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

Mai/Juni 2020

I. Der einen Viren Leid, der anderen Viren Freud´ – Wie steht es um die IT-Sicherheit beim kontaktlosen Bezahlen?

Kontaktloses Bezahlen geht schnell, einfach und hygienisch – ist es aber auch sicher? Bereits Mitte 2019 vermeldete die Schweizer Nationalbank, dass ca. jede zweite Zahlung mit einer kontaktlosen Debit- oder Kreditkarte getätigt würde. Diese Zahlen dürften sich in der Coronakrise und mit der Verdoppelung der Zahlungslimite Anfangs April von 40 auf 80 Franken pro Zahlungsvorgang nochmals deutlich erhöht haben. Denn Zahlen mit einer NFC (Near Field Comunication)- oder RFID (Radio Frequency Identification)-fähigen Karte funktioniert ohne Bargeld, ohne Berührung, ohne Unterschrift, ohne PIN-Eingabe – summa summarum also ohne potenzielle Virenträger. Grund genug, die Frage zu stellen, wie es um die IT-Sicherheit beim kontaktlosen Bezahlen bestellt ist.

In einem 2019 von SRF-"Kassensturz" durchgeführten Experiment versuchten Hacker, sich Zugriff auf die Daten von Karten der Passanten in einem Einkaufszentrum zu verschaffen, die diese in ihrer Tasche hatten. Beruhigend: lediglich in einem von zehn Fällen war der Versuch im Sinne der Angreifer erfolgreich – und der fand unter Idealbedingungen statt.

So wussten die Angreifer zum Beispiel, wo sich die Karte in der Tasche des Opfers befand. Während es ihnen hier gelang, 38 Franken von der Karte ab- und ihrem Konto aufzubuchen, scheiterten sie in allen anderen neun Fällen.

Ein Jahr zuvor hatte c´t-Redaktor Jan-Keno Janssen auf die potenzielle Gefahr des Abfischens der Limitbeträge von kontaktlosen Karten hingewiesen und gezeigt, wie man sich am besten davor schützen kann. Unter anderem hatte er dazu geraten, die Kontaktlos-Karte mit anderen RFID-fähigen Karten im Geldbeutel aufzubewahren. Dann nämlich erfährt das Lesegerät einen sog. Clash, weil es nicht weiss, welche Karte nun belastet werden soll. Zudem hatte Janssen postuliert, dass mobile Bezahldienste wie ApplePay, GooglePay, SwatchPay oder TWINT nochmals sicherer wären als Kontaktlos-Karten, weil jede Abbuchung im «Mobile-Payment» immer eine Bestätigung am Mobilgerat voraussetzt.

Nachzulesen unter:

https://www.srf.ch/news/schweiz/sicherheit-von-bankkarten-hacking-experiment-geld-von-kontaktlos-karte-abgebucht
https://www.heise.de/ct/artikel/So-leicht-laesst-sich-Geld-beim-kontaktlosen-Bezahlen-abfischen-4116033.html
https://www.focus.de/finanzen/banken/kreditkarten/mit-kreditkarte-und-smartphone-so-funktioniert-kontaktloses-bezahlen-im-vorbeigehen_id_5421495.html

II. You´ve got Mail(ware) – Gravierende Sicherheitslücke in Apples Mail App auf iPads und iPhones inzwischen geschlossen

Mitte April schreckte das amerikanische Security-Unternehmen ZecOps Apple-User in Europa mit der Meldung auf, dass Hacker durch eine aus drei Schwachstellen bestehende Sicherheitslücke in Apples Mail App bereits seit Version iOS 6 unbemerkt und extrem einfach Malware auf Tablets und Telefone mit dem Apfel-Logo bringen konnten – und von dieser Einladung offenbar auch Gebrauch gemacht hätten. Das Dementi der Konzernzentrale in Cupertino, wonach man keine Beweise für Angriffe via dieser Lücken habe finden können, kam ebenso umgehend wie die Einschätzung, dass die drei Schwachstellen kein unmittelbares Risiko für Nutzer bedeuteten, weil sie nicht ausreichen würden, die Sicherheit von iPads und iPhones zu umgehen.

Im Gegensatz dazu bewertete das deutsche Bundesamt für Sicherheit in der Informationstechnik BSI die gefundene Sicherheitslücke als "besonders kritisch", weil dadurch Malware mit einer präparierten Email und ohne jede weitere Interaktion der Nutzer aufgespielt werden konnte. Das BSI warnte daraufhin vor dem weiteren Benutzen der App und empfahl, solange auf ein alternatives Programm auszuweichen, bis die Lücke geschlossen sei.

Dies hätte bereits mit den Betaversionen von iOS 13.5 und 12.4.7 geschehen sollen, doch waren die Patches nach Apple-Angaben noch nicht vollständig gewesen. Erst mit dem Update auf die für die Allgemeinheit freigegebenen Versionen 13.5 bzw. 12.4.7 seien alle drei gefundenen Lücken definitiv geschlossen. Das bestätigte auch das BSI und gab am 27. Mai offizielle Entwarnung.

Nachzulesen unter:

https://www.n-tv.de/technik/Apples-Mail-App-hat-eine-gefaehrliche-Luecke-article21735601.html
https://www.heise.de/mac-and-i/meldung/Mail-Bugs-BSI-warnt-vor-iOS-4708945.html
https://www.heise.de/mac-and-i/meldung/Apple-Mail-iOS-Updates-beseitigen-offenbar-schwere-Luecke-4764378.html

III. Alles muss raus – Die "Shade"-Hacker geben nach "Geschäftsaufgabe" hunderttausende von Dechiffrierschlüsseln ab

Wenn physisch präsente Unternehmen ihr Geschäft schliessen, räumen sie im Normalfall Laden und Lager und geben dann die Schlüssel ab. Wenn Hacker, die im Geschäft mit Ransomware zur virtuellen Erpressung tätig waren, dies tun, haben sie Schlüssel der ganz anderen Art abzugeben: Decryption-Keys. Mit ihnen lassen sich jene Daten aus der Geiselhaft befreien, in die sie die Schadsoftware der Hacker genommen hatte. Einziger und meist sehr folgenschwerer Fehler in dieser Analogie: die meisten Cybererpresser geben die Schlüssel eben nicht ab und hinterlassen ihren Opfern nicht mehr nutzbare Daten und Systeme – mit allen, teilweise schwersten Konsequenzen.

Eher selten ist der Fall jener russischen Hackergruppe, die ihren Rückzug aus dem aktiven Geschäft mit einem als "Shade", "Troldesh" oder "Encoder" bekannten Erpressungstrojaner nicht nur offiziell bekanntgab, sondern sich zum einen auch bei allen Opfern entschuldigte und zum anderen neben Entschlüsselungssoftware und einer Anleitung zur Dechiffrierung der kompromittierten Systeme auch noch ca. 750.000 (!) Dechiffrierschlüssel veröffentlichte.

Die Ransomware «Shade» war seit 2014 vor allem in Russland und der Ukraine im Umlauf. Was die «Shade»-Hacker dazu bewogen hat, ihr schändliches und kriminelles Geschäft aufzugeben und öffentlich Busse zu tun, ist indes nicht bekannt.

Nachzulesen unter:

https://www.computerworld.ch/security/ransomware/hackergruppe-veroeffentlicht-schluessel-2532172.html
https://www.heise.de/security/meldung/I-f-Reue-nach-Ransomware-Attacken-Shade-Gang-stellt-Decryption-Keys-online-4711400.html

IV. Schweizer User im Visier von Cyberkriminellen

Meier Tobler, Swiss Windows, Stadler Rail – die Namen der seit 2019 angegriffenen und um Millionenbeträge geschädigten Schweizer Unternehmen liest sich wie das Who is Who erfolgreicher Unternehmen der Alpenrepublik. Dem kurzen Aufatmen über die reuige Geschäftsaufgabe der "Shade"-Hacker steht also die weit drastischere Erkenntnis entgegen, dass Schweizer Unternehmen immer stärker ins Visier extrem gefährlicher Hacker geraten, die nicht nur in Russland zu finden sind.

Neben den Unternehmen stehen aber auch Frau und Herr Schweizer auf der Zielliste internationaler Cybergangs. So war im April dieses Jahres eine polnische Kriminellen-Gang namens «InfinityBlack» aufgeflogen, die LogIn-Daten zu Schweizer Treueprogrammen nutzten, um z.B. Cumulus-Punkte abzufischen und gegen Cryptowährung an andere kriminelle Organisationen weiterzuverkaufen. Die hatten die Punkte dann in den Läden meist gegen teure Elektronik-Geräte eingelöst. Ende April konnte die polnische Polizei nach gemeinsamen Ermittlungen mit Europol und Schweizer Polizeibehörden an verschiedenen Orten fünf Verdächtige festnehmen.

Nicht direkt auf Schweizerinnen und Schweizer gerichtet war der Grossangriff, den laut amerikanischen Geheimdiensten in China zu suchende Hacker auf die Billigfluglinie Easyjet Mitte Mai verübt hatten. Gleichwohl dürften sich unter den erbeuteten 9 Millionen Kundenkonten auch die von Eidgenossen befinden. Gute Nachricht im schlechten Umfeld: Laut Easyjet seien die Passwörter aller 9 Millionen gehackter Konten nicht kompromittiert, auch wenn das Unternehmen eingestehen musste, dass im Zuge des Hacks bei ca. 2200 Konten die Kreditkartendaten abgegriffen worden seien.

Nachzulesen unter:

https://www.nzz.ch/wirtschaft/schweizer-firmen-vermehrt-mit-verschluesselungs-trojanern-attackiert-ld.1499064
https://www.computerworld.ch/security/hacking/cyberangriff-kostet-meier-tobler-millionen-1747538.html
https://www.tagblatt.ch/wirtschaft/bankrott-auch-mit-cyberangriff-begruendet-wurde-moerschwiler-swisswindows-in-den-ruin-gehackt-ld.1198956
https://www.nzz.ch/wirtschaft/hacker-stellen-stadler-rail-ein-ultimatum-ld.1558845
https://www.tagesanzeiger.ch/hacker-pluendern-schweizer-cumulus-kunden-686857470648
https://www.netzwelt.de/news/178548-easyjet-gehackt-hacker-stehlen-9-millionen-kunden-kreditkartendaten.html

V. Elite Targets Hack – (nicht nur) die ETH-Supercomputer Euler und Leonhard wurden gehackt

Ebenfalls Mitte Mai wurden zwei weitere Schweizer Vorzeige-Promis Opfer einer Cyberattacke: Euler und Leonhard – die beiden Supercomputer der ETH Zürich. Von der offenbar gross angelegten und sehr gezielten Angriffswelle gegen Schweizer und

europäische Hoch- und Höchstleistungsrechner wurden auch die Supercomputer des Centro Svizzero di Calcolo Scientifico CSCS in Lugano sowie die der GAUSS-Allianz in Stuttgart, Jülich und Garching erfasst. Betroffen waren mindestens sechs weitere Höchst- und Hochleistungsrechenzentren in Deutschland und die High Performance Rechner aller Mitglieder des Netzwerks Partnership for Advanced Computing in Europe (PRACE).

Ziel war jedes Mal jener Teil des Systems, der die LogIn-Daten und den Benutzerzugriff verwaltet. Nach bisher vorliegenden Informationen des Leibniz Rechenzentrums in Garching bei München (LRZ) kombinierten die Angreifer zwei Schwachstellen und "bedienten … sich kompromittierter Nutzer-Accounts auf externen Systemen, deren private SSH-Schlüssel mit einer leeren Passphrase konfiguriert waren". Zum anderen nutzten sie, so das LRZ, "einen Fehler in der Software, der nach regulärem Login zur Erlangung von Administrationsrechten genutzt werden kann."

Zum Schutz der Daten haben alle Betreiber die Rechner nach Bekanntwerden des Angriffs vom Netz genommen und fahren diese unter extremen Sicherheitsvorkehrungen vorerst nur in einem eingeschränkten Betrieb wieder hoch. Zudem haben die meisten ihre Benutzer aufgefordert, neue Passwörter und Secure-Shell-Keys anzulegen, "wobei unbedingt darauf zu achten ist, dass dem privaten Schlüssel auf dem Rechner, von dem aus der Login erfolgt, keine leere Passphrase zugeordnet werden darf!", so die Aufforderung des LRZ. Außerdem müssten alle Nutzer der LRZ Cluster-Systeme "in ihre ~/.ssh/authorized_keys Datei schlüsselspezifische "from" Klauseln einfügen, um den Zugriff auf die tatsächlich benötigten externen Systeme einzuschränken." Diese Einschränkungen würden bedauerlicherweise so lange in Kraft bleiben müssen, bis der Fall vollständig aufgeklärt sei.

Über die Ziele der Angreifer gibt es bislang nur Spekulationen, die sich um das Erbeuten von Forschungsdaten im Rennen um einen Impfstoff gegen Covid19, drehen. Sie sind aber bislang von keiner offiziellen Stelle kommentiert, dementiert oder bestätigt worden. In Deutschland ermitteln mehrere Landeskriminalämter, um den Tätern und ihren Motiven auf die Spur zu kommen.

Nachzulesen unter:

https://www.tagesanzeiger.ch/eth-supercomputer-gehackt-370887112689
https://www.forschung-und-lehre.de/politik/cyberangriffe-auf-mehrere-supercomputer-2784
https://www.heise.de/security/meldung/Mehrere-Hochleistungsrechenzentren-in-Europa-angegriffen-4721393.html
https://www.tagesanzeiger.ch/hacker-pluendern-schweizer-cumulus-kunden-686857470648
https://www.heise.de/news/Nach-Angriff-auf-HPC-Systeme-Supercomputing-nur-zu-Geschaeftszeiten-4770267.html

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

Der SWITCH Security Report greift aktuelle Themen aus dem Bereich der Cybersecurity auf und wendet sich an interessierte Internetnutzerinnen und -nutzer, um sie für die aktuellen Gefahren zu sensibilisieren. Eine Haftung für die Richtigkeit kann trotz sorgfältiger Prüfung nicht übernommen werden.