Secorvo Security News

März 2025

Selbstmord aus Todesangst?

Den Begriff des „Quantencomputers“ prägten die Physiker Paul Benioff und Richard Feynman im Jahr 1981. Gut 40 Jahre später gibt es erste Prototypen für Quantenprozessoren. Einige Herausforderungen wie die hohe Fehlerrate sind noch nicht gelöst, aber es ist vorstellbar, dass in einigen Jahrzehnten leistungsfähige Quantencomputer existieren. Sollte das gelingen, droht ein „Krypto-Blackout“: Mit einem Schlag wären fast alle im Internet genutzten Verschlüsselungen und Signaturen wirkungslos, denn mit dem Algorithmus von Peter Shor (1994) ließen sich die heute eingesetzten asymmetrischen Kryptoverfahren in kürzester Zeit brechen.

Damit könnte sich die Geschichte wiederholen: 1863 zeigte Friedrich Wilhelm Kasiski, wie man die Vigenère-Chiffre bricht – sie hatte seit dem 16. Jahrhundert als unknackbar gegolten. Nachrichtendienste und Militärs mussten auf simple Codebücher umstellen. Dadurch gelang dem britischen Geheimdienst 1917 die Entschlüsselung des „Zimmermann-Telegramms“, dessen Bekanntwerden zum Eintritt der USA in den ersten Weltkrieg führte. Das Brechen der Rotormaschine Enigma im zweiten Weltkrieg durch polnische und britische Kryptoanalytiker entschied den U-Boot-Krieg – erst der Data Encryption Standard (DES) beendete 1977 diesen Blackout.

Heute wäre ein Krypto-Blackout weit mehr als ein diplomatischer oder militärischer Rückschlag. Daher bemühen sich seit 10 Jahren Kryptologen weltweit um die Entwicklung von quantencomputerresistenten kryptografischen Algorithmen. Im August 2024 wurden die ersten Verfahren als NIST-Standard verabschiedet, und die NSA kündigte an, ab 2033 nur noch Post-Quantum-Kryptografie einzusetzen. Dabei sind die Verfahren längst nicht so gut untersucht wie RSA und DSA, und die Protokollstandards sind nicht einmal alle angepasst. Doch unsichere Post-Quantum-Verfahren, inkompatible Implementierungen und eine übereilte Umstellung können auch zum Blackout führen – sogar ganz ohne Quantencomputer.

Security News

Fix geklickt

Am 13.03.2025 berichtete Microsoft über eine Phishing-Welle, die auf das Gastgewerbe zielt. Auf der in den (vorgeblich von Booking.com stammenden) E-Mails verlinkten Webseite soll der Anwender durch Tastenanschläge beweisen, dass er kein Automat ist – doch die Tastenfolge „Windows+R“, „Strg+V“ und „Enter“ führt (auf Windows-Systemen) den Inhalt der Zwischenablage aus. Dorthin hat die Webseite zuvor

ganz einfach per Javascript den Bootstrap-Code kopiert.

Davor schützt Awareness-Training nur begrenzt. Wenn ein strenges Zulassen nur vertrauenswürdiger Anwendungen (Application-Whitelisting) nicht infrage kommt, sollte zumindest die Ausführung von Programmen aus dem „Downloads"-Ordner und von HTML-Applikationen unterbunden werden. Das gelingt mit AppLocker. Wirksam ist auch das Abschalten der „Run/Ausführen"-Option im Startmenü per Gruppenrichtlinie. Und noch besser wäre es, wenn Javascript erst gar nicht via Zwischenablage aus der Browser-Sandbox ausbrechen dürfte.

Wer kürzer gilt…

Am 19.02.2025 hat Let's Encrypt ihr erstes kurzlebiges Zertifikat mit einer Gültigkeitsdauer von nur 6 Tagen ausgegeben. Das soll die Sicherheit des Webs verbessern, weil so ein abhanden gekommener TLS-Schlüssel auch ohne die Sperrung des Zertifikats nur kurz von einem Angreifer missbraucht werden kann. Die kurze Gültigkeit soll sogar das Prüfen auf Rückrufe ersetzen: Let's Encrypt verzichtet auf die Erstellung von CRLs und auf die Bereitstellung eines OCSP-Dienstes für diese Zertifikate.

Sperrauskünfte sind aufgrund der hohen Verfügbarkeitsanforderungen aufwendig und können Fehlermeldungen auslösen, die die Benutzer überfordern. Firefox unterstützt das: Zertifikate mit einer Gültigkeitsdauer unter 10 Tagen gelten automatisch als „Revocation Checked".

Let's Encrypt hat dazu das ACME-Protokoll um die Auswahl eines Zertifikatsprofils erweitert. Damit können nun auch Zertifikate für (öffentlich zugewiesene) IP-Adressen beantragt werden. Wer den Mechanismus nutzen möchte, muss auf seiner Webseite dafür den Zertifikatserneuerungsprozess automatisieren.

Sesam, öffne dich!

Wenn Zutrittssysteme Schwachstellen aufweisen, können sie „klassischen" Einbrechern die Türen öffnen. Ein besonders drastisches Beispiel meldete am 15.02.2025 der Kanadier Eric Daigle: Er entdeckte zufällig, dass die Zutrittskontrollsysteme „Enterphone MESH" von Identiv (heute Hirsch) mit voreingestellten Passwörtern ausgeliefert wurden und die Einrichtungsprozedur diese nicht ändert. Eine simple Internetsuche findet bis heute über 2.000 dieser Systeme. Mit dem Schwachstellenscanner Nuclei fand Daigle heraus, dass man sich auf 43 % der erreichbaren Systeme mit dem Standardpasswort anmelden kann.

Das niederländische IT-Sicherheits-Unternehmen Modat veröffentlichte am 25.02.2025 die Ergebnisse einer viel breiter angelegten Untersuchung von über das Internet erreichbaren Zutrittskontrollsystemen. Dabei wurden 49.000 Systeme entdeckt – bei jedem dritten System konnten Daten ausgelesen werden; manche gaben sogar biometrische Daten preis. Dabei ist das Problem altbekannt (siehe „Ali baba und die 40 Räuber", SSN 10/2002).

Rififi im Cyberspace

Der vielleicht bekannteste Raub der Filmgeschichte begann mit der Übernahme der Hausmeisterwohnung über einem Juweliergeschäft – der bisher größte digitale Raub mit der Übernahme des Arbeitsplatzrechners eines Entwicklers einer Blockchain-Wallet-Software. Schaden: ca. 1,4 Mrd. US$.

Die Kryptobörse ByBit nutzt Multi-Signatur-Transaktionen, um Blockchain-Transaktionen mit mehr als einem privaten Schlüssel abzusichern. Sie werden von mehreren einzelnen Signaturen freigegeben, was sich auf der Ethereum-Blockchain mithilfe von Smart-Contracts realisieren lässt. Der Smart-Contract für die Cold-Wallet von ByBit wurde jedoch am 21.02.2025 durch einen mit Backdoor ersetzt. Dabei zeigte die manipulierte Wallet-Software eine harmlose Regel-Transaktion an; der CEO prüfte die Transaktion vor seiner abschließenden (dritten) Signatur nur in der Online-App und nicht auf der Signier-Hardware. Anschließend wurden aus der Wallet über eine Milliarde US$ in Coins und Tokens abgezogen.

Nach dem Raub stückelten, tauschten und mischten die Täter ihre Beute, um vor dem Umtausch in „echtes" Geld die Herkunft zu verschleiern, damit Verfolger die Blockchain-Transaktionen nicht einfrieren können. Die Vorgehensweise deutet auf nordkoreanische „Devisenbeschaffer" hin.

Memory Safety

Am 22.01.2025 rief die Association for Computing Machinery (ACM) in ihren *Communications of the ACM* dazu auf, Speichersicherheit endlich zum Standard in der Softwareentwicklung zu machen. Gemeint ist nicht nur der Einsatz zusätzlicher Schutzmechanismen, sondern auch der Wechsel zu speichersicheren Programmiersprachen wie Rust, Swift oder Python. Untersuchungen von Microsoft, Google, NSA sowie CISA belegen, dass nach wie vor sehr viele sicherheitskritische Schwachstellen auf Speicherfehler zurückgehen – etwa durch fehlerhafte Zeigerarithmetik oder Use-after-free-Bugs in C und C++. Die ACM verweist auf die Plattform memorysafety.org, die Wissen, Werkzeuge und Hilfestellungen für den Umstieg bereitstellt.

Google ersetzt in Android-Komponenten C++ bereits durch Rust, Microsoft nutzt Rust für sicherheitskritische Teile von Windows und auch im Linux-Kernel hat Rust Einzug gehalten. Doch das Ersetzen bestehender Software ist mühsam. Wer jedoch weiter auf C oder C++ setzt, muss zumindest für harte Compiler-Optionen, statische Analyse und Laufzeitschutz sorgen.

Angriff via Webcam

Das IT-Sicherheitsunternehmen S-RM berichtete am 05.03.2025, dass die Ransomwaregruppe Akira durch die Übernahme einer ungesicherten Webcam die Endpoint Detection and Response-Software (EDR) umgehen und von dort Netzwerklaufwerke verschlüsseln konnte. Lessons Learned: IoT-Systeme wie Webcams, die öfter Sicherheitslücken aufweisen als Windows-Clients oder Linux-Server, sollten stets in separaten Netzwerksegmenten betrieben werden.

Schlüssel statt Wörter

Mandiant zeigte in einem Beitrag vom 17.03.2025 einen Demonstrator für Phishing mit Browser-in-the-Middle. Damit können Angreifer Sessions und MFA-Codes abfangen, ohne Aufwand in den Nachbau einer Phishing-Webseite stecken zu müssen. Angriffe dieser Art lassen sich durch phishing-resistente Passkeys abwehren. Sie sind ein Ersatz für Passwörter und basieren auf einem Mechanismus, der auch der clientseitigen TLS-Authentifikation (mTLS) zugrunde liegt: Die Nutzer erzeugen ein Schlüsselpaar, hinterlegen den öffentlichen Schlüssel beim verwendeten Dienst und signieren mit dem privaten Schlüssel eine Challenge.

Passkeys haben weitere Vorteile gegenüber Passwörtern: Wenn Angreifer den Server kompromittieren, erbeuten sie nur den öffentlichen Schlüssel, Nutzer können den privaten Schlüssel in sicherer Hardware ablegen und es ist sogar möglich, Nachweise über den Speicherort des privaten Schlüssels zu erstellen. Diensteanbieter können damit beispielsweise die Verwendung von sicherer Hardware vorschreiben – und kontrollieren.

Krypto-Fragilität

Im Zuge der forcierten Migration auf quantenresistente Kryptoalgorithmen hat das NIST am 05.03. 2025 den Initial Public Draft eines Whitepapers zu Crypto-Agility veröffentlicht. Dass das Erreichen des hehren Ziels, schwach gewordene Kryptoalgorithmen schnell durch neue zu ersetzen, kein intuitiver Selbstläufer ist, zeigt sich schon daran, dass zwei unterschiedliche Definitionen von Krypto-Agilität verwendet werden – eine für technische Systeme und eine für Kommunikationsprotokolle.

So ist das Whitepaper eher ein Problemaufriss der hässlichen Seiten der Krypto-Agilität: Herausforderungen bei Interoperabilität, Ressourcenverbrauch und Performance. Und der nachteiligen Auswirkungen in Bezug auf andere Sicherheitsaspekte: Schwierigkeiten bei der Sicherheitsbewertung, erhöhter Schutzbedarf der Aushandlung von Algorithmen und für Updates von Soft- und Firmware im Feld sowie das Restrisiko, den Zugriff auf vorhandene Daten zu verlieren.

Secorvo News

Zertifiziertes Know-how

Im Ernstfall die Nerven und den Überblick bewahren? Als Vorfall-Experte (BSI) sind Sie für den Worst Case gewappnet. Das nächste Seminar findet vom **06. bis 08.05.2025** statt. Noch gibt es freie Plätze.

Mit über 2.200 „T.I.S.P.lern“ ist der TeleTrusT Information Security Professional in der DACH-Region mittlerweile ein renommierter Nachweis für IT-Security-Expertise. Unsere Consultants – die Autoren des T.I.S.P.-Buchs – bereiten Sie vom **19. bis 23.05.2025** auf die Zertifizierung vor.

Alle Seminare bei Secorvo sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (Programme, Online-Anmeldung).

Kettenregeln

In der Softwareentwicklung bedient man sich heute zahlreicher Bibliotheken aus Open-Source-Software oder von Zulieferern. Dadurch wird es schwieriger, die große Zahl direkter und indirekter Abhängigkeiten zu überblicken und auf einem aktuellen Stand zu halten. Beim KA-IT-Si-Event am **15.05. 2025** im dm-dialogicum zeigt Christian Kühn (dmTECH), wie man automatisiert Transparenz über bekannte Schwachstellen in den verwendeten Bibliotheken sowohl im Entwicklungsteam als auch in der zentralen Sicherheitsorganisation herstellen kann. Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Wie immer empfehlen wir eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2025	
28.04.-01.05.	RSA Conference 2025 (RSA Conference, San Francisco/US)
Mai 2025	
04.-08.05.	Eurocrypt 2025 (IACR, Madrid/ES)
06.-08.05.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
06.-09.05.	European Identity & Cloud Conference 2025 (KuppingerCole, Berlin)
12.-15.05.	PKC 2025 (IACR, Roros/NO)
13.-15.05.	26. Datenschutzkongress (EUROFORUM, Berlin)
15.05.	Kettenregeln (KA-IT-Si, Karlsruhe)
19.-20.05.	CIO Cybersecurity Summit 2025 (CIO, München)
19.-23.05.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
20.-22.05.	Datenschutztage 2025 (WEKA, Frankfurt)
26.-28.05.	BvD Verbandstage 2025 (BvD, Berlin)
26.-28.05.	OWASP 2025 Global AppSec (OWASP Foundation, Barcelona/ES)

Fundsache

In einer süffisanten Parabel „A long time ago, in a faraway kingdom" legt der Kryptologe Peter Gutmann dar, warum er die Ressourcen, die in die Entwicklung und Migration zu Post-Quantum-Kryptografie fließen, für Fehlinvestitionen hält. Andere Experten sehen das anders.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Ion Barza, Paul Blenderman, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de