Secorvo Security News

Juli 2025

Informiert und selbstbestimmt

Nicht erst seit der Corona-Krise verstärkt sich der Eindruck, dass der Staat mehr und mehr in Wirtschaft und Leben eingreift. Der Staat agiert wie „Bulldozer-Eltern“: Er versucht, Bürgerinnen und Bürger vor allem Möglichen zu bewahren, nimmt ihnen Verantwortung ab und beraubt sie dadurch ihrer Freiheit. So teilte die Berliner Beauftragte für den Datenschutz am 27.06.2025 mit, dass die chinesische KI-App DeepSeek rechtswidrig sei, da sie „umfangreiche personenbezogene Daten der Nutzer“ verarbeite. Sie müsse deshalb aus den App-Stores von Apple und Google entfernt werden.

Es ist richtig, dass die App unter die DSGVO fällt und sich daran messen lassen muss. Sofern die Nutzer der App transparent über die Übermittlung, Verarbeitung und Speicherung ihrer Daten in der VR China informiert werden, sollten sie jedoch die Freiheit behalten, dafür eine Einwilligung zu erteilen, wenn sie die Verarbeitung bei der Nutzung des Dienstes in Kauf nehmen wollen.

Nicht wesentlich anders verhält es sich beim Quasi-Verbot des Einsatzes von Microsoft 365 durch die Datenschutzkonferenz vom 24.11.2022 und der Warnung vor der Verwendung des Kaspersky-Virenschutzes durch das BSI am 15.03.2022. Tatsächlich stellen solche behördlichen Verbote und Warnungen nicht nur für die betroffenen Hersteller – als Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb – eine Freiheitsbeschränkung dar, sondern auch für die Nutzer. Unternehmen steht es frei darüber zu entscheiden, mit wem sie ihre Daten teilen und welche Arbeitsmittel sie in ihren Betrieben einsetzen, solange die DSGVO eingehalten wird. Das ist ihre Verantwortung, nicht die des Staates.

Solange es nicht – wie bei kritischen Infrastrukturen – um die Funktionsfähigkeit des Staates oder die demokratische Grund- und Werteordnung geht, gilt (mit Ritchie Norton): „Wenn du dich für Freiheit entscheidest, wählst du auch Verantwortung.“

Security News

Prishing

Am 23.07.2025 beschrieb der IT-Sicherheitsexperte Kyle Parrish, wie er bei einer Red-Team-Übung ungesicherte Multifunktionsdrucker für einen internen Phishing-Angriff nutzte: Er druckte gefälschte Zertifikate über Awareness-Schulungen, die den Namen eines Mitarbeiters aus der einsehbaren Druckhistorie trugen, ein Lob enthielten („6 Monate ohne Phish Failures!“) – sowie einen QR-Code zum Einlösen eines 10$-Gutscheins. Der Code führte jedoch auf eine von Parrish erstellte Seite, die zur Eingabe der Anmeldedaten des Unternehmens aufforderte. Mehrere Perso-

nen scannten den QR-Code, eine gab ihre Anmeldedaten ein. Es gelang Parrish außerdem, die Funktion zur Anzeige von Nachrichten auf dem Druckerbildschirm für die Meldung „Authentifizierung erforderlich, um Druck freizugeben“ zu missbrauchen – und ergänzte sie durch einen QR-Code mit Link zu seiner Phishing-Seite.

In Anlehnung an „Quishing“ (Phishing über QR-Code) oder „Smishing“ (Phishing per SMS) nennt Parrish seine Methode „Prishing“ – eine Kofferwort aus „Printer“ und „Phishing“. Weil Menschen dazu neigen, Gedrucktem zu vertrauen, kann so die oft mangelhafte Sicherheit der Drucker zum Problem werden. Drucker gehören daher in ein eigenes, abgeschottetes Netzwerksegment.

Nebulöses Interesse

In den SSN 01/2025 haben wir über das Urteil Mousse/CNIL des EuGH vom 09.01.2025 berichtet. Eine bisher wenig beachtete Passage dürfte größere Auswirkungen auf diejenigen haben, die personenbezogene Daten aufgrund eines berechtigten Interesses verarbeiten: Stützt man Verarbeitungen auf Art. 6 Abs. 1 lit. f DSGVO, muss man den betroffenen Personen das verfolgte berechtigte Interesse unmittelbar bei der Datenerhebung darlegen. Informiert man nicht, gibt es auch keine Rechtsgrundlage für die Verarbeitung. Das kann als DSGVO-Verstoß teuer werden.

Die Formulierung „die Verarbeitung erfolgt aufgrund unseres berechtigten Interesses“ reicht dafür nicht aus; das Interesse muss konkret benannt und es muss verständlich informiert werden. Zahlreiche Datenschutzerklärungen auf Webseiten genügen diesen Anforderungen nicht. Die Korrektur sollte man besser nicht so lange aufschieben, bis die Aufsichtsbehörden die Erklärungen automatisiert prüfen.

Schwachstelle Praktikant

Am 15.06.2025 begann in Lyon der Prozess gegen eine Gruppe junger Betrüger, die beim Personaldienstleister Adecco eine Datenbank mit den Daten von ca. 70.000 Leiharbeitnehmern missbraucht hatten. Sie erstellten falsche Ausweispapiere, betrogen staatliche Hilfsprogramme und buchten von den Konten der Betroffenen jeweils 49,85 € ab – ein Betrag gerade unterhalb des Schwellenwerts, der eine Prüfung durch die Bank ausgelöst hätte. In nur vier Tagen sammelten sie so von 32.000 Konten insgesamt 1,6 Mio. € ein.

Der Coup gelang, weil ein Auszubildender seine persönlichen Zugangsdaten zur Datenbank über das Darknet verkauft hatte – für 15.000 €, die er angeblich nie erhielt. Technische Details des Angriffs wurden nicht veröffentlicht, doch zweifellos wäre das kriminelle Geschäft nicht zustande gekommen, wenn die Anmeldung eine Smartcard oder einen FIDO-Key erfordert hätte.

David gegen Goliath

Am 04.07.2025 hat das LG Leipzig die Meta Inc. zur Zahlung einer Entschädigung in Höhe von 5.000 € wegen der rechtswidrigen Verarbeitung von Nutzerdaten durch die Business Tools verurteilt. Erst am 18.11.2024

hatte der BGH wegen Scrapings lediglich 100 € Schadenersatz zugesprochen. Das LG Leipzig begründet die Höhe des Schadensersatzanspruchs mit dem großen Nutzen der Daten für Meta, die es durch den Einsatz der Business Tools erhält und in deren Verarbeitung der Kläger nicht eingewilligt hatte. Das Gericht stützt sich zur Höhe des Schadensersatzanspruchs auch auf die Rechtsprechung des EuGH, des OLG Dresden und des Bundeskartellamts. Damit dürften die Rahmenbedingungen für eine Sammel- oder Verbandsklage gleichartiger Ansprüche und einer größeren Anzahl Betroffener gegeben sein. Das wird zweifellos einige Betroffene bzw. die Verbraucherverbände ermutigen, auch gerichtlich gegen Meta vorzugehen, sofern die Entscheidung des LG Leipzig nicht durch höhere Instanzen aufgehoben wird.

Wie man sich bettet...

Am 30.06.2025 hat die Bundesbeauftragte für den Datenschutz mitgeteilt, dass sie Webseiten des Bundes automatisiert auf die datenschutzkonforme Einbettung von Youtube-Videos überprüft hat. Dabei wurden insgesamt 40 datenschutzwidrige Einbettungen festgestellt. Das Ergebnis sollte auch nicht-öffentliche Stellen veranlassen zu prüfen, wie Videos auf den eigenen Webseiten eingebunden sind: Wird das Video nicht selbst gehostet, muss eine wirksame Einwilligung (freiwillig, informiert, Zwei-Klick-Lösung) in die Verarbeitung bspw. durch Youtube eingeholt werden. Das Fehlen einer Einwilligung ist ein Verstoß gegen das TDDDG.

Entsprechende Prüfungen der Aufsichtsbehörden für den nicht-öffentlichen Bereich wurden bereits angekündigt.

Volatility für macOS und Linux

Version 2.8.0 des Open-Source-Werkzeugs Volatility 3 bot für die forensische Analyse des Hauptspeichers unter Windows bereits zahlreiche Plugins; die Möglichkeiten für Linux- und macOS-Systeme waren bislang allerdings stark beschränkt.

Die am 16.05.2025 veröffentlichte Version 2.26.0 schließt diese Lücke. Zwar ist die Anzahl der Plugins insgesamt kleiner, doch die verfügbaren Module besitzen eine deutlich größere funktionale Tiefe und Breite. So werden zahlreiche Linux-Kernels (bspw. Debian, Ubuntu, AlmaLinux) und MacOS-Versionen (10.6 bis 15.1) unterstützt.

Als Reaktion auf moderne Angriffsmethoden wie das Manipulieren von Systemaufrufen oder das Löschen von PE-Dateien aus dem Dateisystem gibt es mit processghosting, unhooked_system_calls und etwpatch neue Module für Windows. Einige bekannte Plugins wie cachedump oder hashdump werden nur noch eingeschränkt unterstützt.

Apps vom Flohmarkt

Am 10.07.2025 meldete Kaspersky über Securelist Schadcode auf dem Marktplatz von Cursor AI. Dort war eine manipulierte Version der „Solidity Language Extension“ hochgeladen worden. Überraschend dabei: Die App erzielte durch zeitlich geschicktes Hochladen

und gefälschte Bewertungen eine bessere Platzierung als das Original. Ähnliche Angriffe gab es bereits auf VS-Code-Erweiterungen und mehrere NPM-Pakete, die auf die Entwickler von Blockchain-Anwendungen zielten.

Auch Apple und Google kämpfen regelmäßig gegen Schadsoftware in ihren Stores, wie Kaspersky am 13.02.2025 berichtete. Diese Fälle zeigen, wie schwierig die Kontrolle für Betreiber großer Marktplätze ist. Solche Plattformen funktionieren wie Flohmärkte: Viele Anbieter stellen ihre Software ein, Betreiber sortieren nach Hinweisen schwarze Schafe aus, prüfen vor der Listung aber nur oberflächlich. Umfangreiche Sicherheitschecks sind wegen der großen Zahl an neuen Apps unmöglich. Vor allem Entwickler sollten daher fremden Programmpaketen nie blind vertrauen.

Secorvo News

Secorvo Seminare

Haben Sie noch Weiterbildungspläne für 2025? Dann werfen Sie doch einen Blick auf unsere Seminare im Herbst. Die Autoren des T.I.S.P.-Buchs bereiten Sie vom **22. bis 26.09.2025** auf die T.I.S.P.-Zertifizierung vor. Im Ernstfall die Nerven und den Überblick bewahren? Als Vorfall-Experte (BSI) sind Sie für den Worst Case gewappnet. Das nächste Seminar findet vom **14. bis 16.10.2025** statt. IT Security Insights am **07. und 08.10.2025** bietet aktuelle Themen für IT-Sicherheitsverantwortliche aus der Praxis. Alle Seminare sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (zur Anmeldung).

Teamzuwachs

Am 15.07.2025 hat Vera Kuhlmann das Seminarmanagement übernommen und betreut jetzt zusammen mit Susanne Cussler unsere Veranstaltungen. Herzlich willkommen!

Neues Heim

Nach 20 Jahren in der Ettlinger Straße ziehen wir in rund 500 m entfernte, wunderschöne denkmalgeschützte Räume direkt gegenüber dem Karlsruher Hauptbahnhof. Dort erreichen Sie uns ab dem 14.08.2025 unter der Adresse Bahnhofplatz 8 – vielleicht bei Ihrem nächsten Besuch in Karlsruhe?

Wer die Wahl hat...

Wahlen und Abstimmungen – in Vereinen, Organisationen, Gemeinden, Land und Bund – sind organisatorische und manchmal auch logistische Herausforderungen. Was liegt da näher, als sie zu „digitalisieren"? Bei unserem nächsten KA-IT-Si-Event am **23.10.2025** beleuchtet Frau Professorin Melanie Volkamer (Secuso, KIT) die Sicherheitsanforderungen an Internet-Wahlen und -Abstimmungen, stellt praktische Beispiele vor und diskutiert die Vor- und Nachteile ihres Einsatzes. Anschließend erwartet Sie der Erfahrungsaustausch beim „Buffet-Networking". Wir freuen uns darauf, Sie in der „Church" des CyberForum zu sehen – und empfehlen, wie immer, eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2025	
02.-07.08.	Black Hat USA 2025 (Black Hat, Las Vegas/US)
04.-06.08.	IEEE CSR 2025 (IEEE, LogosRI, Chania/GR)
07.-10.08.	Defcon 33 (DEF CON Communications, Las Vegas/US)
10.-12.08.	SOUPS 2025 (usenix, Seattle/US)
11.-12.08.	SAC Summer School (IACR, Toronto/CA)
13.-15.08.	Selected Areas in Cryptography 2025 (IACR, Toronto/CA)
13.-15.08.	34th USENIX Security Symposium (usenix, Seattle/US)
17.-21.08.	Crypto 2025 (IACR, Santa Barbara/US)
September 2025	
04.09.	Cloud Identity Summit (Azure Meetup Bonn Team, Dortmund
10.-11.09.	secIT digital (Heise, virtuell)
14.-18.09.	CHES 2025 (IACR, Kuala Lumpur/MY)
22.-26.09.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)

Fundsache

Sichere Softwareentwicklung wird immer wichtiger. Wie man auch gleich noch datenschutzkonforme Software entwickelt, zeigt die CNIL in ihren Empfehlungen insbesondere für mobile Apps.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza, Paul Blenderman, Kai Jendrian, Dr. Alexander Koch, Oliver Oettinger, Friederike Schellhas-Mende (Editorial), Jochen Schlichting, Liza Trace, Julian Wahl

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Bahnhofplatz 8
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