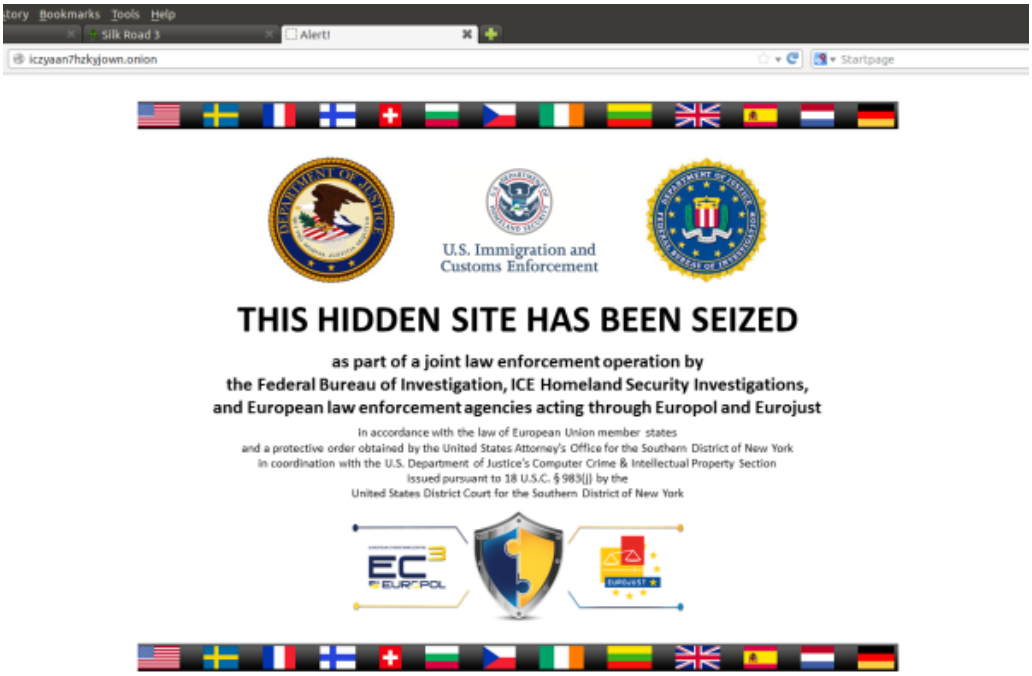
Gefahr für Whistleblower: Tor-Netzwerk fürchtet um Anonymität im Netz

Deutsche Wirtschafts Nachrichten |
Veröffentlicht: 13.11.14

Die Geheimdienste sind möglicherweise in der Lage, die anonyme Kommunikation über das Tor-Netzwerk zu knacken. Dies halten die Macher des Tor-Projekts selbst für möglich, nachdem die Behörden aus 17 Staaten bei einer gemeinsamen Razzia mehr als 50 im Dark Web versteckte Seiten vom Netz genommen haben. Das Risiko für Whistle-Blower und Regierungsgegner ist offenbar höher als bisher angenommen.



Nachdem die Behörden dutzende illegale Webseiten des Dark Webs auffinden und sperren konnten, wachsen die Zweifel an der Anonymität bei der Nutzung des Tor-Netzwerks. (Screenshot)

Nach der erfolgreichen **weltweiten Razzia gegen rund 50 illegale Webseiten** wächst die Sorge, dass der Tor-Browser die Anonymität der Nutzer im Internet nicht mehr ausreichend sicherstellen kann. Die Behörden haben möglicherweise einen Weg gefunden, die Verschleierung von IP-Adressen zu knacken. Dadurch wird es etwa für Whistleblower und Regierungsgegner künftig noch gefährlicher, sich über das Internet Gehör zu verschaffen.

In der vergangenen Woche führten die USA, Deutschland und 15 weitere Staaten gemeinsam die bisher größte Strafverfolgungsaktion gegen Webseiten des Tor-Netzwerks durch. Dabei handelt es sich um Online-Märkte wie die Silk Road 2.0, wo die Kunden illegale Produkte erwerben konnten, vor allem Drogen.

Die beschlagnahmten Webseiten befinden sich im sogenannten „Dark Web", das nur mit dem Tor-Browser zugänglich ist. Dieser Webbrowser verschleiert die IP-Adressen der Nutzer, was ihnen Anonymität verschaffen soll. Doch durch die koordinierte Aktion der vergangenen Woche hat das Vertrauen in den Tor-Browser einen erheblichen Schlag erhalten.

Das Entwicklerteam von Tor ist selbst ratlos, wie die Behörden die Identitäten von so vielen versteckten Webseiten in Erfahrung bringen konnten. „Wir waren genauso überrascht wie Sie", so das Tor Project. Es rechnet jedoch damit, dass bald geklärt werden kann, wie die Behörden an die Informationen gelangen konnten.

„In freiheitlichen Demokratien sollten wir erwarten, dass wenn die Zeit gekommen ist, einige der 17 Verhafteten anzuklagen, dass die Polizei dann dem Richter erklären muss, wie die Verdächtigen zu Verdächtigen wurden,

und als positiver Nebeneffekt der Justiz-Aktion, dass Tor dann erfahren könnte, ob es irgendwelche Sicherheitslücken bei den versteckten Diensten oder anderen entscheidenden mit dem Internet verbundenen Diensten gibt."

Die Behörden hatten unter anderem den 26-jährigen Blake Benthall verhaftet, der den Online-Markt Silk Road 2.0 betrieben haben soll. Benthall droht nun eine lebenslange Haftstrafe wegen des Handels mit illegalen Medikamenten. Gut ein Jahr zuvor wurde ebenfalls in San Francisco der angebliche Betreiber der ersten Silk Road, Russ Ulbricht, verhaftet. Sein Verfahren beginnt im Januar.

Nach Angaben von Europol haben die Behörden weltweit „mehr als 410 versteckte Dienste" vom Netz genommen. Es wurden 17 Personen festgenommen. Zudem beschlagnahmten die Behörden nach eigenen Angaben rund 1 Million Dollar in Bitcoin, 180.000 Euro Bargeld, Drogen, Gold und Silber.

Die Behörden nannten ihre Aktion „Operation Onymous", womit sie zum Ausdruck bringen, dass sie im Internet keine *An*onymität dulden wollen. Troels Oerting, der Chef des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, sagte:

„Lange Zeit haben Kriminelle gedacht, dass sie unerreichbar sind, wenn sie Tor verwenden. Wir können nun zeigen, dass sie weder unsichtbar noch unberührbar sind. Die Kriminellen können rennen, aber sie können sich nicht verstecken. Und unsere Arbeit geht weiter."

Betroffen sind nach Angaben des FBI neben der Silk Road 2.0 mindestens zwei Dutzend weitere Online-Märkte. Bisher hat das FBI eine Liste mit 27 Webseiten veröffentlicht, die allesamt „illegale Produkte und Dienstleistungen" angeboten haben.

Die Silk Road 2.0 und 13 weitere beschlagnahmte Seiten verkauften illegale Drogen. Andere Seiten verkauften gestohlene oder gefälschte Kreditkarten. Außerdem hatten sie Falschgeld, gefälschte Ausweise und andere Dokumente im Angebot. Die Webseite „Executive Outcomes" (iczyaan7hzkyjown.onion) spezialisierte sich auf Handfeuerwaffen.

Das Tor Project selbst, das die Technologie zur Anonymität im Internet bereitstellt, ist vollkommen legal. Es finanziert sich durch Spenden, einer der größten Spender ist die US-Regierung. Aktuell plant sogar der weit verbreitete Webbrowser Mozilla Firefox eine Zusammenarbeit mit dem Tor Project.

Die weltweiten Razzien gegen die illegalen Nutzer der Tor-Technologie nahmen ihren Ausgangspunkt bei einem Treffen im Mai dieses Jahres in Den Haag, berichtet Forbes. Das Treffen wurde vom Europäischen Polizeiamt (Europol) abgehalten.

Die Operation wurde dann zwischen dem FBI, dem Europäischem Zentrum zur Bekämpfung der Cyberkriminalität, der US-Einwanderungsbehörde, der US-Heimatschutzbehörde und der EU-Justizbehörde koordiniert.

Bisher haben sich die Behörden nicht dazu geäußert, wie sie die Betreiber der versteckten Webseiten ausfindig machen konnten. Daher stellt das Tor Project verschiedene Vermutungen an, unter anderem den Einsatz von verdeckten Ermittlern und Sicherheitslücken bei den Betreibern der Webseiten.

Doch auch einen erfolgreichen Angriff auf das Tor-Netzwerk selbst wollen die Entwickler ausdrücklich nicht ausschließen. Sie machen auf die mögliche Gefahr aufmerksam, dass Sicherheitslücken bei den Seiten innerhalb des Tor-Netzwerks von Kriminellen ausgenutzt werden könnten und von den Geheimdiensten im Kampf gegen Regierungsgegner.

Einiges spricht jedoch dagegen, dass die Behörden tatsächlich einen Weg gefunden haben, das Tor-Netzwerk zu knacken. So ist fraglich, ob sie das Bekanntwerden dieser Fähigkeit riskieren würden, nur um ein paar Dutzend Online-Schwarzmärkte von Netz zu nehmen. Außerdem ist nur kurz nach dem Ende der Silk Road 2.0 bereits die Silk Road 3.0 ans Netz gegangen. Deren Macher halten das Tor-Netzwerk offenbar auch weiterhin für sicher genug.