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

September/Oktober 2019

I. Datensicherheit wird zur Challenge für Challenger-Banken

Mit seinem 1994 geäusserten Statement "Banking is neccessary, Banks are not." hat Bill Gates vor 25 Jahren das Mantra für alle FinTech Startups formuliert. Mit N26 und Revolut haben Ende 2018 und im ersten Halbjahr 2019 zwei der erfolgreichsten Challenger-Banken erkennen müssen, dass es im Banking ein weiteres Essential gibt, um das weder klassische noch Smartphone-Banken herumkommen: Sicherheit.

So berichteten verschiedene Medien im März 2019, dass N26-Kunden durch Phishing-Attacken bis zu 80.000 Euro verloren hatten. Im August wurde bekannt, dass mehrere Konten von Revolut-Kunden in der Schweiz geplündert worden waren. Die Schadenssummen bewegten sich dabei zwischen 8.000 und 30.000 Franken, die – wie auch im Fall der N26-Attacken – nach Angaben beider FinTechs den Kunden zwischenzeitlich ausgeglichen worden seien. Obwohl fälschlicherweise als "Hack" bezeichnet, verschafften sich die Cyberkriminellen in beiden Fällen mit klassischem Phishing Zugang zu den Konten der Betroffenen.

Davor, dass der erkennbare Erfolg von Banking-Apps geradezu einen Boom für Mobile-Banking-Trojaner im Darknet gezündet habe, warnt die IT-Security-Firma "Crowdstrike" in ihrem auf unten zitierter Website zum Download bereitgestellten "2019 Mobile Threat Landscape Report". Dem Report zufolge schicken die Angreifer Malware auf drei Wegen auf die Smartphones der Banking-App-User:

Zum einen werden Trojaner in Spiele- oder Sprach-Apps versteckt.

Zum zweiten verschicken die Kriminellen täuschend echt aussehende SMS, in denen sie vortäuschen, die Bank zu sein, die zum Update der App auffordert. Der dafür anzuklickende Link führt dann geradewegs auf eine Fake-Website und führt nach dem Download direkt ins Desaster. Nach Angaben von Crowdstrike bieten die Macher des sich seit März 2019 ausbreitenden Trojaner "Gustuff" inzwischen Fakes für mehr als 100 Finanzinstitute an.

Und zum dritten nutzen Kriminelle nach wie vor klassisches E-Mail-Phishing, das dann seinerseits zu gefakten Websites und den bekannten Konsequenzen führt.

Sicherheitsforscher verweisen in diesem Zusammenhang darauf, dass Textnachrichten in Form von SMS als meistgenutzter Kanal der 2-Faktor-Authentifizierung keine Garantie für sicheres Einloggen biete, weil Textnachrichten relativ leicht abzufangen seien. So überraschte der Kurznachrichtendienst Twitter Ende August 2019 seine Nutzerinnen und Nutzer damit, dass sie keine Tweets per SMS mehr verschicken konnten. Zuvor war der Account des Gründers Jack Dorsey gehackt und zur Verbreitung rassistischer Nachrichten genutzt worden. Aller Wahrscheinlichkeit nach war Dorsey Opfer eines so genannten SIM-Swapping-Angriffs geworden.

Dabei verschaffen sich Angreifer Zugriff auf die SIM-Karten ihrer Opfer und leiten alle Anrufe und Textnachrichten auf ihre eigene Karte um. Fatal: Genau auf diesem Weg erfolgen die meisten 2-Faktor-Authentifzierungen. Um eine SIM-Karte zu kapern, muss sich ein Angreifer bisher aber zunächst die Mobilnummer seines Opfers verschaffen, und dann den Herausgeber der Karte, also den Mobilfunkbetreiber, davon überzeugen, dass er sein Smartphone verloren hat und eine neue Karte braucht. Dabei macht er dann Angaben, die die Umleitung aller Sprach- und Textnachrichten auf sein Handy ermöglichen.

Dass SIM-Swapping eine grösser werdende Bedrohung darstellen dürfte, zeigt sich auch daran, dass Sanyam Jain, ein Sicherheitsforscher der GDI-Foundation, zum Schutz der freien Kommunikation im Internet anfangs September 2019 auf einem Internetserver eine unverschlüsselte Sammlung von insgesamt 419 Millionen Telefonnummern samt Facebook-ID entdeckt hatte. Über die Facebook-ID lässt sich der Username relativ leicht ermitteln, doch war das in vielen Fällen gar nicht mehr nötig, weil die Telefonnummern

teilweise schon mit Klarnamen, Geschlecht und Staatsangehörigkeit verknüpft waren. Facebook hat die Echtheit der Daten zwischenzeitlich bestätigt. Ob sie für SIM-Swapping eingesetzt wurden oder werden, war indes nicht auszumachen. Die Datenbank ist inzwischen vom Serverbetreiber offline genommen worden.

Fest steht dagegen – und das ist die gute Botschaft – dass es einen einfachen Schutz gegen SIM-Swapping gibt. Denn viele Mobile-Betreiber bieten an, die eigene Nummer mit einer PIN oder einem Code zusätzlich abzusichern, ohne deren Bekanntgabe Service-Mitarbeitende weder Änderungen an der Telefonnummer oder der Karte vornehmen, noch überhaupt Informationen an Anrufende weitergeben dürfen.

Nachzulesen unter:

https://www.finews.ch/news/banken/35925-n26-super-gau-und-mieser-service
https://www.handelszeitung.ch/unternehmen/betruger-plundern-konten-von-schweizer-revolut-kunden
https://www.moneytoday.ch/news/vom-revolut-hack-der-keiner-war-und-von-phishing-attacken-die-alle-treffen-koennen
https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019
https://www.trojaner-info.de/mobile-security/aktuell/bankkonto-gepluendert-trotz-zwei-faktor-authentifizierung.html
https://www.zeit.de/digital/2019-09/sim-swapping-technologie-hacking-soziale-medien-datenschutz
https://www.tweakpc.de/news/45034/facebook-419-millionen-telefonnummern-unverschluesselt-im-internet-aufgeta

II. Fertig Pause: Emotet schlägt wieder massiv zu

Im ersten Security-Report dieses Jahres hatten wir ausführlich über die massiven Schäden und Bedrohungen berichtet, die der Multifunktionstrojaner Emotet, auch bekannt als Heodo, in Unternehmens- und anderen Netzwerken angerichtet hatte. Nach einer längeren Sommerpause meldete sich die Emotet-Gruppe Anfang Oktober mit massiven Angriffen zurück, die in Deutschland bereits wieder zu ernsthaften Schäden in Unternehmen, Verwaltungen und Organisationen geführt haben. So wurde unter anderem das Berliner Kammergericht am 2.Oktober Opfer eines Emotet-Angriffs.

Aktuell schicken die Cyberkriminellen gut gemachte, personalisierte Spam-Mails mit Namen und E-Mail-Adressen exponierter Mitarbeitender einer Organisation (zumeist Mitglieder der Geschäftsleitung) an Mitarbeitende dieser Organisation. Die angehängten infizierten Word-Dokumente laden über ein Makro Emotet auf den Windows Rechner des Mail-Empfängers.

In der ersten grossen Angriffswelle zum Jahresanfang kundschaftete Emotet in einem zweiten Schritt das gesamte Netzwerk aus und lud dann TrickBot nach, um unter anderem Zugangsdaten zu Konten abzuphischen, anhand welcher die Hacker abschätzten, welches Lösegeld für ihre Opfer gerade noch zahlbar wäre. Im nächsten Schritt lud TrickBot dann «Ryuk» nach – einen Erpressungstrojaner, der sich dank seiner integrierten Wurm-Komponente durch das komplette Netzwerk frass und alle Daten verschlüsselte. Für die

Freigabe wurden von den Cyberkriminellen seinerzeit Lösegelder von 200.000 Franken und mehr verlangt.

Inzwischen scheinen die Cybergangster hinter Emotet ihr Geschäftsmodell in zwei Dimensionen erweitert zu haben: Zum einen greifen sie offenbar auch vermehrt Privatpersonen an. Und zum anderen verkaufen sie den Zugang zu den mit Emotet infizierten Rechnern, nicht mehr nur an die TrickBot/Ryuk-Kriminellen, sondern auch an andere cyberkriminelle Gruppen. So berichtet Heise online, dass in Deutschland durch das "Emotet-Gate" Malware für den Online-Banking-Betrug nachgeladen wurde.

Die bereits am Jahresanfang publizierten Warnungen der Melde- und Analysestelle Informationssicherung des Bundes MELANI und des deutschen Bundesamts für Sicherheit in der Informationstechnik BSI (die beiden letzten Links unten) haben deshalb nichts von ihrer Aktualität verloren. Zudem findet sich unter dem Link zur Allianz für Cybersicherheit eine ausführliche Liste von Massnahmen zum Schutz vor Cybercrime im Allgemeinen und vor Emotet im Besonderen. Zudem sind auch die Hinweise darauf sehr nützlich, was Organisationen tun sollten, wenn sie feststellen, dass ihr Netzwerk bereits infiziert ist. Zwar sind sie für Organisationen konzipiert, die in Deutschland domiziliert sind, doch können sie im Ernstfall auch Schweizer Betroffenen wichtige Orientierungen geben (anstelle des BSI ist in der Schweiz MELANI erste Ansprechstelle).

Nachzulesen unter:

https://www.switch.ch/export/sites/default/security/.galleries/files/SWITCH-Security_Report_2019-1_de.pdf
https://www.faz.net/aktuell/wirtschaft/diginomics/schadsoftware-legt-berliner-kammergericht-lahm-16413935.html
https://www.heise.de/security/meldung/Trojaner-Alarm-BSI-warnt-vor-zunehmenden-Emotet-Angriffen-4537594.html
https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner-Emotet-greift-Unternehmensnetzwerke-an.html
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html

III. Hacker löchern Apfel bis zum Kern – und spionieren zwei Jahre lang iOS-Geräte aus

Mehr als zwei Jahre lang hatte eine bislang unbekannte Hackergruppe mehr oder weniger unbeschränkten Zugriff auf infizierte iPhones und iPads unter iOS 10 bis 12. Nachdem Googles Sicherheitsforscher im Project Zero Apple am 1. Februar 2019 entdeckt hatten, dass sich Cyberkriminelle 14 Sicherheitslücken in iOS zunutze gemacht hatten, informierten sie den Hersteller aus Cupertino, der sieben Tage später mit dem Update auf iOS 12.1.4. alle entdeckten Lücken schloss.

Gravierend ist der Vorfall deshalb, weil sich die Hacker unter Ausnutzung aller Lücken bis zum Kernel, also zur Basis des Systems, "durchfressen" konnten. Dazu infizierten sie gehackte oder gefakte Websites mit Spyware, die sich bereits beim ersten Besuch auf die Geräte lud. Auf den infizierten Geräten durchlöcherten fünf ebenso komplette wie

einzigartige sogenannte Exploit-Ketten eine Sicherheitsschicht nach der anderen (zur Erklärung: in einer Exploit-Kette nutzen verschiedene Schadprogramme eine Sicherheitslücke, tarnen nach der ersten Infektion eines Gerätes ihre und die Existenz gegebenenfalls nachgeladener Programme und umgehen die Sicherheitsmaßnahmen, die eine Ausbreitung verhindern sollen). Weder die Schutzmechanismen des Browsers noch die des Betriebssystems iOS konnten dieser Angriffswelle standhalten.

Aus den derart infizierten Geräten konnten die Hacker zum Beispiel komplette Chats via Messenger-Dienste wie WhatsApp oder Apples iMessages auslesen. Dazu leitete die Spyware E-Mails, Kontaktlisten, Fotos und sogar den GPS-Standort des Geräts auf die Server der Hacker. Ebenfalls nicht verschont blieb Apples Schlüsselbund, mit dem Apple-User Kennwörter und andere sensible Informationen, wie z.B. Passwörter oder kryptografische Zertifikate speichern und verwalten. Auch sie waren einsehbar.

Wer die Angriffe und die dann folgende Spionageaktion durchgeführt hat, wollten oder konnten die Google-Security-Experten nicht sagen. Allerdings kursieren Gerüchte, die aus der Tatsache folgern, dass die Angreifer sich für auffallend viele Apps interessierten, die in China weit verbreitet sind. Daraus liesse sich ableiten, dass mit der Aktion gezielt Dissidenten und chinesische Minderheiten ausspioniert wurden.

Nachzulesen unter:

https://www.pctipp.ch/news/software/artikel/hacker-nutzen-kritische-sicherheitsluecke-in-ios-ueber-jahre-hinweg-92785
https://www.computerworld.ch/security/apple/ios-geraete-liessen-jahrelang-drive-by-attacken-hacken-1751743.html
https://www.sueddeutsche.de/digital/sicherheitsluecke-apple-iphone-ipad-1.4582499
https://www.spiegel.de/netzwelt/gadgets/google-deckt-riesige-iphone-hackerkampagne-auf-a-1284403.html
https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

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