SWITCH-CERT Report zu aktuellen Trends im Bereich IT-Security und Privacy

Mai/Juni 2019

SWITCH

I. Ans Licht geholt: Bundeskriminalamt schliesst weltweit zweitgrössten illegalen Marktplatz im Darknet

Auch die Bösen haben Geschäftsmodelle – oder imitieren sie aus der Welt der Guten. Im Darknet kombinieren sie e-commerce, Verschlüsselungstechnologien, anonymisierte Browser und Kryptowährungen wie Bitcoin, Ethereum oder Monero zu mehr oder weniger gigantischen Handelsplattformen. Über diese werden Multi-Millionen-Umsätze mit Drogen, Waffen, Menschenhandel, illegaler Pornografie, Malware und anderen illegalen Waren und Dienstleistungen, wie z.B. gestohlenen Log-In-Daten, Cyberangriffen und Botnets, gemacht. So wurden beispielsweise über den 2013 geschlossenen Marktplatz "Silk Road" in nur zwei Jahren Umsätze von mehr als 1,2 Milliarden US-Dollar abgewickelt. Daraus sollen an den US-amerikanischen Gründer und Betreiber Ross Ulbricht ca. 80 Millionen Dollar an Provisionen geflossen sein. Diese lukrativen Perspektiven hatten wohl auch mehrere Deutsche motiviert, die als Betreiber der 2017 ausgehobenen Plattform "Hansa-Market" verhaftet worden waren. Auch sie waren Umsatzmilliardäre und Provisionsmillionäre.

Kaum waren sie hinter Gittern, startete – wieder in Deutschland – der nächste Darknet-Marktplatz: "Wall Street Market". Auch der entwickelte sich binnen kürzester Zeit zu einer Erfolgsmaschine mit bemerkenswerten Geschäftszahlen: 1,1 Millionen registrierte Nutzer.

Täglich ca. 1.250 Transaktionen bei 63.000 Verkaufsangeboten, insgesamt 400.000 Verkäufe, davon 250.000 Betäubungsmittel, will heissen: Drogen. Zum Vergleich: Auf dem mit 3,2 Mio. Mitgliedern grössten legalen Online-Marktplatz der Schweiz (ricardo.ch) tummeln sich rund 360.000 Besucher am Tag. Während die Zahlen des legalen Marktplatzes vom Betreiber selbst stammen, wurden die für Wall Street Market vom deutschen Bundeskriminalamt veröffentlicht.

In einer Medienkonferenz gab das BKA am 3. Mai 2019 bekannt, Wall Street Market nach 18-monatigen, gemeinsam mit der deutschen Zentralstelle für Internetkriminalität (ZIT), Europol, holländischen und amerikanischen Stellen geführten Ermittlungen geschlossen und drei Deutsche im Alter zwischen 22 und 31 Jahren verhaftet zu haben. Sie werden verdächtigt, die illegale Plattform im Darknet betrieben und dafür Provisionen zwischen zwei und sechs Prozent erhalten zu haben. Im Fall einer Verurteilung drohen ihnen bis zu 15 Jahren Haft (zum Vergleich: Silk Road-Gründer Ulbricht wurde zu einer lebenslangen Haftstrafe verurteilt). Verdachtserhärtend dürfte sich auswirken, dass bei Durchsuchungen ihrer Wohnungen mehr als eine halbe Million Euro in Bargeld sowie umfangreiche Unterlagen zu grossen Mengen der Kryptowährungen Bitcoin und Monero sowie eine Schusswaffe gefunden wurden. Ob die Ermittler auf den inzwischen beschlagnahmten Servern auch auf Daten der bis zu 5.400 Verkäufer sowie der mehr als 1 Million Nutzer zugreifen konnten, um diese zu belangen, blieb zunächst offen. Bekannt wurde aber, dass im Laufe der Ermittlungen zwei der aktivsten Verkäufer in Los Angeles verhaftet wurden. Zeitglich mit der Schliessung von Wall Street Market gab Europol bekannt, dass der auch als "Valhalla Marketplace" firmierende finnische Darknet-Marktplatz Silkkitie geschlossen wurde. Die Nachfolger dürften indes bereits schon wieder lanciert sein.

Nachzulesen unter:

https://m.tagesanzeiger.ch/articles/28284916
https://help.ricardo.ch/hc/de/articles/115002981745-Überblick-ricardo-ch-AG
https://techcrunch.com/2019/05/03/how-german-and-us-authorities-took-down-the-owners-of-darknet-drug-emporium-wall-street-market
https://www.heise.de/newsticker/meldung/Wall-Street-Market-BKA-und-FBI-heben-illegalen-Darknet-Marktplatz-aus-4412205.html

II. WhatsApp, Staatstrojaner? Oder: Weshalb Privatsphäre in der Stadt San Francisco besser geschützt ist als auf Zuckerbergs Messenger

Gegensätzlicher könnten zwei Meldungen zum Thema Privatsphäre kaum sein als jene, die uns jüngst aus Kalifornien erreichten. Die schlechte zuerst: Mitte Mai publizierte der zu Mark Zuckerbergs Facebook-Konzern gehörende Messengerdienst WhatsApp eine Sicherheitslücke, durch die Spyware auf iPhones, Android- und Windows-Smartphones sowie TV-Geräten mit Samsungs Tizen-Betriebssystem eingeschleust werden konnte. WhatsApp

hat die Sicherheitslücke inzwischen geschlossen, empfiehlt aber allen Nutzern, ein entsprechendes Update einzuspielen.

Sicherheitsexperten gehen davon aus, dass die Lücke bislang nicht für einen breit angelegten Hack, sondern für gezielte Attacken auf ausgewählte Telefone, insbesondere auf die von Anwälten und Mitarbeitern von Menschenrechtsorganisationen, genutzt worden ist. Die hochentwickelte Spyware konnte per Anruf auch dann auf attackierte Telefone eingeschleust werden, wenn die oder der Angerufene den Anruf gar nicht entgegennahm. Zudem verschwanden die Anrufe in den LogFiles des Telefons. Dafür hätte es die Schadsoftware offenbar ermöglicht, dass die Angreifer Kamera und Mikrofon des befallenen Smartphones einschalten und E-Mails, Nachrichten und Ortungsdaten auslesen konnten. Berichten der Financial Times zufolge sei auch ein Londoner Menschenrechtsanwalt Ziel des Angriffs gewesen. Sein Telefon sei aber stark gesichert gewesen, so dass der Angriff letztlich ins Leere gelaufen war.

All dies liess Fachleute zum Schluss kommen, dass die Spyware von der israelischen Firma NSO Group entwickelt worden war. Die auf einen Firmenwert von 1 Milliarde US-Dollar taxierte Softwarefirma bewirbt ihr Starprodukt "Pegasus" im Mittleren Osten und bei westlichen Geheimdiensten als Spionagesoftware im Kampf gegen Terrorismus und andere Verbrechen. Der angegriffene Anwalt hatte mehrere mexikanische Journalisten und einen saudischen Dissidenten in einer Klage gegen NSO vertreten. NSO konterte entsprechende Nachfragen mit dem Hinweis, dass man die Software Geheimdiensten und Sicherheitsbehörden anbiete, aber nicht selbst einsetze.

Die gute Nachricht in Sachen Privatsphäre kommt ebenfalls aus Kalifornien. Dort hatte die lokale Gesetzgebungsinstanz "Board of Supervisors" am 14. Mai ein Gesetz beschlossen, dass der Polizei und anderen städtischen Behörden den Einsatz von sämtlicher Überwachungstechnologie – von Gesichtserkennungssoftware bis zu Nummernschildscannern – in der ganzen Stadt untersagt oder zumindest genehmigungspflichtig macht. Das Gesetz gilt derzeit nicht für private Firmen, Häfen und Flughäfen, an denen solche Technologien eingesetzt werden. Andere Städte in den USA erwägen ebenfalls, den Schutz der Privatsphäre durch die Einschränkung von Überwachungstechnologien auszudehnen. Und der Kongress in Washington berät derzeit über einen Vorstoss, privaten Firmen die Erfassung und Erkennung von Gesichtern der Konsumenten ohne deren Einverständnis zu verbieten. Gesichtsscanning ist nicht nur deswegen in der Diskussion, weil der flächendeckende Einsatz wie beispielsweise in China in die totale Überwachung führt, sondern auch (noch) relativ fehleranfällig ist. So berichteten die NZZ vom 4. Mai und die SRF-Sendung 10 vor 10 am 3. Juni 2019, dass die überwiegend von Uiguren und Moslems bewohnte Provinz Xinjiang dank Gesichtserkennung und SmartphoneApp quasi unter Totalüberwachung stehe. Und wir berichteten im Security Report 6/2018 darüber, dass eine der prominentesten Unternehmerinnen Chinas irrtümlich an den öffentlichen Pranger gestellt worden war, weil die automatische Gesichtserkennung ihr Werbeporträt auf einem

vorüberfahrenden Bus für das verbotene Überqueren der Strasse bei Rotlicht verantwortlich gemacht hatte.

Nachzulesen unter:

https://www.nzz.ch/digital/sicherheitsluecke-bei-whatsapp-ermoeglichte-die-installation-von-ueberwachungssoftware-ld.1481584
https://www.spiegel.de/netzwelt/apps/whatsapp-sicherheitsluecke-ermoeglichte-gezielte-ueberwachung-update-noetig-a-1267300.html
https://www.nzz.ch/international/san-francisco-verbietet-gesichts-scanner-ld.1481881
https://www.faz.net/aktuell/politik/gesichtserkennung-in-china-totale-kontrolle-15253415.html
https://www.nzz.ch/international/xinjiang-die-polizei-hat-die-uiguren-mit-einer-app-im-griff-ld.1479234
https://www.srf.ch/play/tv/sendung/10vor10?id=c38cc259-b5cd-4ac1-b901-e3fddd901a3d
https://securityblog.switch.ch/2018/12/20/the-november-december-2018-issue-of-our-switch-security-report-is-available

III. Privatsphäre bei Facebook zum Zweiten: Wenn der Anwalt dem Chef widerspricht

Zur Facebook-Entwicklerkonferenz F8 überraschte Mark Zuckerberg mit dem Titel seines Headliners "Die Zukunft ist privat!" Freunde wie Kritiker gleichermassen. War das nur ein neuer Marketing-Gag, oder hatten die Skandale um den laxen Umgang der Datenkrake aus Menlo Park mit der Privatsphäre seiner Nutzerinnen und Nutzer den Konzernchef zur Kursumkehr bewogen? Wer ihm zuhörte musste zunächst Letzteres annehmen. Verkündete doch Zuckerberg nicht weniger als eine strategische Neuausrichtung seines Unternehmens weg vom "digitalen Marktplatz" hin zum "digitalen Wohnzimmer". Facebook-Unternehmen sollten künftig verstärkt die Privatsphäre berücksichtigen. So käme zum Beispiel End-to-end-Verschlüsselung künftig nicht nur bei WhatsApp, sondern auch bei Messenger zum Einsatz. Ob das Unternehmen damit verlorengegangenes Vertrauen zurückgewinnen kann, um neue Angebote, wie eine direkte Shopping-Funktion bei Instagram oder eine eigene Dating-Plattform zum Laufen zu bringen, wird sich zeigen müssen.

Vor diesem Hintergrund darf bezweifelt werden, dass die Aussage des Facebook-Anwalts Orin Snyder bei einer Gerichtsanhörung in San Francisco verkaufsfördernd war. Der hatte im Hearing zum Cambridge Analytica Skandal argumentiert: "Es hat kein Eindringen in die Privatsphäre gegeben, weil es keine Privatsphäre gibt."

Nachzulesen unter:

https://www.faz.net/aktuell/wirtschaft/diginomics/entwicklerkonferenz-von-facebook-die-zukunft-ist-privat-16165374.html
https://www.heise.de/newsticker/meldung/Facebook-Rechtsanwalt-Es-gibt-keine-Privatsphaere-4436701.html

IV. Symmetrie als grundlegendes Prinzip: Gibt es Software as a Service, lässt Cybercrime as a Service nicht lange auf sich warten

Wie schon in Punkt I gezeigt, ist Symmetrie ein grundlegendes Ordnungsprinzip unserer Welt: Yin und Yang, Licht und Schatten, Gut und Böse finden sich auch in der digitalen Welt immer wieder. Jüngster Beweis: Mitte Mai gaben das US Justizdepartement und Europol bekannt, in einer gemeinsamen verdeckten Aktion das Cyberkriminellen-Netzwerk um die Malware Goznym und das bereits zwei Jahre zuvor aufgeflogene Botnetz "Avalanche" dingfest gemacht zu haben. Die Malware hatte bis dahin mehr als 41.000 Rechner befallen und versucht, die Opfer um geschätzte 100 Millionen US-Dollar zu erleichtern. Wie gross der Schaden tatsächlich ist, konnte bislang nicht ermittelt werden.

Dagegen zeigte sich, dass die Täter ein Netzwerk an teilweise hochspezialisierten Cyberkriminellen entwickelt und betrieben hatten, das Steven Wilson, Chef des European Cybercrime Centers als "Supermarkt für Cybercrime Services" bezeichnete. Spezialisten waren jeweils nur für Teile der Operation zuständig, die wie in einer Supply Chain zusammengefügt wurden. Für ihre Dienste warben die aus Russland, der Ukraine, Bulgarien, Moldawien und Georgien stammenden Programmierer, Malware-Entwickler, Bulletproof Hoster und andere Kriminelle in schwer zugänglichen Onlineforen unter dem Titel "Cybercrime as a Service". Symmetrie ist überall – auch im Darknet.

Nachzulesen unter:
https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation
https://www.wired.com/story/goznym-takedown-cybercrime-supply-chain
https://www.heise.de/newsticker/meldung/Malware-Attacken-ueber-Avalanche-Botnet-Drahtzieher-vor-Gericht-4423942.html

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