Switch Security Report

zu aktuellen Trends im Bereich IT-Security und Privacy

November/Dezember 2023

I. Es gibt noch gute Nachrichten: Die Kryptokalypse bleibt aus (noch)

In Zeiten, in denen in der realen wie in der virtuellen Welt eine Krise die nächste jagt, gute Nachrichten zu finden, ist fast schon wie Weihnachten. Wenn die dann auch noch von einer Stelle kommen, die normalerweise eher für die Katastrophenmeldungen verantwortlich ist, dann wird der Q-Day zum C-Day (C für Christmas). Die Rede ist von der Mitte November vorgestellten 2.0-Version der Studie «Entwicklungsstand Quantencomputer» des deutschen Bundesamts für Sicherheit in der Informationstechnik. Dort nimmt das BSI zur Frage Stellung, wann der Tag eintritt, an dem Quantencomputer heute verwendete Verschlüsselungsverfahren knacken können und damit unbrauchbar machen. Dieser Q-Day rückt zwar unaufhaltsam näher – und stellt damit die gesamte Kryptografie vor riesige Herausforderungen –, wird aber nach BSI-Einschätzung dann doch noch ein bis zwei Jahrzehnte auf sich warten lassen. In bisherigen Szenarien standen auch schon einmal lediglich fünf Jahre im Raum. Dennoch empfiehlt das BSI eindringlich, sich bereits heute mit der Kryptokalypse, also der Überwindung gängiger Verschlüsselungsverfahren durch Quantencomputer, auseinanderzusetzen und sich intensiv mit der Entwicklung einer Post-Quanten-Kryptografie zu beschäftigen. Denn zum einen, so die BSI-Studie, sei nicht auszuschliessen, dass disruptive Entwicklungen im Computing den Countdown zum Falldown bislang sicher geglaubter

Verschlüsselungsverfahren extrem beschleunigen könnten. Zum andern würden Migrationsprozesse oft Zeiträume beanspruchen, die dann unter Umständen nicht mehr zur Verfügung stünden. Und zum dritten könnten professionelle Hacker schon heute verschlüsselte Daten bis zur Verfügbarkeit entsprechender quantenbasierter Entschlüsselungsmethoden und -devices zwischenlagern und dann auswerten, wenn Tools und Devices verfügbar seien.

Blickt man auf die aktuell kontrovers verlaufende Diskussion darüber, wie Datensicherheit nach dem Q-Day gewährleistet werden soll/kann, scheint es tatsächlich angeraten, keine Zeit zu verlieren, sich mit der Entwicklung von Standards für eine Post-Quanten-Kryptografie zu befassen. Aktuell hat sich US-amerikanische National Institute of Standards and Technology (Nist) Crystal Kybers, einen von IBM entwickelten Algorithmus als Standard zu etablieren. Dagegen warnen Forscher wie Grégoire Ribordy der Genfer Firma ID Quantique davor, dass aktuell noch gar nicht klar sei, was Quantencomputer eines Tages wirklich leisten könnten. Ob die neuen Algorithmen auch langfristige Sicherheit bieten könnten, sei daher nicht erwiesen. Ribordy plädiert deshalb für die Quantenkryptografie – den direkten Austausch symmetrischer Schlüssel aus einzelnen Lichtquanten durch zwei Benutzende via Glasfaser (eine schematische Darstellung findet sich im unten verlinkten NZZ-Artikel).

Während der Genfer Forscher die Quantenkryptografie als absolut sicher bezeichnet, widerspricht dem eine mächtige Allianz aus NSA und den Cybersecurity-Behörden der USA und Grossbritanniens, die sich für die Post-Quanten-Kryptografie stark machen. Sie bezweifeln die Sicherheitsversprechen der Quantenkryptografie und verweisen auf Hardware-Schwachstellen, hohe Aufwände und Kosten sowie die ungelösten Authentifizierungsprobleme – Argumente, die die Quantenphysikerin und der Quantenphysiker der ETH Zürich Renato Renner und Ramona Wolf nach einer gründlichen Analyse teilweise entkräftet haben. Während aber offenbar die Post-Quanten-Kryptografie-Allianz im Ansatz aus Genf einen Konkurrenten sieht (man darf vermuten, dass diese Perspektive nicht nur sicherheitstechnisch, sondern auch ökonomisch getriggert wird), plädiert Grégoire Ribordy dafür, beide Technologien miteinander zu verbinden, um den neuen Sicherheitsanforderungen gerecht werden zu können. Gut, dass noch ein wenig Zeit zu sein scheint.

Nachzulesen unter:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Entwicklungsstand-Quantencomputer/entwicklungsstand-quantencomputer_node.html
https://www.heise.de/news/BSI-Kryptografisch-relevante-Quantencomputer-brauchen-noch-10-bis-20-Jahre-9459448.html
https://www.nzz.ch/wissenschaft/kryptografie-was-tun-wenn-der-quantencomputer-heutige-schluessel-knacken-kann-ld.1758441
https://blog.iao.fraunhofer.de/post-quanten-kryptographie-wie-man-trotz-quantencomputer-noch-sichere-it-systeme-betreiben-kann
https://www.computerweekly.com/de/feature/Die-Auswirkungen-von-Quantum-Computing-auf-Kryptografie

II. Es gibt aber auch (leider) genug schlechte Nachrichten: Nach Angriff auf einen IT-Dienstleister tauchen erneut sensible Daten Schweizer Bundesbehörden im Darknet auf

IT-Dienstleister Schweizer Bundesbehörden stehen auf der Liste professioneller Hacker offenbar relativ weit oben: Nachdem in Sommer nach einem erfolgreichen Angriff auf XPlain sensible Daten kantonaler und bundespolizeilicher Polizei im Darknet aufgetaucht waren, sind dort vor kurzem hochsensible Daten von US-Kunden Schweizerischer Banken gesichtet worden. Diese stammen offenbar aus dem Angriff auf den Schweizer IT-Dienstleister Concevis, der neben Geldhäusern und Versicherungen auch die Eidgenössische Steuerverwaltung ESTV zu seinen Kunden zählt und von dieser beauftragt war, ein Fallbearbeitungssystem für die Abwicklung von Rechtshilfegesuchen amerikanischer Steuerbehörden an die ESTV zu entwickeln. Die Daten wurden dem Zürcher Tagesanzeiger von einem anonymem Hinweisgeber vorgelegt und konnten bislang nicht verifiziert werden.

Überhaupt zeigt sich der komplette Concevis-Hack als überaus geheimnisumwittert: Fest steht lediglich, dass es Anfang November einen erfolgreichen Ransomware-Angriff auf den Basler IT-Dienstleister gegeben hatte, bei dem auch grössere Datenmenge gestohlen worden waren. Dagegen ist bis heute nicht bekannt (oder veröffentlicht), wem die Tat anzulasten sei. Dafür zeigen sich unschöne Parallelitäten zum XPlain-Hack. Auch dort lagerten Daten von Behörden direkt beim IT-Dienstleister. Und wie im XPlain-Hack scheint auch im Fall Concevis die wahre Tragweite des Falls nur in homöopathischen Dosen an die Öffentlichkeit gelassen zu werden. Was unter Umständen daran liegen mag, dass sich die Behörden dem Vorwurf ausgesetzt sehen, wie im XPlain-Fall ihre Aufsichtspflichten nicht oder nicht zureichend wahrgenommen zu haben.

Will die Schweiz ihren guten Ruf als sicherer und innovativer IT-, Krypto- und/oder KI-Standort behalten oder gar ausbauen, gibt es also einige wichtige Vorsätze fürs Neue Jahr zu formulieren und umzusetzen.

Nachzulesen unter:

https://www.inside-it.ch/bericht-heikle-daten-aus-concevis-hack-aufgetaucht-20231124
https://www.tagesanzeiger.ch/cyber-attacke-hacker-bieten-im-darknet-hochsensible-daten-des-bundes-an-770557314864
https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-98595.html
https://www.nzz.ch/technologie/concevis-ransomware-phobos-bund-hat-it-lieferanten-nie-kontrolliert-jetzt-wurde-er-gehackt-ld.1766717?reduced=true
https://www.nzz.ch/wirtschaft/schweizer-hochschulen-planen-eine-grosse-ki-initiative-ld.1767609?reduced=true

III. Kein Safe Harbour in Down Under: Weihnachtsgeschenke kommen später, weil Hafenbetreiber gehackt wurde

DP World ist Golfenthusiasten als Titelsponsor der höchsten europäischen Golf-Liga bekannt. Daher dürften es australische Golferinnen und Golfer, die sich zu Weihnachten neues Equipment gewünscht habe, als besonders zynisch empfinden, dass ihre Geschenke in diesem Jahr verspätet oder gar nicht ankommen. Denn als einer der grössten Hafenbetreiber der Welt betreibt auch DP World auch die australischen Häfen Brisbane, Freemantle, Melbourne und Sydney, über die normalerweise mehr als 40 Prozent der Warenströme des roten Riesenlandes fliessen. Ein schwerer Hackerangriff hat diese Warenströme Mitte November unterbrochen, DP World dazu gezwungen, die eigenen System vom Internet zu trennen und den Betrieb in allen vier Häfen einzustellen. Mit der Folge, dass aktuell mehr als 30.000 Container an falschen Orten gestrandet sind. Über die Details des Angriffs schweigen sich sowohl DP World als auch die australische Regierung aus. Bekannt ist nur, dass keine Lösegeldforderung eingegangen sei und keine Kunden-, wohl aber die persönlichen Daten von DP World Mitarbeitenden gestohlen worden seien. Und Fakt ist, dass die Hacker einen überaus empfindlichen Nerv Australiens getroffen haben, das in der Woche vor dem DP World Hack vom Totalausfall des zweitgrössten Internetproviders Down Under betroffen war. Entsprechend warnte Claire O´Neil, Ministerin für Inneres und Cybersicherheit, vor den Risiken von Cyberangriffen auf die australische Infrastruktur. Die australische Freight and Trade Alliance warnte ihrerseits davor, dass viele Waren nicht ins oder aus dem Land kämen und Lieferungen verspätet oder gar nicht ausgeführt werden könnten.

Als ebenso ernsthaft könnten sich die Folgen des mit dem Hack vollzogenen Diebstahls der Mitarbeitenden-Daten erweisen. Der australische Sicherheitsforscher Andrew Martin verwies darauf, dass Hacker mit solchen Daten – wenn auch in manchen Fällen erst nach weiteren Anstrengungen – die volle Palette der Cyberverbrechen gegen Personen offen stünde – von der betrügerischen Bestellung beim Food-Service bis zum Umleiten der kompletten Pensionszahlung.

Nachzulesen unter:

https://www.heise.de/news/DP-World-Sicherheitsvorfall-legt-Betrieb-des-Hafenbetreibers-in-Australien-lahm-9408226.html
https://www.heise.de/news/Nach-Cyberangriff-30-000-Container-gestrandet-Australiens-Haefen-arbeiten-wieder-9424439.html
https://www.theguardian.com/australia-news/2023/nov/13/australian-port-operator-hit-by-cyber-attack-says-cargo-may-be-stranded-for-days
https://www.smh.com.au/business/companies/cyberattack-threatens-to-spark-christmas-goods-shortage-20231112-p5ejcm.html
https://theloadstar.com/cyber-attack-has-left-employees-vulnerable-admits-dp-world-australia/#
https://www.bbc.com/news/business-67400164

IV. Namedropping und Panikmache – oder: Zuviel Awareness ist auch keine Lösung

Mit all unseren Security Reports haben wir auch immer wieder versucht, das Bewusstsein für die Risiken der digitalen Welt zu schärfen. Dabei war uns immer klar, dass ein Zuviel das genaue Gegenteil dessen erzeugt, was wir eigentlich wollten. Dass das schnell passieren kann, zeigt das aktuelle Beispiel der von übervorsichtig-voreiligen Polizeistellen ausgelösten Besorgniswelle um Apples neue «NameDrop»-Funktion für iPhones und Apple Watches unter iOS 17. Bringt man zwei damit ausgestattet iPhones eng zusammen, tauschen diese nämlich die Kontaktdaten ihrer Besitzer automatisch aus – allerdings nur, wenn beide iPhones vorher entsperrt waren und deren Besitzerinnen dem Austausch ausdrücklich zustimmen.

Diesen kleinen, aber wichtigen Nebensatz haben viele überlesen (oder weggelassen), die in Sozialen Medien eine Flut an Warnungen ausgelöst haben. Die hat dazu geführt, dass verschiedene Polizeibehörden der US «Datenschutzhinweise» zum Gebrauch von iOS 17 und watchOS 10 veröffentlichten, die ihrerseits den Warnungen dann auch noch die staatliche Autorisierung mitgaben und die eigentlich substanzlose Welle erst recht aufbauschten.

Daraufhin sah sich die Redaktion von WIRED dazu veranlasst, eine Art «halboffizielle Gegen-darstellung» zu publizieren, um Userinnen und Usern die Sorge vor der standardmässig aktivierten NameDrop-Funktion zu nehmen.

Nachzulesen unter:

https://www.wired.com/story/apple-iphone-namedrop-ios17
https://www.heise.de/news/Kontaktinfos-teilen-per-iPhone-Bump-NameDrop-verunsichert-Nutzer-9542624.html
https://www.washingtonpost.com/technology/2023/11/27/namedrop-iphone-ios17-safety

V. Freaky Leaky SMS: Der Spion, der aus der Stille kam

Dass Smartphones Angriffsvektoren, z.B. für sog. Side-Channel-Attacken, liefern können, haben Forschende in einem Experiment nachgewiesen, das sie Freaky Leaky SMS nannten. Im Groben gelang Evangelos Bitsikas von der Northeastern University, Theodor Schnitzler vom Research Center Trustworthy Data Science and Security der Uni Dortmund, Christina Pöpper von der New York University Abu Dhabi sowie Aanjhan Ranganathan von der Northeastern University der Nachweis, dass man aus der Kombination von Übertragungsrouten und -zeiten still versandter SMS den Standort des angesimsten Smartphones ermitteln und damit seine Besitzerin oder seine Besitzer tracken kann (die Details finden sich im unten verlinkten bleeping-computer-Artikel bzw. arvix.org-pdf). Betrachtet man allerdings den Aufwand, der dafür betrieben werden muss, stellt sich auch in diesem Fall die Frage, ob hier nicht ein bisschen zu viel an Awareness-Generierung betrieben wurde.

Nachzulesen unter:

https://www.bleepingcomputer.com/news/security/sms-delivery-reports-can-be-used-to-infer-recipients-location
https://futurezone.at/science/freaky-leaky-sms-standort-sms-spionage/402493016
https://arxiv.org/pdf/2306.07695.pdf

VI. Wo Awareness wirklich gefragt ist: Der booking.com-Fraud und seine Folgen

Dass echte Awareness-Warnungen so dingend und wichtig sind, wie nie zuvor – und deshalb eben nicht von lapidarer oder unrelevanter Panikmache entschärft werden sollten – zeigen die massiv zunehmenden Betrugsfälle, Scam- und Phishing-Versuche, denen sich booking.com-Kundinnen und -Kunden ausgesetzt sehen. Während die weltgrösste Buchungsplattform bis heute bestreitet, gehackt worden zu sein, bekommen Plattform-Nutzende zunehmend viele und immer raffiniertere Aufforderungen zugeschickt, Kundendaten zu validieren oder Kreditkarten- oder Accountdaten erneut einzugeben. Alles im Original booking.com-Design und inzwischen auch nicht mehr nur in Form von Mails, sondern direkt aus der booking.com-App heraus.

Bereits im letzten Security Report haben wir davor gewarnt, dass Hotels zunehmend angegriffen werden, um primär Login- und Kreditkartendaten der Kundschaft zu ergaunern. Diese werden dann zu Preisen zwischen 30 und bis zu 2.000 US$ im Darknet weiterverkauft und erfreuen sich offenbar einer regen Nachfrage. In der Regel werden daraus täuschend echte Nachrichten, die mit korrekten Daten bzgl. Hotelname, Buchungsdatum, Buchungsnummer, eigener Name und booking.com-Code versehen und an Plattformnutzende verschickt werden. Ihr Inhalt: Die Buchung sei gefährdet, weil die Eingaben zur Kreditkarte nicht akzeptiert wurden, weshalb diese innerhalb einer sehr engen zeitlichen Frist nochmals eingegeben werden müssten. Der Zeitdruck wirkt dabei als Betrugs-Booster: Denn weil alle anderen Daten stimmen, bleiben Empfangspersonen zur Authentifizierung einer solchen Nachricht eigentlich nur die Möglichkeit, alles in Rückfrage mit dem infrage kommenden Hotel abzuklären. Genau das wollen die Betrüger aber ja verhindern. Und genau darum gilt aktuell bei allen booking.com-Anfragen: Awareness, awareness, awareness!

Nachzulesen unter:

https://economictimes.indiatimes.com/tech/technology/fraudsters-attack-booking-com-customers-after-hacking-hotels/articleshow/105701847.cms
https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/wochenrueckblick_4.html
https://www.watson.de/leben/urlaub%20&%20freizeit/876741668-booking-com-kunden-aufgepasst-fiese-betrugs-masche-im-umlauf
https://www.igorslab.de/warnung-booking-com-versendet-scam-bloss-nicht-antworten

VII. (Solar)Winds of Change: Wenn´s ums Geld geht, werden auch Security-Muffel plötzlich aktiv

Der Fall ist ebenso einzigartig wie seine Dimensionen: Ende 2020 war bekannt geworden, dass offenbar russische Staatshacker (was die russische Regierung bestreitet) mindestens drei Softwareprodukte von Solarwinds mit Schadcode infiziert hatten, die im anfangs Januar 2019 an mehr als 18.000 Kunden weltweit verschickt worden war. Darunter auch die Sicherheitsfirma Fireeye und etliche US-Regierungsbehörden. Es verging fast ein Jahr, bevor Fireeye selbst Opfer eines Hackerangriffs wurde und dabei die kompromittierte Software als Eingangsportal gefunden hatte.

Nun bekommt der Fall eine juristische Aufarbeitung, die bislang ohne Präzedenz ist: Denn Kläger sind nicht Staats- oder Rechtsanwälte der geschädigten Behörden oder Firmen, sondern die US-amerikanische Börsenaufsicht SEC. Die wirft der seit 2018 börsenkotierten Firma Solarwinds vor, die Cybersicherheits-Risiken in ihren Systemen gegenüber den Aktionären verschwiegen zu haben. Käme die SEC mit ihrer Klage durch, so würden Cybersecurity-Risiken quasi konstitutionelle Bewertungsfaktoren börsennotierter Aktiengesellschaften und würden den Druck auf diese Unternehmen verstärken, über diese Risiken transparent zu informieren.

Wie nicht anders zu erwarten war, bezeichneten denn auch die Solarwinds-Anwälte die Klage als unzulässig, weil die SEC dafür nicht zuständig sei. Dennoch sind die Solarwinds-Entwickler zumindest etwas aktiver geworden und haben im November zwei Sicherheitslücken auf der Solarwinds Platform geschlossen. Userinnen und User sollten daher unbedingt auf Version 2023.4.2 updaten.

Generell darf man also angesichts der oben beschriebenen möglichen Konsequenzen auf den Ausgang des Verfahrens gespannt sein.

Nachzulesen unter:

https://t3n.de/news/solarwinds-hacker-angriff-klage-1585907/
https://www.heise.de/news/Sicherheitsluecke-Schadcode-Attacken-auf-Solarwinds-Platform-moeglich-9543391.html

Dieser Switch Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.