2016/01 Lifestyle

https://shop.jungle.world/artikel/2016/01/twitter-tor-und-sponsored-attacks

Staatliche Hacker greifen Tor-Nutzer über Twitter an

Twitter, Tor und Sponsored Attacks

Von **Enno Park**

Mitte Dezember warnte Twitter einige seiner Nutzer, möglicherweise Opfer einer Hackerattacke in staatlichem Auftrag geworden zu sein. Was genau passierte, ist noch immer unklar. Die Angriffe lösten jedoch eine erneute Debatte um die Sicherheit des Anonymisierungsdienstes Tor aus, den die meisten Betroffenen nutzten.

Die E-Mail, die Twitter an einige Nutzer verschickte, war von der unangenehmen Sorte: »Rein vorsorglich möchten wir Sie darüber informieren, dass Ihr Account zu einer kleinen Gruppe von Accounts gehört, die Ziel eines staatlich motivierten Hackerangriffs geworden sein könnte. Das bedeutet, dass die Hacker möglicherweise mit einer Regierung in Verbindung stehen. Wir vermuten, dass Daten und Informationen wie zum Beispiel E-Mail-Adressen, IP-Adressen und Telefonnummern ausspioniert werden sollten.« Welcher Staat dahinter stecken könnte und anhand welcher Indizien man auf die Angriffe aufmerksam geworden war, mochte Twitter nicht verraten. Man untersuche die Vorfälle weiterhin. Das ist verständlich, schließlich hat Twitter kein Interesse, die Methoden offenzulegen, mit denen der Kurznachrichtendienst Angriffe erkennt. Es war das erste Mal, dass eine solche Warnung vor »Sponsored Attacks«, wie Angriffe von Hackergruppen im Auftrag von Staaten auch genannt werden, von Twitter herausgegeben wurde. Andere große Internetunternehmen wie Facebook und Google verhalten sich in solchen Fällen seit einiger Zeit ähnlich.

Die E-Mail ging an Nutzer aus etlichen Ländern, von der Schweiz bis Indien. Sie haben gemeinsam, dass sie sich für mehr Privatsphäre im Internet einsetzen, gegen staatliche Überwachung oder gegen Zensur im Netz kämpfen – aber auch, dass sie bis auf wenige Ausnahmen den Anonymisierungsdienst Tor verwenden. Betroffen sind beispielsweise die kanadische Hackerorganisation »Coldhak« und die deutsche Politologin Anne Roth. Vor allem sie dürfte diese E-Mail an unangenehme Zeiten erinnern. Als 2007 ihr Lebensgefährte Andrej Holm wegen Verdachts auf Mitgliedschaft in einer terroristischen Vereinigung für mehrere Wochen in Untersuchungshaft war, musste sie am eigenen Leib erfahren, wie sich staatliche Überwachung anfühlt. Die abgehörte Telefonanlage spielte verrückt und Ermittler drangen während ihrer Abwesenheit in ihre Wohnung ein. Die

Vorwürfe gegen Holm erwiesen sich als haltlos. Der Soziologe war ins Raster einer Internetüberwachung geraten, weil er Worte wie »Gentrifizierung« und »Prekariat« in seinen Schriften verwendete. Heute ist Anne Roth Referentin für die Fraktion »Die Linke« und arbeitet im NSA-Untersuchungsausschuss, ist aber auch als feministische Bloggerin bekannt.

Der Informatiker Jens Kubieziel, der ebenfalls eine E-Mail von Twitter erhalten hat, bleibt gelassen. Der Kyptographieexperte schult Mitarbeiter von Unternehmen in der Umgehung von Zensurmaßnahmen – ebenfalls ein Anwendungszweck von Tor. Alles, was er auf Twitter tue, sei ohnehin öffentlich, so dass eine Überwachung über Twitter kein Problem sei. Tatsächlich scheinen sich die Angreifer eher nicht für Metadaten – also wer wann mit wem kommuniziert hat – zu interessieren. Die sind auf Twitter ohnehin weitgehend öffentlich. Während die Hintergründe der Angriffe völlig im Dunkeln bleiben, empfiehlt Twitter den Leitfaden der »Electronic Frontier Foundation« zur Absicherung von Social-Media-Konten. Der beinhaltet unter anderem den Rat, Tor zu verwenden. Das ist nicht ohne Ironie, da häufiger berichtet wird, dass Nutzer sich nicht bei Twitter anmelden können, wenn sie Tor verwenden. Tor scheint der kleinste gemeinsame Nenner hinter den Angriffen zu sein, was auch Anne Roth in ihrem Blog als »Arbeitshypothese« vermutet. Ursprünglich stand die Abkürzung Tor für »The Onion Router«. Eine Technik, die Internetverkehr dadurch anonymisieren soll, dass die Absender verschleiert werden. Das geschieht, indem der Datenverkehr über mehrere Rechner geleitet wird – wie bei den Schichten einer Zwiebel. Die heute unter dem Namen Tor verwendete Technik weicht allerdings in einigen Details vom ursprünglichen Gedanken ab und gilt als weniger sicher. Die Grundidee bleibt: Datenverkehr wird verschlüsselt und üblicherweise über drei sogenannte Tor-Knoten geleitet, so dass am Ende nicht mehr festgestellt werden kann, von wo sie stammen. Theoretisch sollte das ausreichen, um Aktivitäten im Netz zu verschleiern, allerdings gilt Tor nur so lange als sicher, wie nicht größere Teile des Internet permanent überwacht werden. Doch genau das geschieht seit einigen Jahren, wie auch die Enthüllungen von Edward Snowden belegen.

Innerhalb des Tor-Netzwerks befinden sich zahlreiche versteckte Server: das Darknet. In der Öffentlichkeit ist es vor allem als Umschlagplatz für Drogen, Waffen, Kinderpornographie oder von Hackern erbeuteten Kreditkartendaten berühmt geworden. Dabei darf keinesfalls übersehen werden, dass Tor auch von unbescholtenen Menschen genutzt wird, um ihre Privatsphäre aufrechtzuerhalten, und natürlich auch von Dissidenten in totalitären Staaten, die damit eine bestehende Internetzensur umgehen können. Kurz, Ermittlungsbehörden etlicher Länder interessieren sich aus einer Reihe von Gründen brennend für Tor und seine Nutzer. Wer Tor benutzt und dabei erwischt wird, dürfte sich durchaus verdächtig machen. Anne Roths These ist also keinesfalls unwahrscheinlich. Prompt begann eine Debatte um die Sicherheit von Tor. So warnte der Internetaktivist Alvar Freude unter der Überschrift »Du wirst staatlich gehackt, weil Du Tor nutzt!?!« in seinem Blog, die Nutzung von Tor erhöhe die Risiken für normale Anwender, statt sie zu senken. Der Streit wurde unter anderem auf dem Blog Netzpolitik.org ausgetragen, wo Constanze Kurz, Sprecherin des Chaos Computer Clubs, Alvar Freude polemisch angriff: »Die deutsche Marlene Mustermann darf besser brav ihren Browser starten, ihr Surfverhalten protokollieren und sich blinkende Werbung anzeigen lassen, sich nebenbei

Schadsoftware über Werbenetzwerke einfangen und dann im Urlaub nicht mal mehr ihre Lieblingswebsites anschauen?« Jacob Appelbaum, Journalist und Mitglied des Tor-Netzwerks, hält Tor weiterhin für sicher und vermutet, Twitter selbst sei gehackt worden, wolle dies aber nicht verraten.

Alvar Freudes Kritik ist berechtigt. Schließlich funktioniert das Werbetracking, das Constanze Kurz beschreibt, über Cookies und Viren. Die finden unter anderem durch den Aufruf verseuchter Websites den Weg auf den Rechner. Da helfen vor allem Browser-Erweiterungen wie »Ghostery« und Antivirenprogramme, aber eher nicht die Nutzung von Tor. Stattdessen häufen sich die Hinweise darauf, wie unsicher Tor ist. So zeigte 2013 ein Experiment an der Georgetown University, wie leicht die Identität von Tor-Nutzern festgestellt werden kann. Die Forscher protokollierten sechs Monate lang den Datenverkehr im Tor-Netzwerk und waren anschließend in der Lage, die Identität von 80 Prozent der Nutzer zu bestimmen. Fachleute vermuten, dass das mit einer besseren Infrastruktur, wie Geheimdienste sie betreiben, auch in kürzerer Zeit möglich ist. 2014 wurde die »Operation Onymous« des FBI bekannt. Gemeinsam mit europäischen Behörden konnte die US-amerikanische Bundespolizei die Identität etlicher Tor-Nutzer herausfinden, was zu 17 Verhaftungen führte. Unbekannt ist allerdings, welche Techniken die Ermittler verwendet haben – denkbar wäre zum Beispiel auch das Verfolgen von Transaktionen in der Onlinewährung Bitcoin gewesen.

Um Tor zu kompromittieren, genügt es, dass Angreifer selbst einen Tor-Knoten betreiben – was allen Anwendern freisteht. Zudem machen Tor-Nutzer oft den Fehler, dass sie zwar Tor verwenden, aber ansonsten nicht auf Verschlüsselung achten oder sich mit ihrem Namen oder ihrer E-Mail-Adresse bei einem Online-Dienst anmelden, was alle Bemühungen um Verschleierung zunichte macht. Filesharer, die durch die Verwendung von Tor einer Verfolgung entgehen wollen, wenn sie im Netz Filme und Musik tauschen, können sich kaum zurücklehnen: Nur bestimmte Teile des Datenverkehrs bei der Nutzung von Bittorrent werden überhaupt durch Tor geleitet.

Tor ist also allenfalls ein Dienst für versierte Anwender, die genau wissen, was sie tun. So hat auch die Mozilla Foundation Pläne, Tor fest in ihren Browser Firefox einzubauen, auf Eis gelegt. Die Fronten in diesem Streit bleiben verhärtet. Kritiker sehen in Tor ein unwirksames Mittel, das im Zweifel Kriminellen hilft, ihre Taten zu verschleiern, während Befürworter meinen, die aktuelle Diskussion sei eine Kampagne, um die Menschen im Netz davon abzuhalten, Tor zu nutzen. Während die Debatte tobt, ist ihr Auslöser anscheinend vergessen: was nämlich genau hinter den Hackerangriffen steckt, die Twitter gemeldet hat.