secorvo
security consulting

Secorvo Security News

Mai 2024

Keine Märchen

Märchen leben bekanntermaßen davon, dass sie wiederholt erzählt oder gar aufgeschrieben und im Rahmen mündlicher oder schriftlicher Überlieferung verbreitet werden. Märchen sind gemeinhin frei erfundene Prosatexte, und so verhält es sich auch beim Märchen „Datenschutz kann Leben kosten“, das erst wieder am 07.05.2024 von der Süddeutschen Zeitung publiziert wurde.

Denn Datenschutz kostet keine Leben. Geht es nämlich in lebensbedrohlichen Lagen um eine wie auch immer geartete Verarbeitung von personenbezogenen Daten, dann gilt die dafür in der Datenschutzgrundverordnung vorgesehene Rechtsgrundlage des Art. 6 Abs. 1d – der Schutz lebenswichtiger Interessen Betroffener.

Vielmehr kann Datenschutz Leben retten, wie die Geschichte gezeigt hat: In Ländern, in denen in den Melderegistern die Konfession nicht als personenbezogenes Datum erfasst war, wurden unter der NS-Terrorherrschaft nachweislich weit weniger Juden deportiert und ermordet. Es ist deshalb nicht nur „schade“, sondern schädlich, wenn sich Medien oder auch Personen, die im Licht der Öffentlichkeit stehen, durch Wiederholung von Märchen negativ über den Datenschutz äußern – wie beispielsweise Prof. Dr. Alena Buyx, die Vorsitzende des Deutschen Ethikrats.

Datenschutz ist ein Grundrecht. Als solches dient es dem Schutz der Menschen und schadet ihnen nicht. Datenschutz mag in manchen Fällen vermeintlich lästigen Aufwand produzieren, weil man die gesetzlichen Regelungen einhalten muss. Hier ist es hilfreich und aufwandmindernd, sich genauer mit den Anforderungen des Datenschutzes und deren Zweck zu beschäftigen. Dabei sind, wie bei allen anderen Grundrechten auch, Interessen gegeneinander abzuwägen, Lösungen zu suchen (Risikoabwägung) und Kompromisse zu finden.

Datenschutz ist eine Chance. Und ganz bestimmt kein Lebensrisiko.

Inhalt

secorvo
security consulting

Security News

Behördenbußgelder

Die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert in ihrer Stellungnahme vom 12.04.2024 die Streichung des § 43 Abs. 3 BDSG, der öffentliche Stellen bei Datenschutzverstößen von Bußgeldern befreit. Das Argument im Evaluationsbericht des Bundesministeriums für Inneres und für Heimat, das Bußgeld habe bloß eine Verschiebung von Haushaltsmitteln zur Folge, greife zu kurz: So sei die Verhängung von Bußgeldern nicht nur aus Gründen der Gleichbehandlung von nichtöffentlichen Stellen erforderlich, sondern müsse die Bußgeldbehörde die Schwere eines Verstoßes durch die Bußgeldhöhe verdeutlichen können. Nicht zuletzt fehle die abschreckende Wirkung eines Bußgelds. Das könne der Grund dafür sein, dass Datenschutz bei öffentlichen Stellen oft keinen hohen Stellenwert besitzt.

Ein Beispiel dafür ist der rechtswidrige Betrieb von Facebook-Fanpages durch Bundesministerien und -behörden. Der Bundesbeauftragte für Datenschutz und Informationsfreiheit, Ulrich Kelber, hatte am 20.05.2019 darüber informiert und am 16.06.2021 deren Abschaltung bis Ende 2021 gefordert. Kelbers ausführlich begründete Verwarnung des Bundespresseamts (BPA) vom 17.05.2022 mündete nach einer Anhörung in der Anordnung vom 17.02.2023, die Fanpage des BPA abzuschalten. Sie blieb folgenlos – und wurde mit einer (noch nicht entschiedenen) Klage beim Verwaltungsgericht Köln beantwortet. Unvorstellbar, dass sich ein Unternehmen bei einem ähnlichen Verstoß mehr als fünf Jahre aus der Verantwortung stehlen und sogar wacker weitermachen könnte: So startete das BPA am 08.04.2024 eine Präsenz bei TikTok.

Hängepartien

Am 16.05.2024 wählte der Bundestag nach sechsmonatiger Hängepartie (SSN 1/2024) Frau Prof. Dr. Specht-Riemenschneider zur neuen Bundesdatenschutzbeauftragten. Und in Sachsen-Anhalt wurde am 24.04.2024 mit sogar sechsjähriger Verspätung Maria Christina Rost zur Landesdatenschutzbeauftragten gewählt. Offen ist noch die Nachfolge für die seit Februar 2024 vakante Position der Landesbeauftragten für Datenschutz in Bremen.

Mit solchen Verzögerungen schwächen die Volksvertreter den in einer Demokratie so wichtigen Grundrechtsschutz: Die jährlichen Berichte der Datenschutz-Aufsichtsbehörden belegen, dass sich nur mit wirksamer Kontrolle verhindern lässt, dass das Grundrecht auf Datenschutz wirtschaftlichen oder Überwachungsinteressen geopfert wird.

Every Breath You Take (Stalking I)

Stalkerware ist für Betroffene schwer erkennbar. Schutz vor digitalem Stalking (SSN 3/2024) können die Software TinyCheck von Kaspersky (Source in Github) oder die Abspaltung SpyGuard bieten. Mit beiden Lösungen kann man prüfen, ob ein Smartphone mit Stalkerware infiziert ist: Sie werden als WLAN-Hotspot verbunden und analysieren den Datenverkehr des Smartphones auf verdächtige Muster wie bekannte Domainnamen, IP-Adressen oder Zertifikat-Hashwerte.

Über die Stalkerware „TheTruthSpy“ veröffentlichten Zack Whittaker und das Team von Techcrunch am 20.07.2023 eine lesenswerte Hintergrundanalyse. Sie ergänzten am 12.02.2024 einen Online-Dienst, über den man prüfen kann, ob ein Android Device von der Stalkerware betroffen ist: Er prüft, ob eine angegebene IMEI (International Mobile Equipment Identity) oder Werbe-ID in der im Dezember 2023 an Techcrunch geleakten Liste aller betroffenen Geräte enthalten ist.

Every Move You Make (Stalking II)

Auch einige nützliche Produkte können für Stalking missbraucht werden, wie z. B. Apples AirTags – kleine Ortungsgeräte zum Wiederfinden verlegter Gegenstände, die über Bluetooth mit Apples „Find My“-Netzwerk kommunizieren (SSN 3/2022).

Um das zu verhindern benachrichtigt iOS inzwischen den Nutzer, wenn sich ein fremder AirTag über einen längeren Zeitraum mitbewegt. Für Android stellt Apple eine App bereit, die nach AirTags in der Umgebung scannen kann. Die App AirGuard für Android der Forschungsgruppe Secure Mobile Networking Lab an der TU Darmstadt erkennt neben AirTags auch Alternativprodukte von Samsung, Chipolo und Tile, kann im Hintergrund scannen und umfasst ein Dashboard mit einer Übersicht.

Apple und Google haben 2023 eine gemeinsame Spezifikation erstellt, um AirTag-ähnliche Geräte zu erkennen. Am 13.05.2024 haben Apple und Google nun angekündigt, diese Spezifikation ab iOS 17.5 bzw. Android 6.0 zu unterstützen. Damit warnen zukünftig Smartphone-Betriebssystemdienste herstellerunabhängig vor potentiellen Trackinggeräten.

Windows No-Defender

Das Windows Security Center besitzt eine verborgene Schnittstelle zum Abschalten des Microsoft Defenders. Deren Nutzung ist für Hersteller von Virenscannern vorgesehen, die ein Alternativprodukt zum Defender installieren. Die Produkte von Avast nutzen diese Schnittstelle über einen eigenen Dienst namens wsc_proxy.exe. Am 23.05.2024

veröffentlichte der GitHub Nutzer „es3n1n“ ein Tool, das die Installation eines Virenscanners simuliert und den Windows Defender unter Verwendung des Proxy-Dienstes von Avast deaktiviert.

Die Deaktivierungsschnittstelle wird von Microsoft lediglich durch ein NDA geschützt – ein weiteres Beispiel in der langen Liste offenbar unausrottbarer Versuche von „Security by Obscurity“. Wäre Virenschutz wirkungsvoller, wäre das ein GAU. Wer auf den Windows Defender setzt, sollte wohl gelegentlich prüfen, ob er nicht deaktiviert ist.

Bewährter Code

Am 06.04.2024 veröffentlichte das PuTTY-Team Version 0.81 des verbreiteten Windows-SSH-Clients. Sie schließt eine Sicherheitslücke, deren ursprünglicher Code aus dem Jahr 2001 stammt. Darin wird eine bis zu 512 bit lange Nonce (Einmal-Wert) für DSA- und ECDSA-Signaturen gewählt, die für (damalige) DSA-Schlüssellängen adäquat war, nicht aber für ECDSA-Schlüssel mit der Kurve P-521: Dafür sind es neun Bits zu wenig. Fabian Bäumer und Marcus Brinkmann von der Ruhr-Universität Bochum publizierten am 15.04.2024, dass bereits 60 von PuTTY erzeugte ECDSA-Signaturen genügen, um den privaten Schlüssel bestimmen zu können.

Der Fix wechselt auf das bereits 2013 in RFC 6979 beschriebene Verfahren für die Nonce-Generierung. Das hätte das PuTTY-Team spätestens 2017 machen sollen, als es mit der Version 0.68 die Unterstützung des ECDSA-Verfahrens ergänzte.

Der Fall erinnert an die Explosion der ersten Ariane 5 vor 28 Jahren. Ursache war damals ein Integer-Überlauf aufgrund der höheren Geschwindigkeit der Rakete: Die Software war für die Ariane 4 entwickelt und unverändert übernommen worden.

Fehler dieser Art haben zur Entwicklung von Design by Contract geführt. Dabei werden Zusicherungen explizit vereinbart. Damit hätte auch bei PuTTY der Fehler früher bemerkt werden können. Ein kleines, unbezahltes Entwicklerteam stößt bei solchen (berechtigten) Anforderungen jedoch schnell an seine Grenzen.

Secorvo News

Seminare

Wissen verleiht Macht – oder wenigstens ein Zertifikat. Das T.I.S.P.-Seminar vom **24. bis 28.06.2024** bereitet Sie intensiv und fundiert auf die anschließende Zertifikatsprüfung vor. Unser offizielles Begleitbuch zum T.I.S.P. erhalten Sie direkt nach Ihrer Anmeldung. Noch gibt es freie Plätze.

Planen Sie bereits Ihre Weiterbildung für das zweite Halbjahr? Dann werfen Sie doch einen Blick in unseren Seminarkalender. Der Seminarkompass gibt Ihnen einen Überblick über das Seminarangebot.

Was ko$tet die Welt?

Cybercrime-Statistiken, die überall zitiert und gerne zur Begründung von Maßnahmen und Regulierungen herangezogen werden, jonglieren mit Schadenssummen in luftigen Höhen: Milliarden, Billionen, Trilliarden... Allein: Die Quellen sind oft ungewiss.

Am **20.06.2024** um 18 Uhr gehen Wiebke Reimer und Dr. Boris Hemkemeier (Commerzbank) diesen fantastischen Zahlen auf den Grund: Wo kommen sie her? Sind sie fundiert - oder frei erfunden? Worauf kann man sich stützen und was darf man tatsächlich glauben? Was folgt daraus für eine seriöse Risikoabschätzung?

Das KA-IT-Si-Event findet diesmal im Rahmen der FZI-Veranstaltung „Innovativ? Aber sicher“ statt, zu der Sie ebenfalls herzlich eingeladen sind. Sie beginnt um 14 Uhr im House of Living Labs (FZI).

Im Anschluss an den Vortrag erwartet Sie natürlich auch diesmal der Erfahrungsaustausch beim „Buffet-Networking“. Wir freuen uns auf Sie und empfehlen eine baldige Anmeldung.

14. Tag der IT-Sicherheit

Am 18.07.2024 bietet Ihnen der Karlsruher Tag der IT-Sicherheit zum 14. Mal die Möglichkeit, sich über aktuelle IT-Sicherheitsthemen wie AI oder NIS2 und Präventionsmaßnahmen für Unternehmen zu informieren. Lernen Sie interessante IT-Sicherheits-Start-Ups kennen und nutzen Sie in der Network-Pause die Gelegenheit zum Erfahrungsaustausch mit Teilnehmern und Referenten. Wir empfehlen Ihnen – auch für diese Veranstaltung – eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2024	
04.-07.06.	European Identity & Cloud Conference 2024 (KuppingerCole, Berlin)
10.-12.06.	DuD 2024 (COMPUTAS, Berlin)
20.06.	Was ko$tet die Welt? (KA-IT-Si, Karlsruhe)
24.-28.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
24.-28.06.	OWASP 2024 Global AppSec (OWASP Foundation, Lissabon/PT)
Juli 2024	
08.-12.07.	9th IEEE European Symposium on Security and Privacy (IEEE, Wien/AT)
15.-20.07.	PETS 2024 (University of Bristol, Bristol/UK)
18.07.	14. Tag der IT-Sicherheit (CyberForum, IHK, KA-IT-Si, KASTEL, Karlsruhe)
August 2024	
03.-08.08.	Black Hat USA 2024 (Black Hat, Las Vegas/US)

Fundsache

Der Verizon 2024 Data Breach Investigations Report vom 01.05.2024 analysiert über 30.000 Sicherheitsvorfälle aus dem Zeitraum vom 01.11.2022 bis 31.10.2023 und bietet interessante Einsichten über deren häufigste Ursachen (gestohlene Credentials vor Ransomware und Exploits), Motive (Geld, nicht Spionage) und Täter (Organisierte Kriminalität). Lesenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende (Editorial), 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