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

Oktober 2016

SWITCH

I. Hat sich das Schweizer Stimmvolk selbst unter Generalverdacht gestellt? Zur Annahme des neuen Nachrichtendienstgesetzes NDG

In der Referendums-Abstimmung vom 25. September 2016 hat das Schweizer Stimmvolk das neue Nachrichtendienstgesetz (NDG) mit 65.5% Ja-Stimmen überraschend deutlich angenommen. Darin wird der Nachrichtendienst des Bundes NDB ermächtigt, künftig Telefongespräche abzuhören, Privaträume zu verwanzen, in Computer einzudringen, diese zu manipulieren (Art. 25) und in Kabelverbindungen Daten abgreifen zu können, wenn die innere und äussere Sicherheit oder wesentliche Landesinteressen bedroht sind. Zudem kann er die beschafften Daten im Rahmen automatisierter Informationsabtauschprozesse ins Ausland weitergeben. Als Bedrohung gelten u.a. Terrorismus, die Verbreitung von Massenvernichtungswaffen oder Spionage gegen die Schweiz. Die Ja-Kampagne der Befürworter argumentierte zum einen damit, dass das neue NDG der Sicherheit diene und dem NDB enge Grenzen für die Überwachung gezogen würden. Denn je nach Art der beabsichtigten Massnahme zur Datenbeschaffung muss sich der Nachrichtendienst diese durch einen Einzelrichter des Bundesverwaltungsgerichts und den Verteidigungsminister, respektive den Sicherheits-Ausschuss des

Bundesrates, genehmigen lassen. Als Aufsichtsinstanz soll die Geschäftsprüfungsdelegation (GPdel) des Parlaments amten. Bei der Funkaufklärung sieht das Gesetz eine zusätzliche Kontrollinstanz vor.

Dennoch geben auch Befürworter des Gesetzes zu, dass mit seiner Annahme ein Verlust von Freiheit verbunden ist. So warb z.B. die Volketswiler Nationalrätin und BDP-Fraktionspräsidentin im Bundeshaus Rosmarie Quadranti für die Annahme des Gesetzes mit den Worten: «Niemand will aus der Schweiz einen Überwachungsstaat machen, aber niemand möchte zum Schluss den Kopf hinhalten, sollte etwas passieren. Dieser Verlust von Freiheit ist der derzeit wohl meistdiskutierte … Wir haben mit dem NDG ein Gesetz, das die Freiheit des Normalbürgers praktisch nicht tangiert. Die Kontrollmechanismen sind so gut ausgebaut und streng geregelt, dass eine grossflächige Überwachung und Fichierung praktisch ausgeschlossen werden kann … es ist eine kontrollierte Abgabe von Freiheit.»

Demgegenüber führen die Gegner zwei Befürchtungen ins Feld: So liefere das NDG die Grundlage für den Ausbau des Nachrichtendienstes zu einer gigantischen Überwachungsmaschine nach Vorbild der US-amerikanischen NSA. Tatsächlich ist das neue Gesetz u.a. daraus entstanden, dass bisher in zwei getrennten Erlassen enthaltene Vorschriften für die Informationsbeschaffung im In- und im Ausland zusammengeführt wurden. Das widerspiegelt die Entstehung des Nachrichtendienstes des Bundes, der ja 2010 aus dem Zusammenschluss des Strategischen Nachrichtendienst (SND – fokussiert auf Informationsbeschaffung im Ausland) und des Dienstes für Analyse und Prävention (DAP – Informationsbeschaffung im Inland) entstanden war.

Das neue Gesetz führt aber nicht nur bestehende Regelungen zusammen, sondern räumt dem NDB zahlreiche neue Befugnisse ein (Zusammenstellung in der unten genannten Quelle www.digitale-gesellschaft.ch). Gegner monieren, dass diese zu schwerwiegenden Eingriffen in das Recht auf Privatspähre, das Recht auf informationelle Selbstbestimmung und zum Aushebeln von verbrieften Berufsgeheimnissen, namentlich von Ärzten und Anwälten führen und damit gegen die allgemeinen Grund- und Menschenrechte verstossen. Sie verweisen zudem darauf, dass noch kein Geheimdienst einen glaubwürdigen Nachweis dafür erbracht hätte, dass erweiterte Überwachungsbefugnisse das Sicherheitsrisiko

verkleinern würden, dafür aber die Freiheit unbescholtener Bürger deutlich einschränkten.

Nach persönlicher Ansicht der Autoren dieses Security-Reports hat die Abstimmung um das neue NDG aber auch Fragen an die direkte Demokratie – die hier keineswegs in Zweifel gestellt werden soll! – aufgeworfen: Können die Stimmbürger in hochkomplexen Sachfragen mit einer diffizilen Güterabwägung – hier Freiheit vs. Sicherheit – überhaupt eine klare Meinungsbildung finden? Wodurch könnte diese auf objektiver und glaubwürdiger Basis unterstützt werden – durch ein Expertengremium oder durch «Schwarm-Intelligenz?» Sicher ist hier nicht der Ort, diese Fragen abschliessend zu beantworten. Dennoch sollte einem eine Textzeile aus Georg Danzers Stück «Die Freiheit» zu denken geben: «Das ist ja grade», sagte er, «der Gag: Man sperrt sie (die Freiheit, Anm. d. Autoren) ein und augenblicklich ist sie weg!»

Nachzulesen unter:

http://www.lrens-oui.ch/?lang=de
http://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/sicherheit/schweizer-nachrichtendienstgesetz
http://www.nzz.ch/schweiz/aktuelle-themen/abstimmung-ueber-das-nachrichtendienstgesetz-die-sicherheit-nicht-dem-zufall-ueberlassen-ld.111342
https://netzpolitik.org/2016/geheimdienst-in-der-schweiz-stellt-bevoelkerung-unter-generalverdacht
https://www.digitale-gesellschaft.ch/2016/07/30/zusammenstellung-der-umfangreichen-befugnisse-fuer-den-geheimdienst-im-neuen-nachrichtendienstgesetz
https://steigerlegal.ch/2016/01/11/nachrichtendienstgesetz-sicherheitsesoterik

II. Geld oder Gerät – Mobile Banking Trojaner Gugi trickst Android-Benutzer aus

So putzig der Name Gugi auch klingen mag, so fies ist der Smartphone-Trojaner, der die Benutzer von infizierten Mobilgeräten vor die Wahl stellt, entweder die Sperrung des Geräts hinzunehmen oder ihm Overlay-Rechte einzuräumen, mit deren Hilfe er dann die E-banking-Konten des Device-Besitzers abräumt. Zum Verständnis: Um Overlays zu ermöglichen, bei denen bösartige Apps gutartigen, legitimen Apps eigene UI (User Interface) Elemente wie z.B. Input-Kontrollen, Navigations- oder Steuerelemente aufpfropfen, um damit z.B. Zugangs- oder Bankingdaten der Opfer

abzugreifen, zwingt das Mobildevice-Betriebssystem Android seit der Version 6 (Marshmallow) Apps dazu, das Overlay genehmigen zu lassen.

Im Sommer haben die Sicherheitsexperten bei Kapersky eine neue Version des Mobile Banking Trojaners Gugi entdeckt, der diese Overlay-Sperre aushebelt, indem er die Erlaubnis dafür bei den Benutzern befallener Mobilgeräte erzwingt. Weigern sich diese, sperrt Gugi das infizierte Device, und zwar komplett. Lässt sich ein Benutzer auf Gugis Forderungen ein und erteilt die Erlaubnis für Overlay-Rechte, kopiert der bösartige Trojaner bei Kreditkartenzahlungen via Apps oder bei der Nutzung von E-Banking-Apps im Hintergrund die Kreditkarten- und Bankdaten.

Gugi grassierte zunächst in Russland, verbreitet sich aber inzwischen über Social-Engineering und die Nutzung durch Cyberkriminelle rasant weiter: Gemäss Kapersky stieg die Anzahl der Opfer zwischen April und Anfang August 2016 um das Zehnfache.

Um diesem Wachstum Einhalt zu gebieten und die eigenen Geräte zu schützen, sei an dieser Stelle an die «Hilfreichen Sieben» erinnert:

1. Keine automatischen Rechte und Genehmigungen an jegliche Apps vergeben.
2. Wie immer und auf allen Geräten: Nicht auf Links in unbekannten und unerwarteten SMS und MMS Nachrichten klicken.
3. Beim Besuch von Webseiten Vorsicht walten lassen (verdächtige Objekte erkennt man meistens).
4. Apps ausschliesslich von bekannten App Stores herunterladen.
5. Top-Antivirus-Programm für Android installieren.
6. Verbinden auf unbekannte Wi-Fi Hotspots vermeiden.
7. VPN auf Smartphone installieren und möglichst auch benutzen.

Nachzulesen unter:

http://www.heise.de/security/meldung/Banking-Trojaner-Gugi-umgeht-Overlay-Sperre-in-Android-Marshmallow-3315473.html?wt_mc=rss.security.beitrag.rdf
http://www.computerwoche.de/a/banking-trojaner-trickst-android-6-0-aus,3322716
http://newsroom.kaspersky.eu/de/texte/detail/article/banking-trojaner-gugi-ueberlistet-neue-sicherheitsfunktionen-von-android-6
http://www.pc-magazin.de/vergleich/android-antivirus-test-security-apps-vergleich-3195548.html

III. SWIFT und weg – Banken verlieren erneut Geld durch Cyberattacken nach SWIFT-Datenklau

Seit Anfang September ist amtlich, was Bank-Security-Leute seit dem aufgeflogenen Mega-Cyber-Bankraub bei der Nationalbank von Bangladesh (wir berichteten im SWITCH-CERT Security Report vom April 2016) schon immer vermutet hatten: Die in Belgien domizilierte Society for Worldwide Interbank Financial Telecommunication, kurz: SWIFT, hat eingestanden, dass seither weitere Hacks auf Banken erfolgt seien, bei denen die angegriffenen Banken Geld verloren hätten. SWIFT warnte davor, dass die Bedrohung dauerhaft sei, auch weil sich die Täter immer wieder an neue Gegebenheiten anpassen würden. Der Zahlungsdienstleister forderte die 11.000 Geldinstitute, die ihm auf der ganzen Welt angeschlossen sind, auf, die Sicherheitsmassnahmen deutlich zu verbessern. Weil sich offenbar die Erkenntnis durchgesetzt hat, dass die Stärke oder Schwäche eines Systems vom schwächsten Element definiert wird, verlieh SWIFT seiner Forderung Nachdruck, indem es drohte, säumige oder gar untätige Mitglieder an Finanzaufsichtsbehörden oder die anderen angeschlossenen Finanzinstitute zu melden.

Damit schwenkt SWIFT auf die Linie jener Banking-Security-Fachleute ein, die der Ansicht sind, der Zahlungsdienstleister müsse viel stärker als bisher prüfen, ob und in welchem Masse sich seine Mitglieder gegen Cyberattacken schützen und seine Mitglieder motivieren, sich untereinander über Angriffsmuster auszutauschen. Ohne überheblich wirken zu wollen, sei darauf verwiesen, dass SWITCH-CERT seit nunmehr 20 Jahren (Gründung am 20. September 1996) Massstäbe bezüglich des Austauschs von Angrifssmustern in Trustful Communities setzt.

Alarmiert zeigte sich zwischenzeitlich auch die Europäische Zentralbank EZB und ihre Bankenufsicht SSM (Single Supervisory Mechanism). Zusammen mit achtzehn beaufsichtigten Banken hat sie ein Pilotprojekt gestartet. In einer Datenbank werden grosse Bankenhacks gesammelt, um daraus ein Analyse- und Frühwarnsystem ableiten zu können. Und auch SWIFT selbst will nachlegen. Rund 22 Jahre (!) nach Einführung der Banking Telecommunication Message prüft die Zahlungsorganisation verschiedene Sicherheitsoptionen, wie z.B. eine Authentifizierung, die noch sicherer sein soll als jene mit zwei Faktoren oder einen Anomalie-Alarm wie er bei der Kreditkartennutzung eingesetzt wird.

Nachzulesen unter:

http://www.n-tv.de/wirtschaft/Hacker-knacken-globales-Zahlungssystem-article18586731.html
https://www.switch.ch/de/dossiers/20-years-of-switch-cert
http://www.nzz.ch/wirtschaft/wirtschaftspolitik/banken-swift-meldet-cyber-angriff-auf-weitere-bank-ld.82361
https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication
https://www.heise.de/security/meldung/Nach-Angriffen-auf-Banken-SWIFT-will-Sicherheit-verstaerken-3221218.html

IV. Es war nur eine Frage der Zeit – Botnet im Internet of Things entdeckt

Eigentlich musste man damit rechnen. Nun haben Sicherheitsexperten von MalwareMustDie einen Trojaner gefunden, der auf IoT-Geräten eine Backdoor einrichtet, wenn diese eine veraltete, auf LINUX basierende Firmware nutzen. Das Hintertürchen erlaubt es Cyberkriminellen, solche Geräte, wie z.B. fest installierte IP-Kameras, zu Botnetzen zusammenzuschliessen und darüber SPAM oder Malware zu verbreiten. Trojaner wie auch das gesamte Vorgehen zeigen sich in doppelter Hinsicht als besonders perfide: Zum einen werden fest installierte Kameras kaum neu gebootet (was die Malware entfernen würde). Zum zweiten verwischt der Trojaner nach der Infizierung der Geräte alle Spuren und nistet sich im Arbeitsspeicher ein. Darum wurde er wohl auch von den Fachleuten von CZ.NIC zunächst nicht entdeckt. Die Sicherheitsleute des tschechischen Top-Level-Domain-Registrars hatten eine infizierte Kamera gekauft, nachdem ihnen auf ihrem Telnet-Honeypot eine sprunghafte Aktivitätssteigerung aufgefallen war. Damit hatten sie die Entdeckung von Trojaner und IoT-Botnet überhaupt erst ins Rollen gebracht. Allen Benutzern älterer IoT-Geräte seien deshalb drei Sicherheitsmassnahmen dringend ans Herz gelegt:

1. Booten (macht man bei fix installierten Kameras nur sehr selten, hilft aber!)
2. Telnet auf den Geräten deaktivieren oder entsprechende Verbindungen zumindest genau beobachten. Außerdem sollten die Geräte durch eine Firewall geschützt und die Internetverbindung des Ports TCP/48101 gekappt werden, so das möglich ist.
3. Keinesfalls sollten solche Geräte ohne eine Firewall betrieben werden.

Nachzulesen unter:

http://www.heise.de/newsticker/meldung/Sicherheitsexperten-finden-IoT-Botnet-3317830.html
https://en.blog.nic.cz/2015/06/16/more-about-the-honeypot-for-telnet-and-botnets
http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html
http://securityaffairs.co/wordpress/50929/malware/linux-mirai-elf.html
http://t3n.de/news/iot-botnet-fiese-linux-malware-744891

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Michael Fuchs verfasst.