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

März/April 2019

I. Lenin und die Detektive: Mobiispy-Stalkerware macht auch intime Daten überwachter Kinder und Partner öffentlich verfügbar

Wladimir Iljitsch Lenin wird der Satz zugesprochen, dass Vertrauen zwar gut, Kontrolle aber besser sei. Daher gäbe der russische Bolschewikenführer und Revolutionär an und für sich ein gutes Testimonial für Anbieter von Stalkerware ab. Unter diesem Sammelbegriff finden sich erstaunlich viele Programme und Apps, die von Helikoptereltern oder eifersüchtigen Menschen auf den Smartphones ihrer Kinder bzw. Partner installiert werden. Ihre Anbieter wenden sich zumeist an besorgte Eltern, die mithilfe der Software Anrufe mithören, Textnachrichten mitlesen, die Kontaktliste oder aufgenommene Fotos und Videos anschauen oder auslesen, kurz: nahezu alles ausspionieren können, was die Überwachten mit ihrem Smartphone tun. Idealerweise sollten Überwachende die Überwachten informieren und die Software nur nach deren Zustimmung installieren. In Wirklichkeit geschieht zumeist eher das Gegenteil. Und das hat dumme Folgen, die den ursprünglichen Absichten von Eltern und Liebenden konträr gegenüberstehen.

Denn wie die Tech-Info-Plattform motherboard.com Ende März berichtete, hat der Sicherheitsforscher Troy Hunt herausgefunden, dass Mobiispy.com, einer der erstaunlich zahlreichen Stalkerware-Anbieter, 16 Gigabytes an Bildern und 3,7 GB an MP-3-

Aufnahmen in einer unverschlüsselten Cloud-Datenbank gespeichert hat, die via Internet allen Usern frei zugänglich war. Weil unter den ca. 95.000 Bildern und 25.000 Audio-Dateien auch intime Fotos und Gespräche von Minderjährigen gewesen sind, hatte Motherboard zunächst den Anbieter nicht benannt, um seinerseits bösen Absichten keinen Vorschub zu leisten. Nachdem Mobiispy aber auch auf wiederholte Hinweise Hunts und seitens Motherboards nicht reagiert hatte, informierte Motherboard den Internet-Registrar und den Hosting-Service von Mobiispy.com. Letzterer nahm dann Ende März (allerdings auch erst nach dem Motherboard-Bericht) die Website aus seiner Cloud.

Dass der einfache Zugang zu Daten, die von Stalkerware ausspioniert wurden, eher die Regel denn die Ausnahme ist, macht den Fall besonders besorgniserregend: Motherboard listet (neben dem aktuellen) zwölf Stalkerware-Anbieter auf, bei denen in den letzten zwei Jahren solche Daten gehackt oder schlicht ungeschützt online gestellt wurden.

Vielleicht muss Lenins Satz in digitalen Zeiten genau verkehrt herum gelesen werden: "Kontrolle verspricht viel, Vertrauen hält besser!"

Nachzulesen unter:

https://motherboard.vice.com/en_us/article/j573k3/spyware-data-leak-pictures-audio-recordings
https://motherboard.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy
https://futurezone.at/digital-life/ueberwachungs-app-stellt-ueber-95000-fotos-offen-ins-internet/400445902
https://t3n.de/news/datenleak-bei-stalkerware-fuer-eltern-und-eifersuechtige-95000-fotos-einsehbar-1152479/
https://motherboard.vice.com/en_us/topic/when-spies-come-home

II. Erpressungstrojaner LockerGoga legt Firmen lahm

Im Januar 2019 bezeichnete ein Sicherheitsforscher auf bleepingcomputer.com die Ransomware LockerGoga, mit der Cyberkriminelle das französische Technologieberatungsunternehmen Altran angegriffen hatten, als langsam, schlampig programmiert, uneffektiv in der Abwicklung der Lösegeldzahlung und offensichtlich nicht darum besorgt, entdeckt zu werden. Das hinderte LockerGoga aber seit Anfang des Jahres nicht daran, die IT-Systeme mehrerer grosser Industrieproduzenten lahmzulegen und grosse Schäden zu verursachen. Neben ungenannt bleiben wollenden Unternehmen gelang ihnen dies unter anderem bei den beiden fusionierten Spezialchemieherstellern Hexion und Momentive in Columbus, USA und Leuna, Deutschland. Spätestens aber mit dem – aus Sicht der Hacker – erfolgreichen Angriff auf den norwegischen Aluminium-Riesen Norsk Hydro sollte IT-Verantwortlichen und Security-Experten klar sein, dass sich LockerGoga wohl so etwas wie das Ransomware-Gegenstück zum zweiten Todesstern des StarWars-Imperiums ist: Sieht auf den ersten Blick aus, als würde nichts wirklich funktionieren, ist aber voll einsatzfähig und für die betroffenen Unternehmen schlichtweg katastrophal in seinen Auswirkungen. So musste Momentive Hunderte von Desktops und Tablets austauschen, und der finanzielle Schaden bei Norsk Hydro wird alleine für die erste

Woche nach der LockerGoga-Attacke auf ca. 40 Millionen Dollar geschätzt. Entsprechend der Marktbedeutung von Norsk Hydro schlug die Cyberattacke zudem auf den Aluminiumpreis durch, weil Rohstoffhändler einen Engpass befürchteten. Auch verlor Norsk Hydro kurzzeitig bis zu 3,4 Prozent ihres Börsenwerts und hatte auch eine Woche nach der Attacke in einem Geschäftsbereich erst wieder 70-80% des normalen Outputs erreicht, während ein anderer immer noch komplett stillstand.

Abzuwarten bleibt, ob die Cyberversicherung des norwegischen Alugiganten die Schäden deckt. 2017 machte der Lebensmittelkonzern Mondelez nach einem NotPetya-Angriff einen Schaden in Höhe von 100 Millionen Dollar geltend. Das Versicherungsunternehmen verweigert seither die Zahlung mit der Begründung, dass die Regierungen der USA, Gossbritanniens, Australiens und Kanadas NotPetya-Angriffe als Elemente des russischen Cyberkriegs gegen die Ukraine bezeichnet hatten, und der Vertrag eine Klausel enthalte, die eine Zahlung zur Kompensation kriegsbedingter Schäden ausschliesse. In der gleichen Angriffswelle musste der dänische Logistikkonzern Maersk einen Schaden in Höhe von 300 Millionen Dollar verbuchen. Inwieweit dieser von einer Cyberversicherung gedeckt ist, ist aktuell nicht bekannt. Sicher ist demnach nur, dass angesichts zunehmender Cyberangriffe auf kritische Infrastruktur und produzierende Unternehmen Awareness und sicherheitsbewusstes Verhalten aller Mitarbeitenden wichtiger sind denn je.

Nachzulesen unter:

https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/
https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers
https://www.databreachtoday.com/lockergoga-ransomware-suspected-in-two-more-attacks-a-12242
https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms
http://www.spiegel.de/netzwelt/netzpolitik/norsk-hydro-hackerangriff-war-eine-lockergoga-ransomware-attacke-a-1258627.html
https://www.hydro.com/en/media/news/2019/update-on-cyber-attack-march-26
https://www.zdnet.com/article/norsk-hydro-ransomware-incident-losses-reach-40-million-after-one-week

III. Klartext bei Facebook: Wenn Tech-Giganten noch nicht einmal minimale Sicherheitsanforderungen erfüllen

Jüngst sprach sich Facebook-Gründer und -Übervater Mark Zuckerberg in einem Gastbeitrag, der zeitgleich in der Frankfurter Allgemeinen Sonntagszeitung und der Washington Post veröffentlicht wurde, für neue, klare Regulierungen des Internets aus. Klartext? Bei Facebook? Aber sicher! Oder eben nicht.

Um die eventuell entstandene babylonische Sprachverwirrung sofort wieder zu beenden: Zuckerbergs Gastbeitrag wird inzwischen von vielen Branchenkennern und -begleitern nicht als Klartext gewertet, sodern als neue Nebelkerze, mit der von den Problemen des Netzwerk-Konzerns abgelenkt werden soll. Die bestehen aus Vorwürfen, dass Facebook weiterhin millionenfach Nutzungsdaten angemeldeter Kundinnen und

Kunden wie auch nicht angemeldeter User absaugt und zugunsten der eigenen Kasse monetarisiert, Hass- und Gewaltposts nicht in den Griff bekommt und der Manipulation freier Wahlen durch Bots und Trolle Tür und Tor geöffnet hat (und offen hält). Die Rufe nach der Zerschlagung des Konzerns werden lauter.

Und doch scheint es Klartext zu geben bei Facebook. Dummerweise aber nur da, wo er am allerwenigsten hingehört: bei der Speicherung von Passwörtern. Bis zu 600 Millionen Nutzer von Facebook, Facebook Lite und Instagram sind von einem groben Verstoss gegen den Datenschutz betroffen, der Facebook bei einer Routineüberprüfung im Januar aufgefallen sei. Wie Zuckerbergs Konzern am 21. März mitteilte, seien die unverschlüsselten Passwörter nur innerhalb des Unternehmens zugänglich gewesen und von niemandem missbräuchlich verwendet worden. Kurz vor dieser Mitteilung hatte der Sicherheitsexperte Brian Krebs in seinem Blog krebsonsecurity – gestützt auf interne Facebook-Kreise – berichtet, dass mehr als 20.000 Facebook-Mitarbeiter Zugang zu den oft seit Jahren im Klartext gespeicherten Passwörtern gehabt hätten.

Eine solche unverschlüsselte Speicherung von Passwörtern stellt einen klaren Verstoss gegen Artikel 32 der DSGVO dar, der die "Pseudonymisierung und Verschlüsselung personenbezogener Daten" fordert. Die derzeit bestmögliche Lösung, dieser Forderung nachzukommen, sind sogenannte "Hashes", da diese nicht durch Entschlüsseln in Passwörter zurückgewandelt werden können. Hackern bliebe dann nur die Möglichkeit, alle erdenklichen Kombinationen auszuprobieren, um an die richtigen Passwörter heranzukommen (Brute Force-Angriff).

Vielleicht sollte Mark Zuckerberg solchen Regeln im eigenen Haus zur Anwendung verhelfen und damit seinem Konzern helfen, verspielte Glaubwürdigkeit zurück zu erlangen.

Nachzulesen unter:

https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?noredirect=on&utm_term=.778682baeaa8
https://www.faz.net/aktuell/feuilleton/medien/zuckerbergs-aufruf-zur-regulierung-des-internets-16117634.html
https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years
https://www.zdnet.com/article/facebook-we-stored-hundreds-of-millions-of-passwords-in-plain-text
https://www.golem.de/news/datenschutz-facebook-speicherte-millionen-passwoerter-im-klartext-1903-140173.html
https://security.blogoverflow.com/2013/09/about-secure-password-hashing/

IV. Malware ab Werk – oder: Wenn der Shadow Hammer auf die Supply Chain einschlägt?

Auch dieser Security-Report empfiehlt immer wieder, mit regelmässigen Updates mögliche Sicherheitslücken und Angriffsvektoren für Hacker zu schliessen. Diese Empfehlung bleibt auch weiterhin bestehen, obwohl beobachtbar ist, dass Cyberkriminelle zunehmend

Supply Chains der grossen Systemhersteller angreifen, um mit deren Updates unauffällig Malware und Backdoors direkt in die Systeme der User einzuschleusen (wir berichteten beispielsweise über kompromittierte Android-Geräte im Security Report 2/2017). Jüngstes Beispiel: die Malware "Shadow Hammer", die mit einem ASUS-Systemupdate 2018 auf Rechner und mobile Geräte des taiwanesischen Herstellers gelangte. Am 19. Januar 2019 berichteten Kaspersky-Cybersecurity-Experten, dass sie bei knapp 60.000 Kunden Malware gefunden hätten, die über ASUS-Server auf die Geräte geschleust worden war. 12 Tage später habe Kaspersky ASUS informiert, bis heute hätten die Taiwanesen aber keinen ihrer Kunden unterrichtet. Die Angaben Kasperskys wurden später auch vom Wettbewerber Symantec bestätigt. Dass der Schaden bei ASUS nicht bemerkt worden war, führen die Kaspersky-Ingenieure darauf zurück, dass die Malware mit einem digitalen ASUS-Zertifikat signiert war.

Der Fall zeigt auffallende Parallelen zu zwei Supply-Chain-Angriffen aus dem Jahr 2017. Damals waren mit Updates des Säuberungs- und Optimierungstools CCleaner bzw. der Netzwerk-Administrationssoftware ShadowPad Backdoors ausgeliefert worden, die den Angreifern das Datenfischen, Nachladen von Malware oder die Fernsteuerung der kompromittierten Systeme erlaubt hätte. Zwar ist ShadowHammer deutlich besser getarnt als seine Vorgänger, doch haben seine Hintermänner 2017 wie auch aktuell aus tausenden infizierten Systemen nur einige wenige MAC-Adressen tatsächlich angegriffen. Im Fokus dieser eigentlichen Angriffe stehen dabei offenbar Technik- und Telekommunikationsunternehmen in Japan, Taiwan, Grossbritannien, Deutschland und in den USA. Dort will man das Problem gehäufter Angriffe auf Supply Chains der ICT-Unternehmen mit der Bildung einer Task Force begegnen, die die Homeland Security im November 2018 ins Leben gerufen hatte.

Zwischenzeitlich – um genau zu sein, am 26. März – veröffentlichte ASUS eine Pressemitteilung, der zufolge das Live Update Utility gepatcht wurde. Es kann und sollte bei ASUS heruntergeladen werden. Zudem bietet der Hersteller ein Check-Tool, mit dem User prüfen können, ob ihr System betroffen ist. Die entsprechenden Tools von Kaspersky sind im unten zitierten Blogbeitrag von Kaspersky – securelist.com – verlinkt.

Nachzulesen unter:

https://www.heise.de/security/meldung/ShadowHammer-ASUS-verteilte-offenbar-Schadcode-an-ueber-1-Million-Nutzer-4348242.html?wt_mc=rss.security.beitrag.atom
https://m.tagesanzeiger.ch/articles/19690172
https://futurezone.at/digital-life/asus-hat-malware-per-update-an-halbe-million-laptops-verteilt/400446937
https://www.inforisktoday.com/operation-shadowhammer-shows-weakness-supply-chains-a-12251
https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members
https://securelist.com/operation-shadowhammer/89992

In eigener Sache: Neu im SWITCHcert Security Blog

DNSSEC Usage in Switzerland is on the rise after widespread attacks on the Domain Name System

https://securityblog.switch.ch/2019/04/02/dnssecinswitzerland2019/

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

Der SWITCH-CERT Security Report spiegelt nicht die Meinung von SWITCH wider, sondern ist eine Zusammenstellung verschiedener Berichterstattungen in den Medien. SWITCH übernimmt keinerlei Gewähr für die im Security Report dargelegten Inhalte, Meinungen oder deren Richtigkeit.