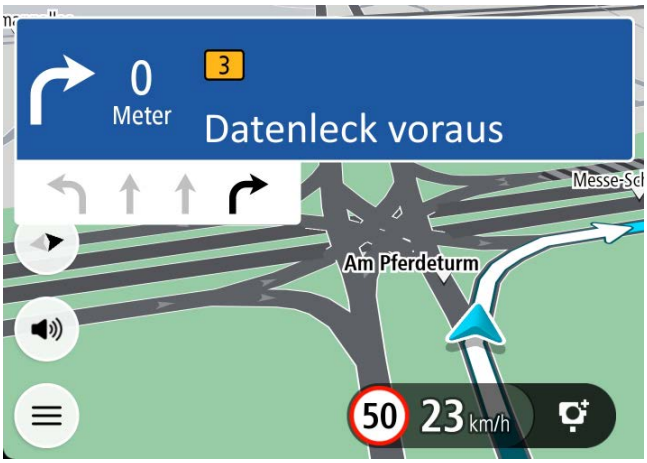
Datenleckleck bei TomTom

Rechnungsdaten unzureichend geschützt



Bildmontage: c't

Auf triviale Weise ließen sich unzählige Online-Rechnungen von TomTom-Kunden unbefugt abrufen. Betroffen sind auch Teilnehmer einer Gratis-Aktion. Ein Fall für die DSGVO.

Von Ronald Eikenberg

Ende Oktober setzte sich ein anonymer Hinweisgeber mit dem Investigativteam der Heise-Redaktionen in Verbindung. Seine Nachricht enthielt einen langen Link auf die TomTom-Website sowie den besorgniserregenden Hinweis: „In der URL lässt sich der Parameter `orderId` frei verändern und man kann alle Daten anderer Bestellungen sehen (Name, Adresse, Land, Preis, bestellter Artikel usw.)." Das wäre höchst problematisch, da es sich um personenbezogene Daten im Sinne der Datenschutzgrundverordnung (DSGVO) handelt.

Laut unseres Tippgebers war ein TomTom-Account die einzige Voraussetzung für den Zugriff auf die Kundendaten des Unternehmens. Um der Sache nachzugehen, legten wir einen an: Die Registrierung dauerte nur eine Minute , es war nicht nötig, einen Kauf zu tätigen. Anschließend steuerten wir die URL aus dem Hinweis an: Uns wurde die Rechnung einer uns fremden Person präsentiert. Wie vom Informanten geschildert konnten wir nicht nur die bestellten Artikel und die dazugehörigen Kaufpreise sehen, sondern auch den Namen und die Anschrift des Bestellers. Zudem war es möglich, die Rechnung im PDF-Format zu speichern.

Leicht zu erraten

Damit wir das Ausmaß des Datenlecks einschätzen konnten, änderten wir die neunstellige `orderID` in der URL geringfügig, indem wir sie um eins hochzählten. Und auch dieses Mal lieferte uns TomTom eine vollständige Online-Rechnung, allerdings von einem ganz anderen Kunden. Bei weiteren Stichproben mit größeren Differenzen zur ursprünglichen ID landeten wir fast immer weitere Treffer, was die Vermutung nahelegt, dass die ID nicht zufällig generiert, sondern schlicht bei jeder Bestellung hochgezählt wird.

Auf diese Weise waren sämtliche Online-Rechnungen abrufbar. Ein Angreifer hätte ein Skript eingesetzt, das die IDs hochzählt, um alle Rechnungen abzurufen. Mit einer niedrigen Frequenz und wechselnden IP-Adressen, etwa durch den Einsatz eines Botnets, wäre dies vermutlich im Grundrauschen der Website untergegangen. Solche trivial ausnutzbaren Fehler dürften zu den häufigsten Ursachen für unberechtigte Datenabflüsse zählen. Derartige Datenlecks treten auf, wenn der Server nicht überprüft, ob der Nutzer berechtigt ist, die zu einer bestimmten ID gespeicherten Daten abzurufen. Das ist insbesondere dann fatal, wenn die IDs nach einem leicht durchschaubaren Muster aufgebaut sind oder schlicht hochgezählt werden.

TomTom reagiert

Nachdem wir das Datenleck verifiziert hatten, setzten wir uns umgehend mit TomTom in Verbindung. Das Unternehmen versprach, den Sachverhalt zu überprüfen. Wenige Tage später meldete sich der Navi-Hersteller erneut bei uns: „Sobald wir auf das Problem mit unserem Webshop aufmerksam gemacht wurden, stellten wir sofort sicher, dass die Rechnungsdaten unserer Kunden für andere Besucher unserer Website nicht mehr einsehbar waren." Tatsächlich war es fortan nicht mehr möglich, Rechnungen fremder Kunden abzurufen. Doch wie konnte es zu dem Datenleck kommen?

„Die Schwachstelle bestand vom 20. August 2020 bis zum 30. Oktober 2020 als Folge eines neuen Software-Updates", erklärte TomTom gegenüber c't. Anzeichen für einen böswilligen Angriff konnte das Unternehmen nach eigenen Angaben nicht feststellen.

TomTom zählte Fremdzugriffe auf die Rechnungen von lediglich 172 Kunden. In Anbetracht der Tatsache, dass der Navi-Hersteller wohl mehrere Millionen Nutzer haben dürfte, ist diese Zahl überschaubar. Bei unseren Stichproben stellten wir fest, dass auch Nutzer betroffen sind, die im Oktober die eigentlich kostenpflichtige Navi-App „TomTom Go" mit einem Gutscheincode für ein Jahr gratis bezogen haben. Diese Aktion dürfte auf reges Interesse gestoßen sein, aus Schnäppchenjägern wurden so registrierte TomTom-Kunden.

Behörde eingeschaltet

Die DSGVO schreibt vor, dass derartige Zwischenfälle unmittelbar an die zuständige Behörde gemeldet werden müssen. TomTom hat den Vorfall offenbar ernst genommen und „innerhalb von 72 Stunden nachdem auf die Schwachstelle hingewiesen wurde bei der niederländischen Behörde für den Schutz personenbezogener Daten gemeldet", erklärte das Unternehmen. Die 172 Kunden, auf deren Daten zugegriffen wurde, hat der Navi-Anbieter inzwischen darüber in Kenntnis gesetzt.

(rei@ct.de) c't

Ihr Hinweis an heise Investigativ:
https://heise.de/investigativ