secorvo
security consulting

Secorvo Security News

Juli 2023

Die Quanten kommen

Im Jahr 1994 schockierte Peter Shor die Krypto-Community mit der Publikation eines Algorithmus', mit dem die Faktorisierung ganzer Zahlen und die Bestimmung diskreter Logarithmen auf einem Quantencomputer mit einen Aufwand von O(log n) möglich ist – also in polynomieller Zeit. Damit erschütterte er die Grundlagen der modernen (asymmetrischen) Kryptographie, kurz: den Kern aller heutigen Schutzmechanismen in vernetzten IT-Systemen. Seitdem beten die Kryptologen, dass Quantencomputer in der erforderlichen Größe (10-100 Mio. QBits für 2048-bit-Schlüssel) so schnell nicht kommen – und suchen derweil fieberhaft alternative, gegen Quantencomputer resistente Algorithmen. Die 2016 vom US-amerikanischen NIST gestartete Standardisierungs-Initiative für Post-Quantum Public Key-Algorithmen hat inzwischen schon zahlreiche gebrochene Verfahren aussortiert – mit anderen mathematischen Problemen, die sich für asymmetrische Verfahren eignen könnten, kennen wir uns eben bei weitem nicht so gut aus wie mit der Faktorisierung ganzer Zahlen und dem diskreten Logarithmus.

Sollten die Kryptologen das Wettrennen gegen die Milliardeninvestitionen in Quantencomputer nicht gewinnen, werden wir wohl in archaische IT-Verhältnisse zurückfallen, denn ohne asymmetrische Kryptografie lassen sich Cloud-Computing, Internet-Banking oder Online-Shops praktisch nicht absichern.

Vielleicht haben die Kryptologen noch etwas Zeit. Denn Quantencomputer heutiger Konstruktion sind nicht so einfach herzustellen: Sie müssen bis nahe an den absoluten Nullpunkt gekühlt werden und verbrauchen daher gigantische Energiemengen. Auch die Bereitstellung einer großen Zahl an QBits ist bisher nicht einfach – und da kann man mit größeren Schlüssellängen ein wenig gegensteuern.

Irgendwann aber wird es solche Quantencomputer geben. Ich habe gewettet, dass das noch mindestens 30 Jahre dauert. Mit mehr als einer Kiste Bier wollte ich dabei allerdings nicht ins Risiko gehen.

Inhalt

secorvo
security consulting

Security News

Dritter Anlauf

Nach dem Scheitern von Safe Harbour und Privacy Shield verabschiedete die Europäische Kommission am 10.07.2023 mit dem Data Privacy Framework (DPF) den dritten Angemessenheitsbeschluss für die USA. Personenbezogene Daten dürfen damit wieder ohne zusätzliche Maßnahmen in die USA übertragen werden, sofern die Empfänger DPF-zertifiziert sind. Das U.S. Department of Commerce pflegt die öffentliche Liste aller zertifizierten Organisationen – die sich blitzschnell mit rund 2.500 Einträgen füllte, da das DPF eine reine Selbst-Zertifizierung ist.

Gemäß den Urteilen Schrems I und Schrems II des EuGH ist die US-Überwachung nach FISA 702 und EO 12.333 nicht verhältnismäßig und damit rechtswidrig. In der EO 14.086 (einer leicht angepassten Version der EO 12.333) wurde eine Verhältnismäßigkeitsprüfung ergänzt, die aber faktisch wenig Relevanz haben dürfte: Beschwerden können an den Civil Liberties Protection Officer (CLPO) gerichtet werden, der die Beschwerde jedoch nur prüfen und interne Weisungen erteilen kann. Das Ergebnis der Prüfung kann von einem Data Protection Review Court überprüft werden. Dem Betroffenen wird jedoch nicht mitgeteilt, ob er tatsächlich von einer Überwachungsmaßnahme betroffen war und welche Wirkung seine (anerkannte) Beschwerde hatte.

Nachdem der EUGH bereits die ersten beiden Angemessenheitsbeschlüsse für nichtig erklärt und Max Schrems angekündigt hat, auch den aktuellen Beschluss gerichtlich prüfen zu lassen, sollte man besser nicht auf eine lange Lebenszeit des DLP wetten.

Blindgänger aus Crypto War

Unter dem Namen TETRA:BURST hat die niederländische IT-Sicherheitsfirma Midnight Blue am 24.07.2023 fünf Schwachstellen veröffentlicht, die sie im Auftrag der NLnet-Stiftung mit Hilfe eines Motorola-Fahrzeugfunkgeräts im TETRA-Standard gefunden hat. Dieser 1995 entwickelte ETSI-Standard wird in über 120 Ländern in den Funknetzen von Polizei und Feuerwehr genutzt.

Die meisten Verwundbarkeiten hängen direkt oder indirekt mit der verwendeten proprietären, geheim gehaltenen 80-bit-Stromchiffre zusammen, für die kein öffentliches Peer Review erfolgte. Aufgrund der damaligen Exportbeschränkungen wurde (wie auch bspw. bei Lotus Notes) sogar eine Schwachstelle eingebaut: Damals entwickelte Export-Geräte verwenden effektiv nur 32 Bit lange Schlüssel, die die Forscher mit einem Laptop in wenigen Minuten knacken konnten. Die Details der Schwachstellen (CVE-2022-24400 bis -24404) sollen am 09.08.2023 publiziert werden.

Eine von der ETSI angekündigte Überarbeitung des Standards und die Updates der Hersteller werden die kompromittierten Kryptoverfahren jedoch kaum komplett ersetzen, da die (ungepatchte) Gebrauchsdauer von einmal beschafften Funkgeräten weit über der eines Durchschnitts-PCs oder Smartphones liegt.

Signierte Malware-Kernel-Treiber

Sophos X-Ops publizierte am 11.07.2023 zeitgleich mit einem Microsoft Advisory (ADV230001), dass sie über 100 mit Malware versetzte Windows-Kernel-Treiber entdeckt haben, die bis April 2021 zurückreichen und von Microsoft und anderen Code-Signing-Autoritäten digital signiert worden waren.

Die entdeckten Treiber waren entweder Varianten bekannter Windows-Rootkits oder „Protection Disabler", die Schutzmechanismen des Betriebssystems deaktivieren. Microsoft hat die Treiber in ihre Sperrliste aufgenommen und Sophos hat die Hashwerte und weitere Details zu den betroffenen Treibern in Github publiziert.

BSI Standard 200-4 – Finale Version

Seit dem 14.06.2023 ist der BSI Standard 200-4 „Business Continuity Management" 1.0 verfügbar, der den BSI Standard 100-4 „Notfallmanagement" abgelöst hat. Dies markiert das Ende eines sehr intensiven Peer-Reviewprozesses von Community Drafts (CD 1.0 01/2021, CD 2.0 09/2022) bis zum international gültigen Standard ISO/IEC 22301:2019 „Security and resilience – Business continuity management systems – Requirements".

Der 200-4 geht inhaltlich deutlich über den ISO/IEC 22301 hinaus und bietet eine Mischung aus Anforderungen, Umsetzungsvorschlägen und selbsterklärenden Texten. Sehr praktisch ist der Anforderungskatalog zum Standard 200-4 in Excel, der ein detailliertes Mapping auf die Anforderungen des ISO-Standards enthält, deren Erfüllung so nach Implementierung eines BCM-Systems (BCMS) nach 200-4 leichter nachgewiesen werden kann.

Da bereits der Vorgängerstandard 100-4 im Umfeld von MaRisk und KRITIS als Anforderungskatalog genutzt wurde, ist davon auszugehen, dass auch der 200-4 eine größere Rolle in der Finanzbranche spielen wird. Dabei eignet er sich für jedes Unternehmen, dass ein BCMS in deutscher Sprache aufbauen möchte.

Besonders wertvoll sind die sehr umfangreichen und ziemlich ausgereiften Hilfsmittel zum 200-4

wie Vorlagen und ein Kennzahlensystem. Einziger Wermutstropfen: Die thematische Struktur folgt nicht genau dem zertifizierbaren ISO 22301:2019.

Mobilfunk-Bewegungsdaten

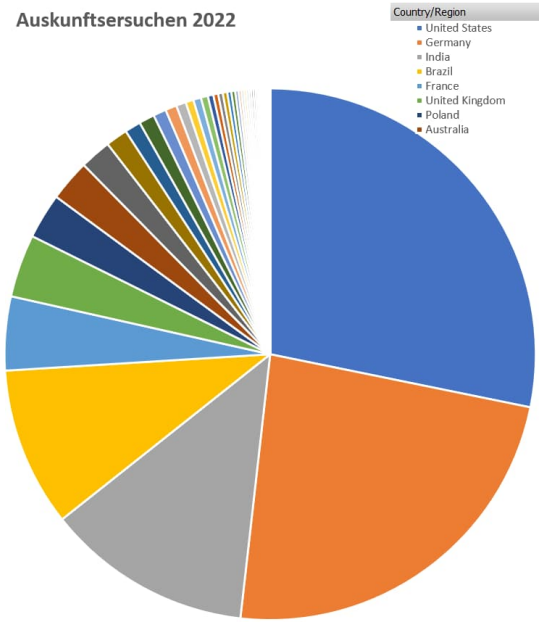
Die Mobilfunknetzbetreiber in Deutschland sammeln, analysieren und verkaufen die Bewegungen ihrer Kunden in anonymisierter Form zu Marketingzwecken an Drittunternehmen. Das ist nicht neu – wir berichteten darüber schon vor fast 15 Jahren (SSN 12/2008).

Durch das Schrumpfen der durchschnittlichen Größe einer Funkzelle in LTE-Netzen werden diese Daten immer genauer – in Städten geben sie ein ziemlich präzises Bewegungsprofil eines Mobilfunkteilnehmers, aus dem sich Wohnort, Arbeitsplatz, Einkaufsverhalten und Freizeitaktivitäten ablesen lassen.

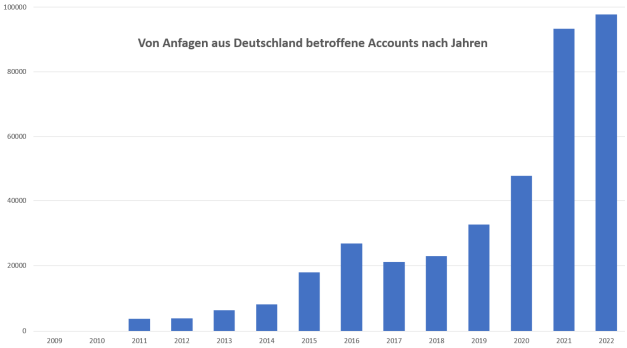
Zwar wirbt Telefónica mit einem dreistufigen Anonymisierungsverfahren; konkrete Informationen über dessen Funktionsweise möchten aber weder sie noch andere Netzbetreiber wie die Telekom herausgeben. Immerhin: Man kann der Verarbeitung der Bewegungsdaten widersprechen. Als Kunde von Telefónica (O2, Blau, Fonic, Simyo u. w.) muss man dafür eine (kostenlose) SMS mit dem Text „Abmelden“ an die Nummer 66866 senden. Telekom-Kunden (Congstar, Klarmobil u. w.) können über ein Opt-Out-Portal widersprechen.

Im Überwachungsstaat

Seit 2009 dokumentiert Google in seinem Transparenzbericht die weltweiten Auskunftsanfragen von behördlichen Stellen. Sieht man sich die Statistiken ein wenig genauer an, kommt man zu ernüchternden Einsichten: Es sind keineswegs die „Schurkenstaaten“, die Google mit Anfragen überhäufen: Auf die USA folgt mit weitem Abstand vor allen anderen 91 Ländern – Deutschland.



Auch steigt die Zahl der von deutschen Anfragen insgesamt betroffenen Accounts seit vielen Jahren. Willkommen im Überwachungsstaat.



Secorvo News

Überarbeitetes T.I.S.P.-Curriculum

Seit dem 01.07.2023 gilt für den TeleTrusT Information Security Professional ein umfangreich überarbeitetes Curriculum. Alle Inhalte wurden von den Anbietern auf den Prüfstand gestellt, aktualisiert, ergänzt oder gekürzt. Hinzu kamen zwei neue Module zu „Virtualisierung“ und „Cloud-Security“. Damit wurden die Inhalte des T.I.S.P.-Seminars zum dritten Mal an aktuelle Entwicklungen der Informationssicherheit angepasst.

In einem Beitrag in der iX 9/2023 stellt Stefan Gora das neue Curriculum des T.I.S.P. ausführlich vor.

Secorvo Seminare

Noch keine Weiterbildung in diesem Jahr besucht? Dann werfen Sie doch mal einen Blick auf unsere Fachseminare im Herbst – Infos und Anmeldung unter https://www.secorvo.de/seminare.

Authenticate. Generate. Repeat.

Das nächste KA-IT-Si-Event am **14.09.2023** (18 Uhr) in der IHK Karlsruhe widmet sich dem Einsatz von PKIs in der Industrie.

Tamás Horváth von Nexus wird einen Überblick über IoT-typische Bedrohungen und die entsprechenden Sicherheitsziele geben. Gemeinsam mit der Firma STIHL wird er am Beispiel des internetfähigen Mähroboters iMow zeigen, wie die Provisionierung digitaler Identitäten mit Hilfe einer autonomen Factory CA gelingt.

Im Anschluss an den Vortrag haben Sie wie immer Gelegenheit zum intensiven Buffet-Networking. Wir freuen uns auf Ihre Anmeldung!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2023	
10.-13.08.	DEF CON 31 (DEFCON, Las Vegas/US)
19.-24.08.	Crypto 2023 (Santa Barbara/US)
September 2023	
11.-13.09.	heise devSec 2023 (dpunt.verlag, heise, Karlsruhe)
14.09.	Authenticate. Generate. Repeat. (KA-IT-Si, Karlsruhe)
18.-22.09.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-27.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
28.09.	IT-Sicherheitsrechtstag 2023 (Swiss Cyber Storm Association, Bern/CH)
Oktober 2023	
9.-12.10.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
10.-12.10.	it-sa 2023 (NürnbergMesse GmbH), Nürnberg
17.-19.10.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)

Fundsache

Eine gute Hilfestellung bei der Prüfung von Auftragsverarbeitungsverträgen bietet die Checkliste des „Datenschutz-Gurus“ Rechtsanwalt Stephan Hansen-Oest.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting

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