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

April 2016

SWITCH

I. Der wohl teuerste Rechtschreibfehler der Geschichte vereitelt den vermutlich grössten Bankraubversuch aller Zeiten

Sie hätten Geschichte schreiben können, hätten sie nur richtig geschrieben. Weil eine Gruppe Cyberkrimineller beim Angriff auf die Zentralbank Bangladeshs aber «Fandation» statt «Foundation» auf ein Transferformular schrieb, flog der wohl grösste Bankraub aller Zeiten auf, noch bevor alle Transfers in Höhe von nahezu einer Milliarde US-Dollar getätigt worden waren. Verglichen damit mögen sich die erbeuteten 80 Millionen wie Peanuts ausnehmen, dennoch ist bereits diese Summe rekordverdächtig. Apropos Peanuts: Aufgefallen ist der Schreibfehler der Deutschen Bank. Doch der Reihe nach: Nach aktuellem Kenntnisstand infizierten bisher nicht identifizierte Hacker offensichtlich Computer der Zentralbank Bangladeshs mit einem ebenfalls noch nicht näher bekannten Trojaner, um sich Kenntnisse darüber zu verschaffen, wie sie am besten bei ausländischen Banken deponiertes Geld der Zentralbank auf eigene Konten transferieren könnten. Zudem stahlen sie SWIFT-Zugangsdaten für die Transfers. Am Wochenende des 4. und 5. Februars 2016 starteten sie dann in schneller Abfolge mehr als 30 Geldtransfers von Konten der Zentralbank beim New Yorker Ableger der US-

Notenbank an offenbar gefakte NGO-Konten in Sri Lanka und auf den Philippinen. Ein 20-Millionen-Transfer an eine «Shalika Fandation» lief auch über die Deutsche Bank, die den Schreibfehler entdeckte und bei der Zentralbank Bangladeshs nachfragte. Zugleich war aufgefallen, dass die Zahlungen nicht von Bank zu Bank erfolgten, worauf der «Shalika»- und alle weiteren Transfers in der Warteschlange gestoppt werden konnten, die zusammengenommen rund 1 Milliarde US-Dollar abgezogen hätten. Trotz eines Grossaufgebots Sri Lankischer und philippinischer Polizei konnte nicht verhindert werden, dass grosse Teile der in den vier geglückten Transfers erbeuteten 80 Millionen Dollars in Casinos gewaschen wurden und nicht mehr auffindbar sind.

Während die Bangladesh Bank die US Federal Reserve mangelnder Sorgfalt bezichtigt, stellen ICT-Security- und Finanzexperten kritische Fragen darüber, wie es denn um die Sicherheit der Bank generell bestellt gewesen sei und ist. Doch sehen sich auch die New Yorker Banker Vorwürfen aus Investoren- wie Politikerkreisen ausgesetzt, das Vertrauen ausländischer Geldhäuser in die Sicherheit der Bank unterminiert zu haben. Ende März hat die Society for Worldwide Interbank Financial Telecommunication SWIFT alle angeschlossenen Bankhäuser angewiesen, ihre Sicherheitsmassnahmen zu verstärken, um Wiederholungsfälle zu vermeiden, zumal zum jetzigen Zeitpunkt der Untersuchung angenommen werden muss, dass die Hacker auch andere Banken im Visier hatten.

Nachzulesen unter:

http://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight-idUSKCN0WC0TC
http://www.tagesanzeiger.ch/panorama/vermischtes/milliardenbankraub-misslingt-wegen-zwei-buchstaben/story/31934921
http://www.zdnet.com/article/malware-was-at-the-root-of-80-million-bangladesh-bank-heist
http://www.zdnet.com/article/bangladesh-bank-debates-lawsuit-against-federal-reserve-over-cyber-fraud
http://www.darkreading.com/cloud/swift-to-issue-warning-in-wake-of-cyberattack-on-bagladesh-central-bank-/d/d-id/1324767

II. Die Schweiz im Fadenkreuz verschiedener Hackergruppen? Serie von DDoS-Angriffen auf Schweizer Webseiten

Mitte März erschütterte eine regelrechte Angriffswelle die Schweiz: Die Webshops von Do-it, Digitec, Galaxus, Interdiscount, LeShop, Melectronics, Micasa und Microspot versagten nach gezielten DDoS-Angriffen zeitweise den Dienst. Betroffen war auch die Website der Schweizerischen Bundesbahnen SBB.

Hinter den Angriffen stecken offenbar mehrere Gruppen mit unterschiedlichen Absichten. So bekannte sich gegenüber inside-it.ch eine Gruppe von «Grey Hats» namens NSHC zu den Angriffen auf Interdiscount, Microspot und die SBB, weil man mit dem Angriff zeigen wollte, dass die Schweiz unzureichend vor Cyberangriffen geschützt ist. Bei einem weiteren Angriff habe NSHC zudem aus der Datenbank der Schweizer Volkspartei (SVP) Namen und E-Mail-Adressen von rund 50.000 Nutzern kopiert – darunter Parteimitglieder, Sympathisanten und Medienkontakte. Auch bei diesem Angriff gehe es NSHC nach eigenen Angaben nicht darum, ihre Opfer zu erpressen oder die Daten zu veröffentlichen.

Dagegen haben andere betroffene Webshops offenbar Erpresserbriefe erhalten. Zudem geht die Melde- und Analysestelle Informationssicherung des Bundes (MELANI) davon aus, dass die Onlineshop-Hacks in Zusammenhang mit 6.000 gestohlenen Kundenkonten und –passwörtern stehen. Hier seien offenbar Black Hats am Werk gewesen, deren Attacken ausschliesslich cyberkriminellen Absichten folgten.

Erpresserschreiben bekamen einige Tage zuvor bereits zahlreiche Schweizerische Finanzinstitute von einer anderen. Diese forderte die Institute auf, 25 Bitcoins zum Schutz vor DDoS-Attacken zu zahlen. in diesem Falle blieben Attacken jedoch auch dann aus, wenn kein Schutzgeld bezahlt wurde.

Nachzulesen unter:

http://www.heise.de/security/meldung/DDoS-Attacken-auf-Schweizer-Websites-3144854.html
http://www.cash.ch/news/alle/onlineshophacks_und_6000_gestohlene_emailkonten_haengen_zusammen-3433299-448
http://www.inside-it.ch/articles/43241
http://www.tagesanzeiger.ch/schweiz/standard/Hacker-erpressen-OnlineShops-mit-Drohbriefen/story/21342550
http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/digitec-reicht-wegen-hackerangriff-strafanzeige-ein/story/13546298

http://www.govcert.admin.ch/blog/19/armada-collective-is-back-extorting-financial-institutions-in-switzerland
http://www.watson.ch/Digital/Schweiz/905636585-DDoS-Attacken-in-der-Schweiz–«Es-meinen-immer-noch-viele--sie-seien-zu-unbedeutend–um-Ziel-eines-Hacker-Angriffs-zu-werden»
http://www.nzz.ch/nzzas/nzz-am-sonntag/cyber-attacken-kriminelle-erpressen-schweizer-online-shops-ld.9083

III. Connected Cars als «Eines der grössten Sicherheitsrisiken dieser Generation»

Man könnte meinen, es sei ein vorab veröffentlichter Aprilscherz gewesen, was da in zahlreichen Medien zu lesen war: Just jenes FBI, das wenige Tage zuvor von Apple die Entsperrung von iPhones von Kriminellen und Terrorverdächtigen verlangt hatte, warnte am 17. März in einem ausführlichen «Public Service Announcement» auf der Webseite www.ic3.gov vor den Gefahren, die das Hacken von vernetzten Autos mit sich bringt. Im SWITCH Security Report hatten wir bereits in mehreren Ausgaben zahlreiche Sicherheits- und Privacy-Aspekte des «Connected Driving» ausgeleuchtet. Nun haben also auch die amerikanischen Sicherheitsexperten erkannt, dass in vernetzten Autos tatsächlich hohe Risiken mitfahren. Conner Forster von zdnet.com bezeichnet sie gar als «eines der grössten Sicherheitsrisiken dieser Generation». Er begründet seine Einschätzung nicht nur damit, dass vernetzte Autos unzureichend gegen Attacken geschützt seien. Vielmehr sammelten sie selbst jede Menge Daten und ermöglichten Hackern tiefe Einblicke ins Leben der Besitzer. Und schliesslich machten die hochkomplexe Arbeitsteilung im Produktionsprozess, die schiere Menge von Fahrzeugen im öffentlichen Raum und ihre Manipulierbarkeit vernetzte Autos zum Hochsicherheitsrisiko.

Derweil nehmen sich auch europäische Automobilclubs des Themas unter verschiedenen Perspektiven an. So hat z.B. der österreichische Automobilclub ÖAMTC vor kurzem die Kampagne «Mein Auto – Meine Daten» gestartet und sich damit in direkten Widerspruch zum Ex-VW-Vorstandsvorsitzenden Winterkorn gestellt, der Ende 2014 auf der 31C3 proklamiert hatte: «Your car´s data are mine!» (wir berichteten im SWITCH Security Report vom Februar 2015). Und der deutsche ADAC hat in einem Test nachgewiesen, dass es gar kein Connceted Car braucht, um Kriminellen ein Angebot zu machen. Die Zutrittstechnik «Keyless Entry» ist – obwohl Gefahrenpotential und Angriffsmethode seit Jahren bekannt sind – immer noch so anfällig, dass alle 24 untersuchten Fahrzeuge, die mit dieser

Komfortfunktion ausgestattet sind, nicht ausreichend gegen ein böswilliges Aufschliessen geschützt sind. Er rechnet damit, dass weitere Hersteller und Fahrzeuge betroffen sein könnten und sieht die Hersteller in der Pflicht, die Sicherheitslücke zu schliessen.

Nachzulesen unter:

http://www.ic3.gov/media/2016/160317.aspx
http://motherboard.vice.com/read/if-the-fbi-is-so-worried-about-car-hacking-why-is-it-fighting-encryption
http://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk
http://www.bbc.com/news/technology-35841571
http://futurezone.at/netzpolitik/oeamtc-chef-auto-daten-gehoeren-dem-konsumenten/186.286.964
http://www.heise.de/security/meldung/ADAC-Viele-aktuelle-Pkw-Modelle-ueber-Funk-knackbar-3140796.html
http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-09_de.pdf

IV. Beschlossene Sache: Das neue BÜPF

Die Eidgenössischen Räte haben in ihrer Frühjahrssession der Revision des Bundesgesetzes zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) zugestimmt und das lange umstrittene Gesetz beschlossen (wir berichteten im SWITCH Security Report 10/2015). Es ermöglicht den Strafverfolgungsbehörden in der Schweiz u.a., bei schweren Straftaten Staatstrojaner auf Computern von Verdächtigen zu installieren oder IMSI-Catcher einzusetzen, um deren Handys zu orten und abzuhören. Im Gegenzug wurde darauf verzichtet, die Fristen zur so genannten Vorratsdatenspeicherung zu verlängern, um für eine Abstimmung im Rahmen eines erwarteten Referendums der BÜPF-Gegner in guter Ausgangslage zu sein.

Dessen Ankündigung liess nicht lange auf sich warten. Angeführt von SVP-Nationalrat Franz Grüter will sich ein Komitee quer durch das politische Spektrum der Schweiz dafür stark machen, das in seinen Augen über das Ziel hinaus schiessende BÜPF doch noch zu Fall zu bringen. Auch der Verein «Digitale Gesellschaft» bedauert, dass nach seiner Ansicht «die Chance verpasst wurde, eine längst fällige Grundsatzdebatte zur Überwachung zu führen» und bewertet den neuen Gesetzesentwurf als «unverhältnismässig und gefährlich». Die nächste Runde im nunmehr mehr als 2-jährigen Ringen um eine mehrheitsfähige

Abwägung zwischen berechtigten Sicherheitsinteressen und Bedrohung der Freiheitsrechte ist also eingeläutet.

Nachzulesen unter:

http://www.inside-it.ch/articles/43257
http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-10_de.pdf
http://www.computerworld.ch/news/politik-gesellschaft/artikel/buepf-unter-dach-und-fach-69857
http://www.netzwoche.ch/de-CH/News/2016/03/17/Das-Buepf-ist-beschlossene-Sache.aspx
http://www.tagesanzeiger.ch/schweiz/standard/Trotz-Bruessel-Komitee-kaempft-gegen-mehr-Ueberwachung/story/24190094
http://www.watson.ch/Schweiz/Büpf/182605621-Telefonüberwachung–Piratenpartei-ergreift-das-Referendum-gegen-das-BÜPF
https://www.digitale-gesellschaft.ch/2016/03/21/buepf-2-0-schlecht-ist-nicht-gut-genug

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.