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

Mai / Juni 2018

SWITCH

I. Microsoft ruft Dich niemals an: Support-Scam nimmt weiter zu

Sie sind keineswegs neu, aber sie werden immer ausgefeilter, immer teurer und immer mehr. Die Rede ist von Anrufen, bei denen sich meist Englisch-sprechende Personen als Mitarbeitende von Microsoft oder anderen bekannten IKT-Unternehmen ausgeben. Unter verschiedenen Vorwänden, zum Beispiel, dass das System der Angerufenen eine Fehlermeldung übermittelt habe oder es Probleme mit der Lizenzvereinbarung gäbe, teilen sie den Betroffenen mit, dass aus Sicherheitsgründen ihre Microsoft-Lizenz gesperrt werden müsse. Um dies zu vermeiden, bieten die Abzocker den Betroffenen an, den Computer sofort per Fernzugriff zu reparieren oder aber ein Support-Abo bzw. eine Garantie abzuschliessen. Um ihren Argumenten Nachdruck zu verleihen, bitten sie ihre Opfer, Microsofts Supporttool «Event Viewer» zu öffnen. Dieses Programm listet tatsächlich in den meisten Fällen Fehlermeldungen auf. Den Telefon-Phishern liefert diese Liste von banalen und harmlosen Fehlermeldungen Argumente, Kreditkartendaten oder eine Zahlung in anderer Form (z.B. in iTunes-Karten) abzuzocken.

Noch weiter gehen die Betrüger mit der Fernzugriffsvariante. Hier werden die Angerufenen zum Download eines Fernwartungsprogramms aufgefordert, das den Kriminellen unbeschränkten Zugriff auf das System gewährt – Backdoor für spätere illegale Aktivitäten oder Nutzung als Bot inbegriffen. Obwohl Microsoft selbst, aber auch Polizei und öffentliche Stellen wie MELANI immer wieder vor diesen Anrufen

warnen, nehmen sie seit Jahren sowohl an Häufigkeit als auch an Dreistigkeit und Folgenschwere zu.

Die ersten Anrufe meldete heise.de bereits 2016. Schon damals stellte Microsoft klipp und klar fest, dass das Unternehmen keinerlei unaufgeforderten Anrufe tätige, um technischen Support anzubieten. 2017 warnte der Software-Gigant auf der firmeneigenen Newsseite erneut vor «Tech Support Scam» und veröffentlichte Ergebnisse einer Studie der Microsoft Digital Crime Unit, derzufolge weltweit jeder Dritte Befragte schon einmal angerufen worden sei. Im März 2018 gab das Internet Crime Complaint Center (IC3) bekannt, dass die gefakten Anrufe Schäden in Höhe von annähernd 15 Millionen Dollar verursachten. Während die meisten Opfer Verluste von 200 bis 400 Dollar beklagten, sind auch Einzelfälle bekannt, in denen die Betrüger mit den gephishten Zugangsdaten eines Angerufenen dessen Konto um mehr als umgerechnet 100.000 Schweizer Franken erleichterten.

Aktuell wird der betrügerische Security- oder Tech-Support nicht nur telefonisch, sondern auch via E-Mail und Malvertising angeboten. IC3 hat unter dem nachstehend angegebenen Link eine Liste mit Schutzmassnahmen veröffentlicht. Die drei wichtigsten Tipps: 1. Seriöse Firmen machen in keinem Fall Support-Angebote per Telefonakquise. 2. Es ist wichtig, sich nicht unter Druck setzen lassen, schnell (und unüberlegt) zu handeln. 3. In keinem Fall darf Unbekannten Zugang zu den eigenen Systemen oder Konto- bzw. Kreditkartendaten gegeben werden.

Nachzulesen unter:

https://www.luzernerzeitung.ch/zentralschweiz/nidwalden/buochs-microsoft-masche-40-jaehrige-faellt-auf-cyberbetrug-herein-ld.43021

https://www.melani.admin.ch/melani/de/home/themen/fake_support.html

https://www.heise.de/ct/ausgabe/2016-23-Falsche-Microsoft-Support-Anrufe-3359912.html

https://news.microsoft.com/de-de/microsoft-anrufe-scam

https://gizmodo.com/microsoft-warns-that-tech-support-scams-are-still-on-th-1825502696

https://www.zdnet.com/article/windows-warning-tech-support-scammers-are-ramping-up-attacks-says-microsoft

https://www.ic3.gov/media/2018/180328.aspx

II. «Efail» zwischen Hype und Desaster: Security muss kommunizieren lernen

Der Schaden ist angerichtet. Betroffen sind Nutzer, Security- und Softwarefirmen, IT-Entwickler und Security-Forscher. Alles begann mit einer Sicherheitslücke, die die Forscher Damian Poddebniak, Christian Dresen, Jens Müller, Fabian Ising, Sebastian Schinzel, Simon Friedberger, Juraj Somorovsky und Jörg Schwenk im Oktober 2017 entdeckt und auf den einprägsamen Namen «Efail» getauft hatten. «Efail» eröffnet die Möglichkeit, dass Punkt-zu-Punkt-verschlüsselte und bis dato als sicher geltende E-

Mails in Klartext gelesen werden können, wenn E-Mails mit Programmen auf Basis der ebenfalls bis dato als äusserst sicher und zuverlässig geltenden Protokolle «OpenPGP» und «S/MIME» verschlüsselt werden. Die Electronic Frontier Foundation (EFF) entschloss sich daraufhin, Informationen über die Lücke gemeinsam mit der Empfehlung zu veröffentlichen, Mails künftig nur noch unverschlüsselt zu senden. Unklar ist, warum die EFF diese Meldung ausserdem auch früher herausgab, als dies in Fachgremien und mit anderen Forschern und Entwicklern abgesprochen war. Aber genau das hat die zweite, vielleicht sogar schwerwiegendere Schadenswelle ausgelöst. Denn nun griffen Medien das Thema auf und kreierten mit der weitgehend unreflektierten Übernahme der EFF-Empfehlungen einen «Efail-Hype».
In der Folge fühlten sich betroffene Entwickler von der EFF überrumpelt, die «Efail»-Forschergruppe war nicht auf Krisenkommunikation vorbereitet und die Befolgung der EFF-Empfehlung, «PGP»- oder «S/MIME»-basierte Programme nicht mehr zu nutzen, eröffnete völlig neue Sicherheitsrisiken. Heise online-Autor Fabian A. Herschel bringt das Hauptproblem auf den Punkt: „Die Entwickler von PGP- und S/MIME-Programmen werden wahrscheinlich Jahre damit verbringen müssen, dieses Image-Desaster zu reparieren. Wenn das überhaupt möglich ist."

Nachzulesen unter:

https://de.wikipedia.org/wiki/Efail
https://efail.de
https://thehackernews.com/2018/05/efail-pgp-email-encryption.html
https://www.wired.com/story/efail-encrypted-email-flaw-pgp-smime
https://www.heise.de/newsticker/meldung/Efail-Was-Sie-jetzt-beachten-muessen-um-sicher-E-Mails-zu-verschicken-4048988.html
https://www.heise.de/security/meldung/Efail-Welche-E-Mail-Clients-sind-wie-sicher-4053873.html
https://www.heise.de/newsticker/meldung/Kommentar-Efail-ist-ein-EFFail-4050153.html
https://blog.cryptographyengineering.com/2018/05/17/was-the-efail-disclosure-horribly-screwed-up
https://searchsecurity.techtarget.com/news/252441216/Efail-disclosure-troubles-highlight-branded-vulnerability-issues

III. Angriffsvektor Schallwelle, aktuelle Fälle lassen aufhorchen

Der von Snowden aufgedeckte Überwachungsskandal scheint vergessen. Die ehemals empörte Öffentlichkeit zahlt neuerdings freiwillig viel Geld dafür, dass digitale Assistenzsysteme ihre Nachrichten verschicken, Einkaufsprofile anlegen oder ihre Gespräche aufzeichnen. Alexa, Siri, Cortana, O.K. Google und Watson hören aber nicht nur zu, sondern teilen im Extremfall auch anderen mit, was sie da so zu hören bekommen. So geschehen in Oregon. Ende Mai berichtete die Nachrichtenagentur Bloomberg darüber, dass ein Amazon-Echo-Lautsprecher das private Gespräch eines Ehepaars aufgezeichnet und an einen Bekannten geschickt hatte.

Amazons Erklärung für Alexas Fehlverhalten mag tatsächlich zutreffend sein, klingt aber dennoch unglaublich. In der im unten zitierten arstechnica-Beitrag nachzulesenden Erklärung heisst es, dass Alexa und ihre digitalen Kolleginnen und Kollegen bei situativ geminderter Hörfähigkeit Gesagtes eigenständig interpretieren und entsprechend handeln. Jedoch haben sprachgesteuerte Assistenzsysteme erwiesenermassen ein sehr gutes Gehör. Bereits 2016 bewiesen Studenten aus Berkeley und der Georgetown University, dass sie mit sogenannten Dolphin Attacken sprachgesteuerte AI-Systeme übernehmen und steuern können. Dabei werden in Musik, Videos oder Streaming-Dateien für das menschliche Ohr nicht wahrnehmbare hochfrequente Töne eingebettet, die im System als Befehl interpretiert und von diesem entsprechend ausgeführt werden. Dabei müssen Manipulationsszenarien nicht immer böse Absichten verfolgen oder ausgefeilte Technologien einsetzen, um Sprachsysteme für ihre eigenen Zwecke zu nutzen. Burger King verschickte einen Sprachbefehl an von «O.K. Google» sprachgesteuerte Android-Devices, um diese dazu zu bringen, die Wikipedia-Seite über den «Whopper» zu öffnen. Und die Macher von South Park gestalteten eine komplette Episode mit Sprachbefehlen, die den zuhörenden Assistenzsystemen diverse Obszönitäten entlocken konnten.

Dass Schall in der ICT-Welt grosse Schäden anrichten kann, erkannte bereits 2008 ein SUN-Microsystems-Mitarbeiter. Er hatte entdeckt, dass die I/O-Latenz seiner Festplatten immer dann anstieg, wenn er das Disk-Rack anbrüllte. Ende 2016 berichtete motherboard.vice.com, dass während einer Brandschutzübung Löschgase mit lautem Geräusch freigesetzt worden waren und die Schallwelle Dutzende Festplatten im Hauptrechenzentrum der ING Bank in Bukarest zerstört hatte. Dies hat sich Ende April in Schweden in ähnlicher Form wiederholt, wo der Klang austretenden Löschgases zahlreiche Festplatten in Servern von Nasdaq Nordic und zweier skandinavischer Banken zerstört und für den stundenlangen Ausfall des Börsenhandels in mehreren skandinavischen und baltischen Staaten gesorgt hatte.

Letztlich darf aber bei aller Kritik an sprachgesteuerten AI-Systemen nicht vergessen werden, dass sie die Lebensqualität vieler Menschen, die sich aufgrund von Beeinträchtigungen oder Unfällen allein auf verbale Kommunikation stützen, verbessern. Der Sydney Morning Herald berichtet die Geschichte eines verunfallten und schwer verletzten, bewegungsunfähigen Motorradfahrer, der nur deswegen rechtzeitig gerettet werden konnte, weil er mit verbalen Befehlen via Siri den Notruf alarmieren konnte.

Nachzulesen unter:

https://www.bloomberg.com/news/articles/2018-05-25/amazon-s-alexa-snafu-should-be-a-turning-point-for-tech

http://www.handelsblatt.com/technik/gadgets/amazon-echo-amazons-digitaler-assistent-verschickt-heimlich-privatgespraech/22602528.html?ticket=ST-4540107-l9pyLGcf2bsSOp2GvFAr-ap3

https://arstechnica.com/gadgets/2018/05/amazon-confirms-that-echo-device-secretly-shared-users-private-audio/

https://netzpolitik.org/2018/amazon-echo-alexa-sendet-privatgespraech-heimlich-an-arbeitskollegen
https://futurezone.at/digital-life/in-musik-versteckte-befehle-lassen-alexa-und-co-einkaeufe-taetigen/400033990
https://www.cnbc.com/2018/05/10/new-york-times-digital-alexa-and-siri-can-hear-this-hidden-command-you-canat.html
https://arstechnica.com/information-technology/2018/05/attackers-can-send-sounds-to-ddos-video-recorders-and-pcs
https://windowsunited.de/dolphinattack-sicherheitsloch-sprachsteuerung
https://www.heise.de/newsticker/meldung/Loeschanlagen-Ton-zerstoert-Festplatten-in-schwedischem-Rechenzentrum-4029730.html
https://motherboard.vice.com/de/article/qvjb7w/ungewoehnlicher-vorfall-beweist-geraeusche-koennen-festplatten-zerstoeren
https://www.smh.com.au/national/nsw/teen-uses-siri-to-call-triple-zero-after-after-bike-crash-in-bush-20180525-p4zhen.html

IV. Waterholing-Attacken: Infrastruktur ist und bleibt Angriffsziel

Netcom BW, ein regionaler Internet-Anbieter und Tochterunternehmen des deutschen Energieversorgers EnBW, war Ziel einer Waterholing-Attacke. Die Sache ging glimpflich aus und der Energieversorger kam ohne Schaden davon, denn der Angriff wurde in einem frühen Stadium entdeckt. Waterholing-Attacken sind aufwändig, brauchen Geduld und gute Vorbereitung. Vergleichbar mit Grosskatzen, die an Wasserlöchern auf durstige Beutetiere warten, warten die Hacker hinter den Websites auf den Besuch ihrer Opfer, um ihre Geräte mit Schadsoftware zu infizieren und auf diese Weise weiter ins System des angegriffenen Unternehmens vorzudringen. Ermittler schreiben die EnBW-Attacke russischen Hackern zu welche der Regierung nahestehen. Denn das Angriffsmuster passt zu einem Hack, bei dem der Stromversorgung der Ukraine im Dezember 2015 schwerer Schaden zugefügt worden war. Auch der schwere Hackerangriff auf den deutschen Bundestag war nach neustem Ermittlungsstand als Waterholing-Attacke von russischen Hackern geführt worden.

Nachzulesen unter:

https://www.heise.de/newsticker/meldung/EnBW-Tochter-war-2017-Ziel-von-Cyberangriff-Erfolgreich-abgewehrt-4050711.html
http://www.handelsblatt.com/wirtschaft-handel-und-finanzen-roundup-enbw-tochter-war-2017-ziel-von-cyberangriff-erfolgreich-abgewehrt/22573752.html?ticket=ST-4689874-ceC6NRgxtrnfrSPl1seN-ap3
https://www.inside-it.ch/articles/51112
http://www.sueddeutsche.de/digital/enbw-tochter-hacker-haben-deutschen-energieversorger-angegriffen-1.3980625
http://www.sueddeutsche.de/digital/computerviren-angriff-liebesgruss-der-schlange-1.3987245

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