SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

Juli 2014

SWITCH

I. Gegenwind für Schweizer Überwachungsgesetz

Als sich am 19. März dieses Jahres der Ständerat mit der Revision des Gesetzes zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) befasste, war man sich weitgehend einig: Die gesetzlichen Grundlagen für die Strafverfolgung müssen der Entwicklung der modernen Informationstechnologie angepasst werden. Die vorgesehene Ausdehnung der Vorratsdatenspeicherung von 6 auf 12 Monate und der Einsatz von sogenannten Staatstrojanern zur Überwachung von Verdächtigen sei daher zu befürworten. Der Ständerat stimmte dem BÜPF mit 30 zu 2 Stimmen bei 4 Enthaltungen zu. Im nächsten Schritt muss sich nun der Nationalrat im Herbst mit dem Thema befassen.

Unterdessen formiert sich Widerstand aus verschiedenen Richtungen. Die Kritik bezieht sich zum einen auf die Verhältnismässigkeit und Wirksamkeit der vorgesehenen Massnahmen. «Ich kenne keine Fälle, bei denen wegen der heute geltenden Frist ein schweres Delikt nicht verhindert oder aufgeklärt werden konnte.», sagt beispielsweise Hanspeter Thür, Datenschützer des Bundes, zur Ausweitung der Vorratsdatenspeicherung im Interview mit der NZZ.

Ausserdem sind viele Fragen offenbar nicht hinreichend geklärt: Bei welchen Delikten soll der Einsatz der Schnüffelsoftware erlaubt sein? Reichen beispielsweise schwerer Diebstahl oder Sachbeschädigung aus? Wie wird garantiert, dass auf einem durch «GovWare» überwachten Computer keine Daten hinzugefügt oder verändert werden? Wie soll die Mitwirkungspflicht bei kleineren (WLAN-)Anbietern in der Praxis aussehen?

Ein weiteres Lager der Kritiker lehnt eine Ausweitung staatlicher Überwachung kategorisch ab und verweist dabei auf das Grundrecht auf Privatsphäre als notwendige Eigenschaft eines demokratischen Staates. Die Historikerin Nathalie Baumann fragt in diesem Zusammenhang: «Was für ein Selbstverständnis hat ein Staat, der rund ein Viertel seiner Bürgerinnen und Bürger überwachen lässt?» Sie bezieht sich dabei auf die Fichenaffäre der neueren Schweizer Geschichte und vermisst eine breite gesellschaftliche Diskussion.

Diese könnte nun entstehen. Denn ein Ende Mai gegründetes überparteiliches Referendumskomitee will sich gegen die BÜPF-Revision einsetzen, sollte das Gesetz durch den Nationalrat unverändert verabschiedet werden. Das Komitee ist dabei breit abgestützt, alle Jungparteien mit Ausnahme der Jungen CVP sind vertreten, ebenso wie der ICT-Branchenverband Swico.

Der Bund bereitet derweil Investitionen in Höhe von 91 Millionen Schweizer Franken bis 2021 für die Modernisierung und den Ausbau der Überwachung des Post- und Fernmeldeverkehrs vor. In einer Medienmitteilungen vom 1. Juli 2014 lässt das Eidgenössische Justiz- und Polizeidepartement (EJPD) zudem sinngemäss verlauten: Wenn es um die Aufklärung von schweren Straftaten oder auch die Suche nach vermissten Menschen in Not geht, sei ein Eingriff in die Grundrechte durch Auswertung von Telefon- oder Mailverkehr gerechtfertigt. Zum einen gäbe es ein grosses öffentliches Interesse. Zum anderen hätte der Gesetzgeber die Verwendung gespeicherter Daten durch hohe gesetzliche Hürden eingeschränkt.

Das ist auch der Kern der Begründung, mit der das EJPD die Gesuche von sechs Mitgliedern der Digitalen Gesellschaft Schweiz gegen die Vorratsdatenspeicherung ablehnt. Letztere begrüsst zwar, dass man erkannt habe, dass die Vorratsdatenspeicherung einen schweren Eingriff in die Grundrechte darstellt, möchte ansonsten aber den ablehnenden Entscheid anfechten. Nötigenfalls soll der Weg bis zum Europäischen Gerichtshof für Menschenrechte (EGMR) führen.

Der Europäische Gerichtshof (EuGH) hatte übrigens am 8. April 2014 die EU-Richtlinie über die Vorratsspeicherung von Daten für ungültig erklärt. Denn diese sei «ein besonders schwerwiegender Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten».

Zum Weiterlesen:

http://www.srf.ch/news/schweiz/session/staenderat-votiert-fuer-schnueffel-software

http://www.nzz.ch/aktuell/schweiz/privatsphaere-wird-zu-einem-privileg-1.18256915

http://www.netzwoche.ch/News/2014/03/25/Georg-bitte-lies-diese-Karte-nicht.aspx

http://www.inside-it.ch/articles/36499

http://www.inside-it.ch/articles/36172

http://www.nzz.ch/aktuell/schweiz/angst-vor-dem-schnueffelstaat-1.18313578

http://www.netzwoche.ch/de-CH/News/2014/06/02/Bund-will-weitere-91-Millionen-fuer-Ueberwachung-aufwenden.aspx

http://www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2014/2014-07-01.html

https://www.digitale-gesellschaft.ch/2014/02/21/digitale-gesellschaft-erhebt-beschwerde-gegen-vorratsdatenspeicherung/

http://www.steigerlegal.ch/2014/07/01/urteil-pro-vorratsdatenspeicherung-in-der-schweiz/

http://www.zeit.de/digital/datenschutz/2014-04/vorratsdatenspeicherung-europaeischer-gerichtshof-eugh

II. Versuchskaninchen Facebook-User

Dass man als Nutzer des Sozialen Netzwerks Facebook mit seinen Daten bezahlt, ist klar. Auch dass Facebook bestimmt, welche Nachrichten aus dem Kreise der «Freunde» im persönlichen Newsfeed – bei Facebook «Timeline» genannt – angezeigt werden und welche nicht, haben die Nutzer geschluckt. Denn Facebook ist immer darum besorgt, dass wir nur das sehen, was uns auch wirklich interessiert: Improved User experience. Das ist doch eine gute Sache!

Anfang Juni wurde nun eine Studie im wissenschaftlichen Magazin PNAS veröffentlicht, die zeigt, dass Facebook im Januar 2012 Hunderttausende Facebook-Nutzer einem unfreiwilligen Experiment unterzogen hatte: Im Rahmen einer wissenschaftlichen Untersuchung manipulierte man eine Woche lang die Timeline von 310 000 Nutzern. Bei der einen Hälfte reduzierte Facebook die Zahl der Postings mit positiven Emotionsäusserungen, bei der anderen Hälfte entsprechend die Negativen. Weitere 310 000 Probanden diente als Kontrollgruppe ohne veränderte Timeline. Untersucht wurde dann, wie sich die Manipulation auf die Stimmung bzw. das eigene

Postingverhalten der Nutzer auswirkte. Ergebnis: Facebook kann die Stimmung der Nutzer in die eine wie die andere Richtung manipulieren, wenn auch nur geringfügig.

Nach der Veröffentlichung der Studie ging eine Welle der Entrüstung über Facebook her. Der Hauptkritikpunkt liegt darin, dass Facebook seine User als Versuchspersonen missbrauchte, ohne vorher deren Einverständnis einzuholen. Nun gibt es zwar schlaue Leute die sagen, «Datenverwendung für Forschung» steht doch in der Data Use Policy drin. Aber noch schlauere haben herausgefunden, dass dieser Passus erst 4 Monate nach Durchführung der Studie dort aufgenommen wurde. Ausserdem schliesst eine «Datenverwendung für Forschung» ja nicht mit ein, dass Nutzer ungefragt als Versuchskaninchen herhalten müssen. Adam Kramer, der Facebook-Mann der die Studie leitete, äusserte sich am 29. Juni 2014 auf Facebook so: «Der Grund für diese Forschungsstudie ist, dass wir uns um den emotionalen Einfluss von Facebook auf unsere User sorgen. [...] Das Ziel all unserer Forschung bei Facebook ist, einen besseren Service zu bieten.» Improved User experience eben.

Laut einem Bericht von «The Register» nimmt sich nun die britische Datenschutzbehörde dem Thema an und prüft eine Klage gegen die Social-Media-Plattform. Zudem hat die US-amerikanische Gruppe EPIC (Electronic Privacy Information Center) eine Beschwerde bei der Aufsichtsbehörde FTC eingereicht. Wie sich dies auf die Stimmung von Mark Zuckerberg auswirkt, ist allerdings nicht bekannt.

Nachzulesen unter:

http://www.businessinsider.com/how-the-facebook-news-feed-works-2014-2

http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/der-facebook-boersengang/facebook-manipuliert-nutzer-gefuehle-fuer-eine-studie-13016744.html

http://www.pnas.org/content/111/24/8788.full

http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/

https://www.facebook.com/akramer/posts/10152987150867796

http://www.theregister.co.uk/2014/07/01/uk_and_irish_data_watchdogs_wade_in_on_facebook_messin_with_your_head_scandal/

III. Cyber-Angriff auf unsere Köpfe

Beim Thema Cyberwar denken wir meist an Dinge wie hochspezialisierte Computerviren, manipulierte Industrieanlagen und Denial-of-Service-Attacken auf kritische Systeme. Weniger bekannt sind Armeen von Auftragstrollen, die in Social-Media-Communities und Kommentar-Bereichen von Nachrichtenportalen gezielt Stimmung machen.

Wie die Süddeutsche Zeitung nun berichtete, gibt es beispielsweise in Sankt Petersburg eine Firma mit rund 600 Mitarbeitern, deren Hauptaufgabe es ist, Meinungen im Internet im Sinne der russischen Regierung zu manipulieren. Kosten: umgerechnet etwa eine Million Dollar – pro Monat. Diese Manipulationen beschränken sich dabei nicht auf den russischen Sprachraum, sondern vor allem auch den Englischsprachigen.

Eine Gruppe von Hackern soll nach Angaben der Süddeutsche Zeitung den E-Mail-Account eines leitenden Mitarbeiters der Petersburger Agentur geknackt und Ende Mai über 800 Mails veröffentlicht haben. Aus diesen ergibt sich ein Bild, wie das «organisierte Trollen» vor sich geht: Zunächst werden englischsprachige Internetmedien systematisch nach Kategorien wie Altersverteilung der Nutzer, Tageszeiten höchster Aktivität und politischer Einstellung des Publikums analysiert.

Dann erhalten die Bezahl-Trolle exakte Anweisungen zur Kommentierung in den jeweiligen Foren. Themen, Schlüsselwörter und Kriterien werden klar vorgegeben. Bezahlt wird nach Leistung, Tagessoll: 50 Kommentare auf Nachrichtenportalen, 50 Tweets und nebenbei die Bewirtschaftung von 6 Facebook-Seiten.

Aber auch andere Geheimdienste nutzen die sozialen Netzwerke für ihre Propaganda. So haben die Amerikaner beispielsweise bis Herbst 2012 eine Twitter-artige Plattform für Kuba betrieben mit dem Ziel, Unruhen in Kuba zu provozieren. Und im britischen Geheimdienst soll seit letztem Jahr eine mindestens 150 Mann starke Spezialabteilung namens «Joint Threat Research Intelligence Group» für Meinungsmanipulation und gezielte Diskreditierung in den Sozialen Medien zuständig sein.

In seinem Vortrag «There is no democracy without media literacy» (Ohne Medienkompetenz keine Demokratie) hat Jaroslaw Lipszyc auf der diesjährigen Medienkonferenz «re:publica» in Berlin darauf aufmerksam gemacht, dass das einzige Gegenmittel in Zeiten des Information Wars eine umfassende Medienkompetenz ist.

Wie wichtig der bewusste und kritische Umgang mit Medien tatsächlich ist, zeigte jüngst noch ein weiteres Beispiel: Mehrere vorsätzliche Falschmeldungen auf Facebook und per E-Mail führten Ende Juni zu grosser Panik bei Sparern in Bulgarien. Inhalt der Postings waren Aussagen, dass Einlagen von Kunden einer bulgarischen Bank nicht mehr sicher seien. Daraufhin begannen tausende Kunden ihre Konten leerzuräumen. Innerhalb eines Tages zahlte die Bank rund 400 Millionen Euro aus und war nach kurzer Zeit gezwungen, alle Schalter zu schliessen. Bulgariens Zentralbank wertete dies als einen systematischen Versuch, das Land durch Angriffe auf das Bankensystem zu destabilisieren.

Mehr dazu:

http://www.sueddeutsche.de/politik/propaganda-aus-russland-putins-trolle-1.1997470

http://www.nzz.ch/international/putins-internetpiraten-1.18324628

http://www.faz.net/aktuell/snowden-dokumente-wie-man-die-oeffentlichkeit-infiziert-12881233.html

http://re-publica.de/session/there-no-democracy-without-media-literacy

http://futurezone.at/digital-life/falschmeldung-auf-facebook-verursacht-bankenansturm/72.895.325

http://in.reuters.com/article/2014/06/27/bulgaria-banks-idINL6NOP81SG20140627

http://news.yahoo.com/white-house-defends-cuban-twitter-stir-unrest-222510641.html

https://netzpolitik.org/2014/neues-aus-der-jtrig-abteilung-von-gchq/

IV. Was passierte mit TrueCrypt?

Die Nachricht schlug ein, wie eine Bombe: Am 28. Mai 2014 wurde auf der offiziellen Webseite von TrueCrypt – einer weit verbreiteten, quelloffenen und anerkannt sicheren Verschlüsselungssoftware – plötzlich bekanntgegeben, dass die Entwicklung eingestellt würde und die Software potenziell unsicher sei. Statt der ursprünglichen Inhalte der Homepage wurde nur noch eine Empfehlung veröffentlicht, wie man seine verschlüsselten Daten zu Microsofts Krypto-Lösung BitLocker migrieren könne.

Das Ganze sah zunächst ganz nach einem fiesen Defacement-Hack aus. Allerdings wurde auf Sourceforge auch nur noch eine funktionsbeschränkte Version der Software angeboten – und diese war mit dem gültigen Schlüssel der Entwickler signiert. Da ausserdem niemand die TrueCrypt-Homepage wieder in Ordnung brachte, glaubte man bald nicht mehr an einen Hack. Allerdings meldete sich auch niemand aus dem weitgehend im Anonymen agierenden Entwicklerteam, um die Sache aufzuklären.

Natürlich mehrten sich sogleich viele Theorien, die das ganze Geschehen mit den Geheimdiensten in Verbindung brachte. Kreative Zeitgenossen fanden ausserdem heraus, dass die Warnung, die die Entwickler in roter Schrift neu auf ihre Homepage

aufgeschaltet hatten, nämlich «Using TrueCrypt is not secure as it may contain unfixed security issues», die Anfangsbuchstaben «utinsaimcusi» ergibt. Und diese führen als «uti nsa im cu si» bei Google Translate eingegeben zu einer Übersetzung aus dem lateinischen, die da heisst: «If I wish to use the NSA».
Die Sicherheit von TrueCrypt war ein Jahr zuvor im Rahmen der Snowden-Enthüllungen ins Interesse von Forschern gerückt. Man hatte Spenden gesammelt und das Open Crypto Audit Project (OCAP) gegründet, um die Software genau zu untersuchen. Der erste Teil des Audits ergab im März, dass TrueCrypt keine Backdoor enthält, aber verschiedene Schwachstellen. Das OCAP-Team hat zwischenzeitlich die letzte vollständige Version (7.1a) im Netz bereitgestellt und bemüht sich um eine Nachfolgeregelung für die Software.

TrueCrypt hat nach wie vor unter Security-Leuten einen guten Ruf. Das ist nicht bei allen Verschlüsselungsprodukten der Fall. «Die meisten kommerziellen Verschlüsselungsprodukte sind Müll» twitterte etwa kürzlich Matthew Green, Professor für Kryptografie und einer der angesehensten, unabhängigen Experten auf dem Gebiet.

Zum Weiterlesen:

http://truecrypt.sourceforge.net/

http://grahamcluley.com/2014/06/truecrypt-hidden-message/

http://opencryptoaudit.org/

http://www.heise.de/security/meldung/TrueCrypt-geprueft-Keine-Backdoor-laxe-Programmierstandards-2170398.html

http://www.nzz.ch/aktuell/digital/truecrypt-71a-download-open-crypto-audit-project-ocap-1.18319652

https://github.com/AuditProject/truecrypt-verified-mirror

https://twitter.com/matthew_d_green/status/478956352237076480

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Wenn eine entsprechende Anordnung einer US-Behörde vorliegt, müssen amerikanische Firmen gemäss einem neuen Gerichtsurteil auch Daten herausgeben, wenn sich diese auf Servern im Ausland befinden:

http://www.nzz.ch/wirtschaft/wirtschafts-und-finanzportal/europaeische-datenwolken-als-beliebte-loesung-1.18308010

In einem zweiteiligen Blogpost befassen sich Bryce Boland und Greg Day von Fireeye damit, wie man Business Case und ROI-Betrachtungen von IT-Security-Massnahmen in den Griff bekommt:

http://www.fireeye.com/blog/corporate/2014/07/economics-of-security-part-i-translating-information-security-risks-to-business-risk.html

Symantec berichtet in einem Blogpost und einem Whitepaper über die Hackergruppe «Dragonfly» alias «Energetic Bear», die derzeit die westliche Energiewirtschaft ins Visir nimmt:

http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf

Dieser SWITCHcert Security Report wurde von Frank Herberg verfasst.

Der Security Report spiegelt nicht die Meinung von SWITCH wider, sondern ist eine Zusammenstellung verschiedener Berichterstattungen in den Medien. SWITCH übernimmt keinerlei Gewähr für die im Security Report dargelegten Inhalte, Meinungen oder deren Richtigkeit.

Information in eigener Sache: Aus personellen Gründen geht der SWITCHcert Security Report im August in die Sommerpause. Der nächste Report erscheint am 5. September. Wie immer halten wir Sie auf securityblog.switch.ch über die wichtigsten Security-Themen auf dem Laufenden.