Secorvo Security News

Januar 2024

Checks & Balances

Datenschutz ist schon immer ein kontroverses Thema. Zwar hört man die Gleichsetzung der 80er Jahre „Datenschutz = Täterschutz“ und das naiv-plakative „Ich habe nichts zu verbergen“ („Dann geben Sie mir doch bitte Zugriff auf Ihr E-Mail-Konto“) nur noch selten. Doch jüngst häufen sich Äußerungen, die ihn als Verhinderung jeder modernen Datenverarbeitung schmähen.

Eine beunruhigende Entwicklung. Denn angesichts der um sich greifenden Digitalisierung gibt es kein wichtigeres Grundrecht. Darüber wachen in Deutschland mehrere Aufsichtsbehörden. Für Bundesbehörden und Unternehmen, die bundesweit Post- und Telekommunikations¬dienste erbringen, ist der Bundesdatenschutzbeauftragte zuständig: eine unabhängige Kontrollinstanz, die auf Vorschlag der Bundesregierung vom Bundestag gewählt wird.

Jede funktionierende unabhängige Kontrolle ist unbequem, auch für demokratische Regierungen. Wie unbequem die des Bundesdatenschutzbeauftragten Ulrich Kelber ist, kann man in seinen Tätigkeitsberichten nachlesen. Im jüngsten Bericht kennt die Ampel, mit der er die Umsetzung seiner Empfehlungen aus dem Vorjahr bewertet, nur eine Farbe: rot. Aber er wirkt: Die Liste der konkreten Beanstandungen und Verwarnungen an Bundesbehörden umfasst knapp drei Seiten – im Vorjahr war die Liste noch zehn Seiten lang.

Die Amtszeit von Ulrich Kelber endete am 07.01.2024. Trotz seiner unbestrittenen rechtlichen und technischen Kompetenz und seiner unaufgeregten Art will die Bundesregierung sie nicht verlängern. Über die Nachfolge wird gerade politisch geschachert. Das ist bedenklich, denn funktionierende Kontrolle ist der Seismograf einer Demokratie. Regierungen, die einem wirksamen Grundrechtsschutz nicht die gebührende Achtung entgegenbringen, demontieren nicht nur ihre eigene Legitimität, sondern schaden der gesamten demokratischen Ordnung.

(Eine Langfassung dieses Editorials erschien in der iX 1/2024.)

Security News

Falschmeldung

Noch am 16.10.2023 hat die U.S. Börsenaufsicht SEC ihre X-Follower gewarnt: „Seien Sie vorsichtig bei dem, was Sie im Internet lesen. Die beste Quelle für Informationen über die SEC ist die SEC selbst.“ Und bereits im Dezember 2022 hatte sie Anklage gegen acht Social-Media-Influencer erhoben – wegen Aktienmanipulation über Discord und Twitter im Wert von 100 Mio. Dollar.

Nun musste die SEC am 09.01.2024 einräumen, dass ihr eigenes X-Konto mit 750.000 Followern

kompromittiert und eine gefälschte Erklärung, dass künftig Bitcoin-Fonds zugelassen würden, den Bitcoin-Kurs kurzfristig hatte steigen lassen. Dabei stellte sich heraus, dass die SEC ihr X-Konto nicht mit einem zweiten Faktor gesichert hatte: Das Passwort ließ sich per SMS zurücksetzen, sodass der Account via SIM-Swap kompromitiert werden konnte. Lesson Learned: IT-Sicherheitsverantwortliche sollten auch die Social-Media-Konten ihrer PR-Abteilung im Blick behalten.

Mitarbeitertracking

Die französische Datenschutzaufsichtsbehörde CNIL hat am 27.12.2023 gegen Amazon France Logistique wegen exzessiven Monitorings des Beschäftigtenverhaltens eine Geldstrafe von 32 Mio. € verhängt. Sie beanstandete, dass Amazon bei den Mitarbeitern erhebt, wenn die Dauer des Abscannens unter 1,25 Sekunden liegt, Unterbrechungen länger als eine und Pausen über 10 Minuten dauern, und diese Daten über 31 Tage speichert. Zudem wurden Zeitarbeiter bis April 2020 nicht korrekt über die Erhebung informiert.

Die Niedersächsische Datenschutzbeauftragte hatte Amazon diese Praxis im Logistikzentrum in Winsen bereits am 28.10.2020 untersagt; die Entscheidung wurde jedoch vom Verwaltungsgericht Hannover am 09.02.2023 aufgehoben. Das seit April laufende Berufungsverfahren ist noch nicht abgeschlossen.

Durch das Fehlen präziser Regelungen zum Beschäftigtendatenschutz dürften solche Fragen weiterhin über Jahre die Gerichte beschäftigen: So wurde das Datenschutzkontrollverfahren in Niedersachsen bereits am 27.11.2017 eingeleitet.

Post-Quantum-Debatten

Das BSI empfiehlt seit Oktober 2021, quantensichere Public-Key-Algorithmen zunächst mit klassischen zu kombinieren, da erstere noch nicht gut erforscht seien – sie könnten daher anfällig für Implementierungsfehler oder Seitenkanalangriffe sein. Die am 07.01.2024 von Daniel J. Bernstein veröffentlichte KyberSlash-Schwachstelle in Implementierungen von Crystals Kyber zeigt, dass es für die Vorsicht des BSI und von Krypto-Experten wie Bernstein gute Gründe gibt.

Die NSA hingegen lehnt hybride Lösungen wegen der damit verbundenen Komplexität ab. Dabei wurde deren Praktikabilität bereits mehrfach demonstriert, z. B. mit OpenSSH 9.0 vom 08.04.2022. Bernstein vermutet daher, die NSA könnte Einfluss auf die Auswahl des NIST genommen haben, insbesondere bei Kyber-512: Dessen Sicherheitsanalysen wiesen große Unsicherheitsintervalle auf und seien teils fehlerhaft.

Sicher ist: Die jüngsten Angriffe auf PQC-Algorithmen wie SIKE (siehe SSN 7/2022) oder Kyber wecken Zweifel an deren Einsatzreife.

Identische Public Keys

Auf dem 37. Jahreskongress des Chaos Computer Club vom 27. bis 30.12.2023 präsentierten Christoph Saat Johann und Sebastian Schinzel vom Fraunhofer SIT erschreckende Schlampereien im KIM (Kommunikation im Medizinwesen). Dieser Dienst zum verschlüsselten Austausch von Nachrichten in der Telematik-

Infrastruktur der gematik nutzt S/MIME 3.2 (RFC 5751) und soll die Vertraulichkeit und Authentizität von Nachrichten sicherstellen.

Tatsächlich waren jedoch im gemeinsamen LDAP-Adress-Verzeichnis zeitweise fünf und weiteren drei Krankenkassen jeweils dieselben öffentlichen Schlüssel zugeordnet – etwa 28% der Versicherten waren davon betroffen. Die Ursache könnte eine fehlerhafte Schlüsselerzeugung mit Hardware-Security-Modules gewesen sein. Bei der Signierung durch die Certificate Authorities wurde nicht erkannt, dass sechs Schlüssel bereits vergeben waren.

Die gematik hat nun die Umsetzung der Regelung GS-A_4906 aus ihrer Certification Policy erweitert, die eine Einzelzuordnung von Schlüsseln sicherstellen soll (S. 25): So müssen nun neue zu signierende öffentliche Schlüssel mit bereits erstellten verglichen (A_23900-TSP-X.509, S. 21) und geprüft werden, ob es schwache Schlüssel sind (A_17294-TSP-X.509, S. 23).

Treuen Lesern der SSN wäre ein solcher Anfängerfehler vermutlich nicht passiert: Im Februar 2012 haben wir über eine Studie von Forschern der EPFL Lausanne berichtet, die Millionen identische öffentliche SSL-Schlüssel im Observatory der EFF entdeckt hatten (SSN 2/2012). Vielleicht hätte die gematik frühzeitig jemanden fragen sollen, der sich auskennt...

Datenschutz-Werkzeugkästen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) NRW hat am 10.01.2024 einen „Werkzeugkasten" für kleine und mittlere Unternehmen veröffentlicht – der sich bei genauer Betrachtung als magere Linksammlung zu Stellungnahmen des LDI und anderer Behörden entpuppt. Dass und wie es besser geht, zeigen die Landesbeauftragten für Datenschutz aus Bayern und Thüringen, die auf ihren Webseiten zahlreiche Muster und Vorlagen bereitstellen, die Unternehmen an ihre Erfordernisse anpassen können, sowie eine hilfreiche 36-seitige FAQ zur Umsetzung der DSGVO.

Ersatz immaterieller Schäden

Der Europäische Gerichtshof (EuGH) hat am 25.01.2024 entschieden, dass bei einem Verstoß gegen die DSGVO nur derjenige Anspruch auf Schadensersatz hat, der seinen immateriellen Schaden hinreichend plausibel darlegen kann. Nach der Ablehnung einer Bagatellgrenze für immaterielle Schäden durch den EuGH am 14.12.2023 (siehe SSN 11+12/2023) stellen die Richter klar, dass ein rein hypothetisches Risiko einer missbräuchlichen Verwendung durch Unbefugte (z. B. durch eine kurzzeitige Weitergabe personenbezogener Daten an einen Dritten) nicht ausreicht, um einen Schaden wegen des Risikos eines Kontrollverlusts zu begründen.

Zwar bleibt damit die Schadensersatzregelung in Art. 82 DSGVO auslegungsbedürftig. Massenhafte Schadensersatzforderungen von Betroffenen bei kleineren Datenschutz-Verstößen oder -Vorfällen müssen Unternehmen jedoch nicht befürchten.

Secorvo News

Teamzuwachs

Seit dem 11.12.2023 verstärkt der Volljurist und Datenschutz-Experte Robert Eitel, LL.M. (VCI) unser Team. Herzlich willkommen!

Vorträge

Auf der 31. DFN-Konferenz "Sicherheit in vernetzten Systemen" (30.-31.01.2024) in Hamburg sprachen Friederike Schellhas-Mende und Christian Blaicher über das Risiko von Auskunftsersuchen für Verantwortliche in Recht und Praxis. Der Beitrag findet sich auch im Tagungsband der Konferenz.

Seminare

Das Frühjahr kündigt nicht nur wieder längere Tage an, sondern auch viele interessante Seminare. Kurz vor Ostern können Sie sich mit unserem T.I.S.P.-Seminar vom **11. bis 15.03.2024** auf die Zertifizierung vorbereiten.

Im April bieten wir die Aufbauschulung zum BSI Vorfall-Experten (**09.–11.04.2024**), das Seminar PKI – Grundlagen, Vertiefung, Realisierung (**15.–18.04.2024**) und die Schulung zum TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) (**22.–25.04.2024**) an.

Weitere Termine und Informationen finden Sie unter www.secorvo.de/seminare. Wir freuen uns auf Ihre Anmeldung!

HackGPT

Was kommt mit dem neuen Hackerspielzeug ChatGPT, FlipperZero & Co auf uns zu? Liefern diese Tools wirklich Anleitungen zum Hacken? Können sie umgekehrt zur Absicherung gegen Cyberangriffe verwendet werden? Und wo liegen die Grenzen solcher Off-the-Shelf-Tools?

Diesen Fragen widmet sich nach einer magischen Einführung durch Dr. Rolf Häcker (Landtag BW) Dr. Swantje Westpfahl (UNISS) beim Jahresauftakt-Event der KA-IT-Si am **22.02.2024**, die auf Einladung der IHK Karlsruhe im Haus der Wirtschaft stattfindet.

Im Anschluss an die Vorträge haben Sie wie immer Gelegenheit zum Networking am Buffet.

Wir freuen uns auf Sie – und empfehlen eine schnelle Anmeldung, denn es gibt nur noch wenige freie Plätze.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2024	
22.02.	Jahresauftaktevent „HackGPT“ (KA-IT-Si, Karlsruhe)
März 2024	
05.-07.03.	secIT 2024 (Heise Medien, Hannover))
11.-15.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-22.03.	DFRWS EU 2024 (DFRWS, Zaragoza/ES)
April 2024	
09.-11.04.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
15.-18.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.04.	Blackhat Asia 2024 (Blackhat, Singapur/ASE)
22.-25.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Fundsache

Nachdem OWASP bereits im Oktober 2023 eine gute Übersicht der wichtigste Angriffstechniken auf LLMs veröffentlichte, bietet das NIST nun mit AI 100-2 E2023 eine detaillierte Systematik möglicher Angriffe und Gegenmaßnahmen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, 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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.