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

Juni 2016

SWITCH

I. Richtig UnAngenehme Geschichte: Unbekannte erbeuten bei einem Cyber-Angriff auf die RUAG 20 Gigabyte Daten

Unternehmen, die im Marktsegment «Defense» unterwegs sind, tun das in aller Regel lieber in Ruhe. Nun sorgt ausgerechnet die 1998 aus der Zusammenlegung der eidgenössischen Produktions- und Unterhaltsbetriebe der Schweizer Armee hervorgegangene «RüstungsUnternehmen-AG» RUAG mit der Meldung eines APT (Advanced Persistent Threat)-Angriffs auf ihre IT-Infrastruktur für Schlagzeilen. Im Dezember 2015 tauchten erstmals Hinweise darauf auf, die jedoch zurückgehalten wurden, um die eingeleiteten Ermittlungen nicht zu gefährden. Im Mai 2016 gelangten dann durch ein Leck Informationen über den Fall an die Medien, die diesen denn auch prompt publizierten. In der Folge blieben weitere Angriffe aus, so dass die Ermittlungen zu Fragen der Täterschaft nicht weiter fortgesetzt werden konnten und bislang erfolglos blieben. Eine detaillierte Timeline findet sich im technischen Kurzbericht der Melde- und Analysestelle Informationssicherung MELANI (siehe Link unten), die in bemerkens- und lobenswerter Geschwindigkeit unmittelbar nach Bekanntwerden des Falls eine

ausführliche Analyse veröffentlicht hatte, um auch anderen Unternehmen Hinweise zu geben, dass und wie sie sich gegen solche Angriffe schützen müssen.

Die Fakten: Die RUAG wurde überaus professionell, geduldig und über einen langen Zeitraum hinweg mit einer Schadsoftware der Turla/Advig-Familie angegriffen. Bei diesem Angriff wurden ganz gezielt mehr als 20 Gigabyte Daten von den Servern des Unternehmens kopiert. Ursprüngliche Medienberichte, wonach Daten erbeutet worden seien, die zur Enttarnung von Angehörigen militärischer Eliteeinheiten oder des Nachrichtendienstes des Bundes führen könnten, bezeichneten Verantwortliche sowohl der RUAG als auch der zuständigen Stellen des Bundes ebenso als reine Vermutung wie solche, nach denen die Angreifer in Russland zu suchen seien.

Dass der Fall dennoch zu hoher Nervosität bei allen Beteiligten und möglichen Betroffenen führt, zeigt die Auseinandersetzung zwischen dem VBS (Departement für Verteidigung, Bevölkerungsschutz und Sport) und der RUAG um die Frage, wem der Angriff eigentlich gegolten habe. Wohl auch, um seine Kunden nicht nur im Marktsegment «Defense», sondern auch im zweiten Kerngeschäft «Aerospace» zu beruhigen, hatte das Unternehmen kommuniziert, dass keine RUAG-Daten, sondern ein der RUAG überlassenes Adressverzeichnis der Bundesverwaltung gestohlen worden sei. Deshalb gehe man davon aus, dass es die Angreifer auf den Bund abgesehen hätten, was Verteidigungsminister Guy Parmelin dahingehend kommentierte, dass der Angriff auf die RUAG und nicht auf sein Departement erfolgt sei. Da inzwischen sowohl die CVP als auch einzelne Politiker anderer Parteien den aktuellen Status quo alles andere als zufriedenstellend finden, wird die RUAG in dieser Sache wohl so schnell nicht zur Ruhe (zurück) kommen können.

Nachzulesen unter:

https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/fachberichte/technical-report_apt_case_ruag.html
http://www.vbs.admin.ch/internet/vbs/de/home/documentation/news/news_detail.61788.nsb.html
http://www.golem.de/news/hack-von-ruestungskonzern-schweizer-cert-gibt-security-tipps-fuer-unternehmen-1605-121048.html
http://www.tagesanzeiger.ch/schweiz/standard/ruaghacker-hatten-es-wohl-auf-bund-abgesehen/story/31611068
http://www.srf.ch/news/schweiz/hackerangriff-auf-die-ruag-schweizer-elitetruppe-enttarnt
http://www.nzz.ch/cyber-spionage-angriff-auf-ruag-mehr-als-20-gigabyte-daten-entwendet-ld.84138
http://www.inside-it.ch/articles/43929
http://www.nzz.ch/schweiz/aktuelle-themen/ruag-cyber-angriffe-lassen-sich-nicht-ausschliessen-ld.83097

http://www.heise.de/newsticker/meldung/Hacker-stahlen-mehr-als-20-GByte-Daten-bei-Schweizer-Ruestungsbetrieb-3216344.html
http://www.computerworld.ch/news/politik-gesellschaft/artikel/cvp-fordert-debatte-zu-cyber-angriff-auf-ruag-70219
https://www.balthasar-glaettli.ch/2016/05/23/ruag-hack-untersuchungsbericht-wirft-fragen-auf/

II. Twitter macht dicht: US-Kurznachrichtendienst sperrt sich gegen US-Nachrichtendienste

Im Mai hat Twitter eine neue Landmarke in der Auseinandersetzung zwischen US-Nachrichtendiensten und –Strafverfolgungsbehörden auf der einen und dem Silicon Valley auf der anderen Seite gesetzt. Das oft (und in diesem Zusammenhang durchaus ironisch) als Kurznachrichtendienst bezeichnete Unternehmen hat durchgesetzt, dass der mit ihm verbundene Analysedienst Dataminr die Zusammenarbeit mit den Geheimdiensten beendet. Twitter hält 5% des Aktienkapitals und gewährt Dataminr exklusiv den Zugang zu allen Tweets, die auf Twitter gepostet werden und das Recht, die daraus gewonnenen Daten weiter zu verkaufen. Dataminr durchforstet neben Twitters Firehose (eben jenen Nachrichtenstrom aller Tweets) auch Verkehrsdaten, Nachrichten und andere Quellen nach Stichworten, die von Dataminr-Kunden nachgefragt werden, und verknüpft diese mit Marktinformationen und Geodaten, um u.a. die Relevanz, Glaubwürdigkeit oder Dringlichkeit von Informationen zu prüfen und im Bedarfsfall zahlende Nutzer zu alarmieren.

In der jüngst abgelaufene Testphase war die Zusammenarbeit zwischen Dataminr und den US-Behörden offenbar so erfolgreich, dass sie von beiden Seiten dauerhaft hätte weitergeführt werden sollen. Offenbar aus Sorge darum, dass eine als zu eng empfundene Verbindung zwischen Twitter und den US-Diensten einerseits zur Verärgerung von Usern und Kunden, andererseits zur Motivation für Terrorgruppen zu Angriffen auf Twitterverantwortliche führen könnte, hat Twitter-CEO Jack Dorsey seine vertraglich zugesicherte Vetokarte gezogen und darauf verwiesen, dass alle Nachrichten auf Twitter ohnehin ja öffentlich zugänglich seien. Die Geheimdienste bräuchten daher keinen privilegierten Zugang. Inwieweit es da ins Bild passt, dass der russische Auslandssender RT weiterhin Dataminr-Kunde bleiben kann, weiss wohl Jack

Dorsey allein. RT wurde 2005 vom russischen Staat und seinem Präsidenten (und ehemaligen Chef des russischen Inlandsgeheimdienstes FSB) Putin als Gegengewicht zu westlichen Medien und deren Informationen ins Leben gerufen.

Nachzulesen unter:

http://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682
http://www.heise.de/newsticker/meldung/Schutz-vor-Ueberwachung-Twitter-kappt-Analyse-Zugang-der-US-Geheimdienste-3198781.html
http://www.cnbc.com/2016/05/13/why-twitter-chose-to-do-battle-with-the-cia.html
https://www.dataminr.com/dataminr-partnership-with-twitter
http://www.valuewalk.com/2016/05/twitter-restricts-us-allows-russia
http://www.wsj.com/articles/twitter-picks-russia-over-the-u-s-1463346268

III. iPhone hält dicht: Nach 48 Stunden verlangt Touch ID das Passwort

Dass neue Technologien neue Rechtsbeurteilungen erfordern ist nichts Neues. Dass Strafverfolger versuchen, Beschuldigte zu Taten zu bewegen, mit denen sie sich selbst belasten könnten und die deshalb im Rechtsstaat nicht erzwungen werden dürfen, auch nicht. Aus der Kombination beider Erkenntnisse stellt sich aber die neue und überaus interessante Frage: Wenn Smartphones mit einem Fingerabdrucksensor und nicht mit einem Passwort geschützt sind, die Abnahme von Fingerabdrücken aber ein legales Mittel der Strafverfolgung ist – ist es dann legal, wenn die Ermittler eine/n Beschuldigte/n auffordern, ihr/sein mit Touch ID geschütztes Smartphone zu entsperren? Security-Experten haben bei der Einführung dieser Technologie immer wieder genau davor gewarnt. Nun hat eine kalifornische Richterin dem FBI binnen weniger als einer Stunde einen Durchsuchungsbefehl für das iPhone einer des Identitätsdiebstahls Beschuldigten erteilt, auf dem die Ermittler Daten einer Gang vermuteten, der der Freund der Beschuldigten nach Aussagen des FBI angehörte. Sowohl jenseits als auch diesseits des Atlantiks ist nun unter Digital Rights-Experten eine Kontroverse drüber entstanden, ob dieser Zwang zum Entsperren des eigenen Telefons via Fingerabdruck geltendes Recht verletzt oder nicht.

Pech für die Ermittler: Auch nachdem sie die Beschuldigte mit dem gültigen Beschluss gezwungen hatten, das iPhone via Fingerabdruck zu entsperren, blieb das Telefon auch noch gesperrt, nachdem sie der Beschuldigten mit jedem ihrer 10 Finger einen Unlock-Versuch abgefordert hatten. Apples Touch ID verlangt

nämlich aus Sicherheitsgründen zusätzlich ein Passwort, wenn der Fingerabdrucksensor 48 Stunden lang nicht aktiviert wird.

Wem weder Passwort noch Fingerabdrucksensor genügend Sicherheit liefern, der wird voller Spannung auf das warten, was derzeit in Mountain View, Kalifornien, entwickelt wird. Dort will Googles Forschungsteam ATAP bis spätestens 2016 einen sicheren Zugang zu Apps und Devices schaffen, der ganz ohne Passwort und Fingerabdruck auskommt und dennoch zuverlässig schützen soll (mehr dazu im nächsten Artikel).

Nachzulesen unter:

http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html
http://www.heise.de/mac-and-i/meldung/US-Richterin-ordnete-iPhone-Entsperrung-per-Fingerabdruck-an-3195443.html
https://www.lawblog.de/index.php/archives/2016/05/03/die-sache-mit-dem-fingerabdruck
http://money.cnn.com/2016/05/12/technology/fbi-fingerprint-iphone

IV. Passwort für e-Banking und anderes? Künftig getrost vergessen!

ATAP als Googles schnellen Brüter für Mobile-Device-Innovationen zu bezeichnen ist wohl keine Untertreibung. Denn das urprünglich bei Motorola angesiedelte Forschungsteam gibt sich grundsätzlich maximal 2 Jahre, um aus einem Projekt ein marktfähiges Produkt zu machen. Das gilt auch für Abacus. 2015 gestartet können User, wenn es nach ATAP geht, damit bis spätestens 2017 zumindest auf Android-Geräten Passwörter oder Fingerabdrucksensoren getrost vergessen. Ein Algorithmus berechnet aus Sensorendaten im Gerät, Gesichtserkennung und anderen biometrischen Daten, Tippgeschwindigkeit, bekannten Bluetoothgeräten in der Nähe und anderen Komponenten einen sogenannten Trust Score. Je nach Sensibilität und Sicherheitsrisiko sollen Apps mit unterschiedlich hohen Trust Scores gesichert werden – also Spiele mit eher niedrigen, e-Banking-Apps mit sehr hohen Scores. Verständlich, dass viele Finanzinstitute bereits Interesse an Abacus angemeldet haben und nach Aussagen von Projektleiter Daniel Kaufmann bereits mehrere grosse Finanzunternehmen diese neue Authentifizierung aktiv testen. Bis Ende 2016 will Google ATAP Entwicklern die neue Trust API zur Verfügung stellen – wobei

man in diesem Zusammenhang das Kürzel API wohl nicht nur als Application Programming Interface, sondern auch als Advanced Personal Identification lesen könnte.

Nachzulesen unter:

http://www.zeit.de/digital/datenschutz/2016-05/android-google-trust-score-passwoerter
http://m.heise.de/security/meldung/Google-will-bis-2017-Passwoerter-auf-Android-Geraeten-loswerden-3217827.html
https://www.theguardian.com/technology/2016/may/24/google-passwords-android
http://www.pcworld.com/article/3072887/android/googles-trust-api-pushes-password-free-login-capability-for-android-apps.html
http://www.infoworld.com/article/3074249/security/googles-abacus-api-adds-security-by-subtracting-passwords.html

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