9. Jul. 2015

von Martin

in Cyber Security

Kommentare (1)

Kontrolliert die Feinde des Internets – Der Hacking Team Leak zeigt wie wichtig Exportkontrolle von Software ist

von Martin Schmetz

In der Nacht vom letzten Sonntag wurde, größtenteils unbemerkt von der deutschen Presseöffentlichkeit, der italienische Softwareanbieter Hacking Team gehackt und über 400gb seiner internen Daten im Netz verteilt. Die Daten umfassen alles: E-Mails der Firmenleitung, der Programmierer und des Verkaufspersonals, interne Dokumente und Verträge und den kompletten Programmcode. Die Reaktion der Netzgemeinde war die umfassender Schadenfreude: Hacking Team stellt Spionage- und Überwachungssoftware her und verkauft diese weltweit an Regierungen – gerne auch solchen der autoritären Art. Diese Software wurde, wie die Leaks nun zeigen, tatsächlich zur Bekämpfung von Oppositionspolitikern und Menschenrechtsaktivisten eingesetzt, etwa in Äthiopien oder Sudan. Nicht umsonst führen Reporter ohne Grenzen Hacking Team in ihrer Liste der Feinde des Internets. Der Leak zeigt, dass die von diversen NGOs und Forschern, allen voran das Citizen Lab, geäußerten Vorwürfe stimmen: Hacking Team unterstützt autoritäre Regimes in Ihrem Kampf gegen Oppositionelle und ignoriert dabei auch Sanktionen, in dem es etwa an den Sudan oder Russland verkauft.

Das sollte nicht sein. Denn rechtlich ist die Ausfuhr dieser Software spätestens seit Ende 2014 in der EU problematisch. Zu dieser Zeit wurde die Überarbeitung des Wassenaar-Abkommens in der EU verabschiedet. Das Wassenaar-Abkommen regelt den Export von konventionellen Waffen und Gütern mit militärischen sowie zivilen Anwendungen. In der neuesten Version zählen dazu auch Überwachungs- und Spionagesoftware („Intrusions-Software“). Das Abkommen ist durchaus umstritten, denn die Formulierungen, die sich auf Überwachungs- und Spionagesoftware beziehen sind extrem weit und unpräzise gefasst. Bessere Vorschläge existieren durchaus, etwa in dem man sich nicht auf das Eindringen in Systeme und Ändern von „Standard-Ausführungspfades eines Programms oder Prozesses“ konzentriert, sondern auf das Ableiten von Daten aus den Rechnern anderer. Die Software von Hacking Team (Remote Control System) etwa wäre von dieser Definition immer noch betroffen, gängige Sicherheits- und Programmiertools aber nicht. So bleibt zu hoffen, dass das Abkommen in Europa eine sinnvolle Anwendung auf nationaler Ebene findet. Diese könnte inspiriert werden von der Debatte in den USA, wo die Änderungen noch nicht verabschiedet wurden und weiterhin Kritik geübt wird. Wenn Sicherheitsforscher auf Grund des Wassenaar-Abkommens Selbstzensur betreiben müssen, zeigt dies, dass die Politik nachbessern und solange die Verwaltung je nach Fall entscheiden muss.

Nichtsdestotrotz zeigt der Leak, dass die Idee des Abkommens richtig ist: Derartige Software eignet sich, wie die UNO zurecht bemerkte, kaum für sinnvolle zivile Aufgaben, wohl aber für geheimdienstliche und funkaufklärerische Aktivitäten. Deshalb gehören Hersteller dieser Software kontrolliert und in ihrem Exportgeschäft erheblich eingeschränkt. Diese Werkzeuge gefährden das Leben von Menschenrechtlern und Oppositionellen in autoritären Ländern. Vermutlich haben sie auch schon

SOCIAL MEDIA

SUCHE

Suche...

Suche

TWITTER FEED

Die offene Gesellschaft im Zangengriff – Was tun gegen islamistischen #Extremismus und #Islamfeindlichkeit? https://t.co/he1sNyzNRo
27. Januar 2016, 7:40 from Twitter Web Client

Diana Schubert über die Rolle von #Kommunen in der #Prävention von #Radikalisierung https://t.co/6F0QGmsxoQ #Salafismus
26. Januar 2016, 7:54 from Twitter Web Client

Fördern die Medien #Salafisten? Dynamiken, Verantwortung & Grenzen der Berichterstattung über salafistische Gruppen https://t.co/YM8phOlqdf
25. Januar 2016, 9:14 from Twitter Web Client

TAGS

BELIEBT KOMMENTARE NEU

"Die Flüchtlinge", "die Rassisten" und "Wir" – zu den Ambivalenzen

Leben gekostet. Die Kontrolle des Geschäfts mit dieser Software ist also nicht nur ein esoterisches Randthema für Turbonerds. Es muss im Kerninteresse einer Demokratie liegen, den Export solcher Werkzeuge zu verhindern, denn sie sind nicht mit demokratischen Werten kompatibel.

Das Wassenaar-Abkommen darf deshalb nicht nur leeres Gesetz bleiben. Es obliegt nun Politik und Verwaltung, das Abkommen sinnvoll umzusetzen. Das betrifft uns auch in Deutschland, denn wir haben eine ganze Reihe von Firmen, die derartige Software herstellen. Dass diese Abkommen durchaus Erfolg haben können, zeigt, dass mit Vupen einer der bekanntesten Verkäufer von sogenannten 0-Days (also ungepatchten Lücken in Software, die Angriffe erlauben) aus seinem Heimatland Frankreich in die USA umgezogen ist. Dort könnte es nun bald ebenfalls einen schweren Stand bekommen, denn auch dort droht Wassenaar.

Der Verkauf von derartigen Lücken (den im Übrigen auch Hacking Team betrieben hat) ist übrigens besonders perfide: Denn damit werden nicht nur gezielt einzelne Individuen angegriffen. Solange die Lücke in der Software existiert, sind alle, die diese Software einsetzen, potenziell gefährdet. Und es ist nicht unwahrscheinlich, dass derartige Lücken von mehr als einem Akteur genutzt werden. Im Gegensatz zu Forschern, die ebenfalls danach suchen und dies entweder kostenfrei oder gegen Geld an die Hersteller der Software weiterreichen, ist das Ziel hier nie größere allgemeine Sicherheit. Diese Firmen verdienen Geld, in dem Sie die demokratische Gesellschaft in der sie existieren, substanziell unsicherer machen. Eine solche Gesellschaft sollte sich berechtigt fragen, ob sie ein derartiges Geschäftsmodell tolerieren will.

Solche Firmen zum Auswandern oder zur Schließung zu zwingen heißt natürlich nicht, dass niemand mehr diese Dienste anbietet. Ein Umzug in ein autoritäres Land ist allemal eine Option. Oder es wird dort direkt eine neue Firma gegründet. Aber diese Länder sind im Allgemeinen deutlich weniger attraktiv für die Programmierer, die bei solchen Firmen arbeiten. Dieser Standortvorteil sollte als Druckmittel genutzt werden. Noch mehr wiegt aber, dass es schlicht ethisch nicht zu vertreten ist, derartigen Firmen freien Lauf zu lassen. Wenn andere Regierungen dies als mit Ihren Werten kompatibel erachten – bitteschön. Wir können aber nicht immer darauf bauen, dass Hacker unsere Gesellschaft vor solchen Auswüchsen schützen in dem sie solches Verhalten erst aufdecken. Ob auf europäischer oder nationaler Ebene: Eine demokratische Gesellschaft und ihre Regierung sollte in Zukunft anders entscheiden noch bevor ein weiterer Hack auf derartiges Fehlverhalten aufmerksam macht.

Tags: Äthiopien, demokratie, Deutschland, EU, Hacked Team, Hacking Team, russland, Rüstungskontrolle, spionage, Sudan, Überwachung, Wassenaar

« Terroristischer Weltkrieg am Badestrand – Der Anschlag von Sousse und die Symbolik von Terroranschlägen an Urlaubsorten
Wir und die Anderen? Die Beeinflussung der öffentlichen Meinung über Muslime und den Islam durch die westlichen Medien »

Trackbacks/Pingbacks

im aktuellen Flüchtlingsdiskurs

Ich bin Paris! Ich bin Muslim! Ich bin Nato? Die offene Gesellschaft und ihre Feinde nach dem 13. November.

Der Dschihad der Auslandskämpfer: Ausdruck einer Subkultur

Terroristen oder Bürgerkriegsflüchtlinge? Was wir gegen diese Verwechslung tun müssen

Fördern unsere Medien die Salafisten? Dynamiken, Verantwortung und Grenzen der Berichterstattung über salafistische Gruppen

KATEGORIEN

Außenpolitik (64)
Bürgerkriege (24)
Cyber Security (52)
Demokratisierung (14)
Drohnen (15)
Flüchtlinge (17)
Humanitäre Interventionen (15)
Innere Sicherheit (32)
Interviews (10)
Katastrophen (4)
Konferenz (29)
Militär (31)
Pandemien (2)
Podcast (7)
Popkultur (22)
Raketenabwehr (1)
Sanktionen (8)
Security Culture (27)
Sicherheits-Kommunikation (16)
Sicherheitskultur (237)
Sozialwissenschaft Online (71)
Stellenangebote (55)
Strategie (12)
Terrorismus (60)

1. **USA: Außeministerium klassifiziert „Cyber Produkte“ nicht als Waffen | netzpolitik.org** - 30. Okt. 2015

   [...] Genehmigung durch die nationalen Aufsichtsbehörden ausgeführt werden. Doch auch hier wird kritisiert, dass die Formulierungen, die sich auf Überwachungs- und Spionagesoftware beziehen, extrem weit [...]

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Wählen Sie alle Bilder mit Gras aus.

reCAPTCHA

Bestätigen

Soll die Herausforderung einfacher sein?

Datenschutz - Nutzungsbedingungen

Kommentar senden

Benachrichtige mich über nachfolgende Kommentare per E-Mail.

Theorie (5)

Umwelt (1)

Versicherheitlichung (23)

Visualisierung (6)

Whistleblowing (8)

WikiLeaks (17)

WMD (10)

Zivilgesellschaft (67)

BLOGROLL

Arbeitskreis soziale Bewegungen

Augen geradaus

Dan Drezner

Dart-Throwing Chimp

David Campbell

de.hypotheses.org

Demokratieforschung Göttingen

Duck Of Minerva

Future and Politics

Hylaean Flow

Internet und Politik

IR Blog

Just Security Blog

justsecurity.org

Killer Apps

Kings Of War

MPC Journal – Muslim Politics and Culture

netzpolitik.org

percepticon

shabka.org

Terrorismus in Deutschland

theorieblog.de

Verfassungsblog

Vom Bohren harter Bretter

whistleblower-net.de

ARCHIV

Wähle den Monat

Dieses Werk bzw. Inhalt steht unter einer Creative Commons Namensnennung-NichtKommerziell-KeineBearbeitung 3.0 Unported Lizenz.
Über diese Lizenz hinausgehende Erlaubnisse können Sie unter redaktion@sicherheitspolitik-blog.de erhalten