7. Nov. 2011

von Martin

in Cyber Security, WikiLeaks

Kommentare (3)

Im Netz ist immer irgendwo High Noon

von Martin Schmetz

Cybersecurity wird zunehmend als Herausforderung wahrgenommen und Leaks sind ein nicht unerheblicher Teil davon. Begegnet wird diesem Problem aber oftmals in Wildwest-Manier: Jeder ist sich selbst der nächste, allgemein verbindliche Regelungen werden nicht angestrebt. Verschiedene staatliche und nicht-staatliche Akteure nutzen dabei die ihnen zur Verfügung stehenden Mittel konsequent aus und überschreiten dabei mal mehr, mal weniger rechtliche Grenzen.

Die USA sind und waren von den WikiLeaks-Veröffentlichungen am stärksten betroffen. Dementsprechend harsch fielen die Reaktionen der Obama-Administration aus: Sprecher Julian Assange wurde als Terrorist und Verräter gebrandmarkt, Geldflüsse an WikiLeaks über westliche Finanzinstitutionen wurden teilweise gestoppt, das Netzwerk der Unterstützer wurde ausgekundschaftet. Aber mit welchen Mitteln genau widmete man sich dieser Herausforderung?

In der International Strategy for Cyberspace gibt sich die US-amerikanische Regierung (noch) versöhnlich. Der Cyberspace wird dort zwar bereits als Sicherheitsproblem definiert, aber man betont den Bedarf an internationaler Zusammenarbeit und verweist auf zivile Stakeholder.

Von Wikileaks öffentlich gemachte Dokumente und Botschaftsdepeschen legen allerdings nahe, dass die USA tatsächlich wenig Interesse an einer internationalen Verregelung von Offensivpotenzial im Netz hat:

> „USDel [United States Delegates, also Delegierte der USA in den Verhandlungen] should continue to oppose Russian arguments for arms control-like constraints on information technology and offensive capabilities. USDel should continue to stress that the most value can come from exchanges on defensive measures and/or strategies, mitigation, and remediation.“ [Quelle]

Das Vorgehen gegen Bedrohungen im Netz soll also nicht Gegenstand von Einschränkungen sein, man möchte sich eine möglichst große Bandbreite an Offensivoptionen offen halten. Und unter diesen Vorzeichen kann man auch das Vorgehen gegen WikiLeaks durch verschiedene Parteien sehen:

SOCIAL MEDIA

SUCHE

Suche...

Suche

TWITTER FEED

Neue #Jobs für Politikwissenschaftler_innen! http://t.co/f3vSzfJpMG
ungefähr 3 Stunden her von &s

In den nächsten Wochen bei uns: Eine Beitragsreihe zu #Cyberpeace. Großartige Autoren, spannende Posts! http://t.co/z54MUpBFNc @fiff_de
3. Dezember 2014, 12:28 von &s

Ein kleiner Konferenzbericht zur #doeff14 von @seditioni und ein großes Lob an die Organisator_innen! http://t.co/tUtsCX4Vdg
1. Dezember 2014, 10:08 von &s

TAGS

So identifizierte bereits 2008 ein Report der US-Army WikiLeaks als Problem. Hier werden auch mögliche Reaktionen aufgezählt, vom direkten Vorgehen gegen die Leaker bis zum physischen Zugriff auf die WikiLeaks-Internet-Server, etwa durch die Kooperation mit ausländischen Geheimdiensten oder lokal zuständigen Strafverfolgungsbehörden.

Das Vorgehen gegen die Leaker selbst – sowohl die interne Ermittlung als auch das Schaffen von Abschreckungsstrukturen in der US-Verwaltung um Leaking selbst zu verhindern – scheint in den USA hingegen weiter zu gedeihen. Die Logik scheint zu sein: Säht man genügend Zweifel über die Authentizität der Dokumente und erhöht die Angst beim Leaker, erwischt zu werden, minimiert man die Gefahr weiterer Leaks.

Auch private Akteure gehen gegen WikiLeaks vor, im prominenten Fall der Bank of America auch deutlich aggressiv – oder versuchen dies jedenfalls. Im Falle der Bank of America wurden die Dokumente geleakt bevor die Pläne umgesetzt werden konnten. Die Bank beauftragte drei Unternehmen (HBGary, Berico und Palantir), gemeinsam Strategien zur Unterwanderung oder gar Zerstörung der WikiLeaks-Plattform zu entwickeln. Diese Strategien reichten dabei von der Verbreitung von Desinformationen, der publizistischen Attacke prominenter Unterstützer in den Medien über das Überwachen von Mitarbeitern in sozialen Netzwerken, bis hin zu Cyberattacken auf die Infrastruktur und individuelle Personen. Dies deckt sich zumindest teilweise mit dem staatlichen Vorgehen: Überwachung der Mitarbeiter und das Anfertigen detaillierter Profile wird in beiden Fällen angestrebt. Während die staatlichen Pläne aber vor allem auf physische Zugriffe durch Strafverfolgungsbehörden abzielen und Cyberangriffe wenn überhaupt nur implizit erwähnen, werden Cyberangriffe bei den nichtstaatlichen Akteuren ganz klar als mögliches Werkzeug erwähnt. Rechtliche Bedenken diesbezüglich tauchen nur am Rand auf: In einigen der geleakten Mails wird die Rechtsabteilung konsultiert, allerdings scheint dies keine weiteren Konsequenzen nach sich zu ziehen.

Leaking wird zunehmend als ein erstzunehmendes Problem wahrgenommen, gegen das staatliche und auch nichtstaatliche Akteure vorgehen wollen. Eingeschränkt werden wollen sie in ihrem Vorgehen aber nicht, jedenfalls nicht mehr, als sie es momentan sowieso schon sind. Ein zivilgesellschaftlicher Akteur wie WikiLeaks wird so zum Feind staatlicher und nicht-staatlicher Stellen. Zur Verteidigung der Informationshoheit scheint beiden Akteursgruppen die Selbsthilfe das Mittel der Wahl, um die Kontrolle über die eigenen Informationen sicherzustellen, auch gegenüber den eigenen Mitarbeitern. Eine Zusammenarbeit mit Akteuren außerhalb der Sicherheitsorgane oder –firmen, um den Phänomen Leaking oder Cybersecurity zu begegnen, wird dabei offensichtlich nicht angestrebt.

Nicht nur hat das Leaking von vertraulichen Dokumenten und Informationen und wie die betroffenen Akteure darauf reagieren weitreichende Implikationen für jeden demokratischen Rechtsstaat, sondern fördert eine Selbstermächtigung der Betroffenen. Sollte sich dieses Verhalten

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science! Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier Raum sein

Deutschlands Irak-Politik – Verantwortung nach außen, Intransparenz nach innen.

Wir haben Geburtstag!

„Mit Sicherheit nicht!“ Sexuelle Gewalt als politisches Mittel

KATEGORIEN

Außenpolitik (59)

Bürgerkriege (16)

Cyber Security (40)

Demokratisierung (9)

Drohnen (15)

Humanitäre Interventionen (15)

Innere Sicherheit (24)

Interviews (10)

Katastrophen (4)

Konferenz (20)

Militär (27)

Pandemien (2)

Podcast (7)

Popkultur (20)

Sanktionen (8)

Security Culture (13)

als akzeptabel durchsetzen, so können wir uns tatsächlich auf den Wilden Westen im Netz freuen. Beim High Noon Duell gewinnt bekanntlich derjenige mit der größeren Pistole oder den schnelleren Reaktion . Und irgendwo ist im Netz immer High Noon

Tags: Cablegate, Team Themis, Wikileaks

« Kommunikativer Staat im Krisenfall
Tipping Point!? Die Palestine Papers im fragilen Kontext des Nahost-Konfliktes »

3 Kommentare zu “Im Netz ist immer irgendwo High Noon”

andrea | 14. Nov. 2011 um 8:49 | **#1**

Ich denke es sollte klarer unterschieden werden zwischen Whistleblower Leaks und gehackten Leaks – letzteres ist digitaler Diebstahl und wie du es schön dargestellt hast, Waffe gegen unliebsame Gegner. Whistleblower hingegen wollen eher auf Missstände hinweisen, in der Hoffnung, sie dadurch beseitigen zu können.
Aber ich frage mich.. hat WikiLeaks jemals einen Leak gehackt?

ANTWORTEN

literally | 16. Nov. 2011 um 0:00 | **#2**

WikiLeaks (bzw. damit assoziierte Personen) selbst hat meines Wissens nie selbst Leaks gehackt. Ich bin mir nicht mal sicher, ob WikiLeaks jemals etwas veröffentlicht hat, was durch einen Hack an die Öffentlichkeit kam. Spontan fiele mir jedenfalls nichts ein, allerdings ist der Katalog von WikiLeaks auch sehr umfangreich.
Was die Unterscheidung zwischen Hacks und Whistleblowing angeht: Ich stimme zu, dass eine derartige Unterscheidung Sinn macht. Betrachtet man aber die anschließende Diskussion um die Daten (und zwar nicht normativ), bin ich mir nicht so sicher – wenn in der Diskussion die Herkunft selbst keine entscheidende Rolle spielt, wäre die Herkunft in der Betrachtung auch eher unwichtig.

ANTWORTEN

andrea | 21. Nov. 2011 um 3:57 | **#3**

Dennoch verwundert es doch sehr: In der Podiumsdiskussion wurde eindeutig Leaking als “schlecht” und Whistleblowing als “gut” dargestellt. Bei WikiLeaks wurde kaum nach der Legitimität einzelner Leaks gefragt: entweder die Plattform an sich war eine Gefahr, oder eine neue Institution für transparentere Politik. Warum gab es diese grundlegende Diskussion eigentlich erst bei WikiLeaks und nicht bspw schon bei Cryptome?

Sicherheits-Kommunikation (14)
Sicherheitskultur (204)
Sozialwissenschaft Online (57)
Stellenangebote (42)
Strategie (10)
Terrorismus (14)
Theorie (2)
Umwelt (1)
Versicherheitlichung (21)
Visualisierung (5)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (48)

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
netzpolitik.org

ANTWORTEN

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Geben Sie den Text ein.

reCAPTCHA

Bestätigen

Datenschutz - Nutzungsbedingungen

Kommentar senden

☑ Benachrichtige mich über nachfolgende Kommentare per E-Mail.

shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat