idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Freie Universität Berlin
Kerrin Zielke

17.06.2013
http://idw-online.de/de/news538851

Forschungsprojekte
Gesellschaft, Informationstechnik, Mathematik, Medien- und Kommunikationswissenschaften, Wirtschaft
überregional

Gefahren für Informanten bannen

Der Informatikprofessor Volker Roth von der Freien Universität Berlin forscht im AdLeaks-Projekt an einem System, mithilfe dessen eine Person bei der Datenübertragung über das Internet unerkannt bleibt. Eine unerkannte Datenübertragung ist etwa für sogenannte Whistleblower relevant, Personen, die interne Informationen öffentlich machen, um über Missstände zu informieren. Beispiele sind Mark Klein und zuletzt Edward Snowden, die enthüllt haben, in welchem Umfang der US-amerikanische Geheimdienst NSA (National Security Agency) das Internet überwacht.

Die aktuelle Diskussion konzentriert sich stark auf das nun bekannt gewordene PRISM-Programm. Dieses ermöglicht der NSA den Zugriff auf Nutzerdaten, die Google, Apple, Microsoft und andere Firmen speichern. Dabei gerät in den Hintergrund, dass die NSA auch Daten direkt von Glasfaserverbindungen abzweigt, über die große Teile der Kommunikation im Internet laufen. Hiervon sind die Inhalte der Kommunikation betroffen, aber auch die einfach zu speichernden Verbindungsdaten, aus denen hervorgeht, wer wann mit wem kommuniziert.

„Man muss die Zivilcourage von Edward Snowden bewundern, der seine Zukunft für seine rechtsstaatliche Überzeugung opfert, indem er Missstände aufdeckt“, sagt der Informatikprofessor Volker Roth. Nicht alle Whistleblower wagen den Schritt in die Öffentlichkeit, der häufig mit Stigmatisierung, dem Verlust des Arbeitsplatzes oder Strafverfolgung einhergeht. „Auch Whistleblower, die unerkannt bleiben wollen, gehen Risiken ein, wenn sie über das Internet Informationen weitergeben, denn die von der NSA gesammelten Verbindungsdaten erlauben es, einmal getätigte Anrufe oder Internetverbindungen weit in die Vergangenheit zurückzuverfolgen.“ Daran würde auch eine Verschlüsselung nichts ändern. Deswegen empfehle sich die Nutzung von Anonymisierungsdiensten wie „Tor“, die Verbindungen über mehrere Rechner leiten und deren Herkunft verschleiern. Die Zeitschrift „The New Yorker“ rate potenziellen Whistleblowern ebenfalls zu dieser Vorgehensweise, um anonym Informationen an den eigenen Strongbox-Dienst zu übermitteln.

Ob dieser Schritt bei einem Dienst wie der NSA ausreicht, sei jedoch noch unklar. „Schon durch die Nutzung von Tor könnte man sich verdächtig machen“, erklärt Volker Roth. Das Tor-Netzwerk versuche zudem, eine geringe Latenz von Verbindungen herzustellen, was unter Umständen eine Verkehrsanalyse ermögliche. Hierbei misst ein Abhörer, wann Nutzer Daten senden und wann Daten am Zielrechner ankommen. Bei ausreichender Übereinstimmung ließen sich so Verbindungen Personen zuordnen. „Wenn sowohl Nutzer als auch Server ihren Sitz in den USA haben, könnte die NSA in der Lage sein, eine solche Verkehrsanalyse auszuführen“, sagt Roth.

Diese Gefahr durch eine Verkehrsanalyse veranlasste ihn, gemeinsam mit Studenten nach einer Lösung zu suchen. In Kooperation mit dem Informatikprofessor Sven Dietrich vom Stevens Institute of Technology in New Jersey entwickeln sie ein System, das auch unter einer Vollüberwachung des Internets eine Datenübermittlung erlaubt, die nicht ohne Weiteres zurückverfolgt werden kann.

Das sogenannte AdLeaks-System nimmt den Verbindungsdaten ihre Bedeutung. Es macht sich kleine Programme zunutze, mit denen die meisten Websites dynamisch und interaktiv gestaltet werden. Eingebracht in populäre Websites,

verschlüsselt und übermittelt ein solches Programm automatisch leere Nachrichten an die AdLeaks-Server, wann immer eine solche Website aufgerufen wird. Whistleblower können einen modifizierten Browser verwenden, der anstelle leerer Nachrichten vertrauliche Nachrichten verschlüsselt. Ein Überwacher, der das Internet beobachtet, kann beide Arten von Nachrichten nicht unterscheiden. Er kann auch keine Erkenntnisse aus den Verbindungsdaten ziehen, weil alle Internetnutzer gleichermaßen Daten übermitteln und daher keinerlei Absicht vermutet werden kann. Die notwendige Software wird auf ähnliche Weise an alle Nutzer verteilt, ohne heruntergeladen werden zu müssen.

Das AdLeaks-System wird derzeit im Rahmen des EU-Projekts CONFINE untersucht und getestet. Eine erste Version des Quellcodes ist zum Download verfügbar.

Weitere Informationen
Professor Dr. Volker Roth, Stiftungsprofessur der Bundesdruckerei GmbH für Sichere Identität am Institut für Informatik der Freien Universität Berlin, Telefon: 030 838-75281, E-Mail: volker.roth@fu-berlin.de

URL zur Pressemitteilung: http://www.adleaks.org