server am folgenden Tag vom Netz nahm, um den Fehler zu reparieren. Am 30. April informierte Beurer den zuständigen Datenschutzbeauftragten von Baden-Württemberg.

Auf Nachfrage von c't gab Beurer die Sicherheitslücke unumwunden zu. Laut Firmenangabe bestand die Serverlücke bei „Sanitas Health Coach“ seit September 2015 und bei „HealthForYou“ seit November 2017. Allerdings fand die Firma nach eigenen Aussagen keine Hinweise darauf, dass die Sicherheitslücke von Angreifern ausgenutzt wurde. Zur Anzahl der von der Lücke betroffenen Nutzerkonten wollte sich Beurer nicht äußern.

Gesalzene Hashes

Nutzer der App „Sanitas Health Coach“ können nicht prüfen, ob ihr Konto kompromittiert wurde. Anwender der HealthForYou-App sollten laut Trovent zumindest ihr Mail-Postfach checken: Die Server verschicken eine Mail, wenn sich ein Nutzer von einem neuen Gerät aus beim Online-Konto anmeldet. Wer solche Benachrichtigungen entdeckt und nicht zuordnen kann, ist womöglich Opfer eines Angriffs geworden.

Da potenzielle Angreifer neben sensiblen Gesundheitsdaten auch Passwort-Hashes samt Salts erbeuten konnten, rief Beurer sämtliche registrierten Nutzer beider Apps nach Pfingsten per Mail auf, ihre Passwörter zu ändern. Mit Erscheinen dieses Heftes werden alle übrigen Passwörter automatisch zurückgesetzt und müssen von Anwendern neu gewählt werden. Da der Hersteller für die Hashes und Salts das weitgehend sichere Verfahren „bcrypt“ eingesetzt hat, ist eine Rekonstruktion der Passwörter nahezu ausgeschlossen – zumindest solange Nutzer nicht allzu kurze oder unterkomplexe Passwörter benutzt haben. *(hag@ct.de)* c't

Sicherheits-Infos von Trovent: ***ct.de/y9bj***