Switch Security Report

on the latest IT security and privacy trends

November/December 2023

I. There is still good news: The cryptocalypse is not happening (yet)

Finding good news in times of crisis after crisis in the real and virtual world is almost like Christmas. And when it comes from an organisation that is normally responsible for disaster reports, then Q-Day becomes C-Day (C for Christmas). We are talking about the 2.0 version of the study "Development status of quantum computers" published by the German Federal Office for Information Security in mid-November. In it, the BSI comments on the question of when the day will come when quantum computers will be able to crack the encryption methods used today and thus render them useless. Although this Q-Day is inexorably approaching - and thus poses huge challenges for cryptography as a whole - the BSI estimates that it will be another one to two decades before it happens. In previous scenarios, only five years have ever been envisaged. Nevertheless, the BSI strongly recommends that the cryptocalypse, i.e. the overcoming of conventional encryption methods by quantum computers, should be addressed today and that the development of post-quantum cryptography should be intensively analysed. For one thing, according to the BSI study, it cannot be ruled out that disruptive developments in computing could extremely accelerate the countdown to the fall of encryption methods that were previously thought to be secure. Secondly, migration processes would often require periods of time that may then no longer be available. And thirdly, professional hackers

could already store encrypted data until the corresponding quantum-based decryption methods and devices are available and then analyse it when tools and devices are available.

Looking at the current controversial discussion about how data security should/can be guaranteed after Q-Day, it seems advisable to waste no time in developing standards for post-quantum cryptography. The US National Institute of Standards and Technology (Nist) Crystal Kybers is currently endeavouring to establish an algorithm developed by IBM as a standard. However, researchers such as Grégoire Ribordy from the Geneva-based company ID Quantique warn that it is not yet clear what quantum computers could really achieve one day. Whether the new algorithms could also offer long-term security has therefore not been proven. Ribordy therefore advocates quantum cryptography - the direct exchange of symmetrical keys consisting of individual light quanta between two users via optical fibre (a schematic diagram can be found in the NZZ article linked below).

While the Geneva researcher describes quantum cryptography as absolutely secure, this is contradicted by a powerful alliance of the NSA and the cybersecurity authorities in the USA and the UK, who are strongly in favour of post-quantum cryptography. They doubt the security promises of quantum cryptography and point to hardware vulnerabilities, high effort and costs as well as unsolved authentication problems - arguments that quantum physicists Renato Renner and Ramona Wolf from ETH Zurich have partially refuted following a thorough analysis. However, while the Post-Quantum Cryptography Alliance apparently sees the approach from Geneva as a competitor (one can assume that this perspective is not only triggered by security issues, but also by economic factors), Grégoire Ribordy is in favour of combining both technologies in order to meet the new security requirements. It's a good thing that there still seems to be a little time left.

Read more at:

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. But there is also (unfortunately) enough bad news: After an attack on an IT service provider, sensitive data from Swiss federal authorities once again appears on the darknet

IT service providers of Swiss federal authorities are apparently relatively high on the list of professional hackers: After sensitive cantonal and federal police data surfaced on the darknet in the summer following a successful attack on XPlain, highly sensitive data from US customers of Swiss banks has recently been spotted there. The data apparently originated from the attack on the Swiss

IT service provider Concevis, whose clients include not only financial institutions and insurance companies but also the Swiss Federal Tax Administration (FTA), which had commissioned it to develop a case processing system for handling requests for legal assistance from US tax authorities to the FTA. The data was provided to the Zürcher Tagesanzeiger by an anonymous whistleblower and has not yet been verified.

In general, the entire Concevis hack is shrouded in mystery: all that is known is that there was a successful ransomware attack on the Basel-based IT service provider at the beginning of November, during which a large amount of data was stolen. However, it is still not known (or publicised) who was responsible for the attack. However, there are unsavoury parallels to the XPlain hack. Data from public authorities was also stored directly with the IT service provider. And as in the XPlain hack, the true extent of the case in the Concevis case also appears to have been publicised only in homeopathic doses. This may be due to the fact that, as in the XPlain case, the authorities are facing accusations that they did not fulfil their supervisory duties, or did not do so sufficiently.

If Switzerland wants to maintain or even build on its good reputation as a secure and innovative IT, crypto and/or AI centre, there are some important resolutions to formulate and implement for the New Year.

Read more at:

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. No Safe Harbour Down Under: Christmas presents arrive later because port operator was hacked

DP World is known to golf enthusiasts as the title sponsor of Europe's top golf league. Australian golfers who wanted new equipment for Christmas are therefore likely to find it particularly cynical that their presents will arrive late or not at all this year. As one of the largest port operators in the world, DP World also operates the Australian ports of Brisbane, Freemantle, Melbourne and Sydney, through which more than 40 per cent of the red giant's goods normally flow. A serious hacker attack interrupted these flows of goods in mid-November, forcing DP World to disconnect its own systems from the Internet and shut down operations at all four ports. As a result, more than 30,000 containers are currently stranded in the wrong places. Both DP World and the Australian government are keeping quiet about the details of the attack. All that is known is that no ransom demand was received and that no customer data, but the personal data of DP World employees was stolen. And the fact is that

the hackers have hit a very sensitive nerve in Australia, which was affected by the total outage of the second-largest internet provider Down Under in the week before the DP World hack. Accordingly, Claire O'Neil, Minister for Home Affairs and Cyber Security, warned of the risks of cyberattacks on Australia's infrastructure. For its part, the Australian Freight and Trade Alliance warned that many goods would not be able to enter or leave the country and that deliveries could be delayed or even cancelled.

The consequences of the theft of employee data carried out with the hack could prove to be just as serious. Australian security researcher Andrew Martin pointed out that hackers with such data - albeit in some cases only after further efforts - would have access to the full range of cybercrimes against individuals - from fraudulently ordering food from a food service to diverting the entire pension payment.

Read more at:

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. Name-dropping and scaremongering - or: too much awareness is no solution either

With all our security reports, we have also repeatedly tried to raise awareness of the risks of the digital world. In doing so, we have always realised that too much will produce the exact opposite of what we actually wanted. The current example of the wave of concern triggered by overly cautious and premature police authorities about Apple's new "NameDrop" function for iPhones and Apple Watches under iOS 17 shows that this can happen quickly. If two iPhones equipped with this function are brought close together, they automatically exchange the contact details of their owners - but only if both iPhones were previously unlocked and their owners expressly consent to the exchange.

Many people overlooked (or omitted) this small but important subordinate clause, which triggered a flood of warnings on social media. This led to various police authorities in the US publishing "privacy advisories" on the use of iOS 17 and watchOS 10, which in turn added government authorisation to the warnings and further fuelled the insubstantial wave.

As a result, the WIRED editorial team felt compelled to publish a kind of "semi-official rebuttal" to allay users' concerns about the NameDrop function, which is activated by default.

Read more at:

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: The spy who came out of the silence

Researchers have demonstrated that smartphones can provide attack vectors, e.g. for so-called side-channel attacks, in an experiment they called Freaky Leaky SMS. Evangelos Bitsikas from Northeastern University, Theodor Schnitzler from the Research Center Trustworthy Data Science and Security at the University of Dortmund, Christina Pöpper from New York University Abu Dhabi and Aanjhan Ranganathan from Northeastern University were able to prove that the location of the targeted smartphone can be determined from the combination of transmission routes and times of silently sent text messages and thus its owner can be tracked (the details can be found in the bleeping-computer article linked below or in the arvix.org-pdf). However, if you consider the effort required to do this, the question arises as to whether a little too much awareness has been generated here.

Read more at:

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. Where awareness is really needed: The booking.com fraud and its consequences

The fact that genuine awareness warnings are more urgent and important than ever before - and should therefore not be defused by terse or irrelevant scaremongering - is demonstrated by the massive increase in cases of fraud, scam, and phishing attempts to which booking.com customers are exposed. While the world's largest booking platform still denies that it has been hacked, platform users are receiving an increasing number of increasingly sophisticated requests to validate customer data or re-enter credit card or account details. All in the original booking.com design and no longer just in the form of emails, but directly from the booking.com app.

In our last Security Report, we warned that hotels are increasingly being attacked, primarily to steal login and credit card data from customers. These are then sold on the Darknet at prices of between US$ 30 and US$ 2,000 and are apparently in high demand. As a rule, deceptively genuine messages are sent to platform users with the correct data regarding the hotel name, booking date, booking number, own name and booking.com code. Their content: The booking is jeopardised because the

credit card details were not accepted, which is why they have to be re-entered within a very tight deadline. The time pressure acts as a fraud booster: because all the other data is correct, the only way for the recipient to authenticate such a message is to clarify everything with the hotel in question. But that's exactly what the fraudsters want to prevent. And that is precisely why the following currently applies to all booking.com enquiries: Awareness, awareness, awareness!

Read more at:

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: When it comes to money, even security grouches suddenly become active

The case is as unique as its dimensions: At the end of 2020, it became known that Russian state hackers (which the Russian government denies) had apparently infected at least three Solarwinds software products with malicious code that had been sent to more than 18,000 customers worldwide in early January 2019. These included the security firm Fireeye and a number of US government agencies. Almost a year passed before Fireeye itself fell victim to a hacker attack and found the compromised software as an entry point.

The case is now being dealt with by the courts, which has no precedent to date: the plaintiffs are not government lawyers or lawyers from the authorities or companies that have suffered damage, but the US Securities and Exchange Commission (SEC). The SEC accuses Solarwinds, which has been listed on the stock exchange since 2018 of concealing the cybersecurity risks in its systems from its shareholders. If the SEC were to prevail with its complaint, cybersecurity risks would become quasi-constitutional valuation factors for listed stock corporations and would increase the pressure on these companies to provide transparent information about these risks.

As was to be expected, Solarwinds' lawyers also labelled the lawsuit inadmissible because the SEC had no jurisdiction over it. Nevertheless, the Solarwinds developers have at least become somewhat more active and closed two security vulnerabilities on the Solarwinds Platform in November. Users should therefore definitely update to version 2023.4.2.

In view of the possible consequences described above, it will be interesting to see the outcome of the proceedings.

Read more at:

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

This Switch Security Report was written by Dieter Brecheis and Frank Herberg.

The Switch Security Report does not reflect the opinion of Switch but is a compilation of various reports published in the media. Switch assumes no liability whatsoever for the content, opinions or correctness of the information presented in the Security Report.