Secorvo Security News

Oktober 2026



„Kreative“ KIs?

In den zurückliegenden Monaten haben KI-Systeme zahlreiche bislang offene mathematische Fragestellungen gelöst. Einige Beweise gelangen durch die Konstruktion eines Gegenbeispiels: Dass das mit hoher Rechenleistung möglich ist, ist nicht verwunderlich. Beeindruckender sind die direkten Beweise, wie der der Erdös-Sós-Vermutung (1963): Die elegante, auf eine Tafel passende Beweisführung fand GPT-6 im September 2026.

Dass LLMs gute Sprach- und damit auch Programmiermaschinen sind, ist wenig verwunderlich – dafür sind sie gemacht. Mittlerweile haben sie aber auch Erfolg in Bereichen, die wir „kreativ“ nennen und daher als inhärent menschliche Domäne verstehen. Wie sollen wir damit umgehen?

KIs werden uns in immer mehr Tätigkeiten überflügeln, die sich formalisieren, analysieren und argumentativ bearbeiten lassen – so auch in Rechtsfragen oder philosophischen Diskussionen. Schach- und Go-Computern ist das schon vor dem Durchbruch von LLMs gelungen. Solche Tätigkeiten sind eine Herausforderung für den menschlichen Intellekt – aber sind sie tatsächlich „kreativ“? Vielleicht müssen wir einsehen, dass menschliche Kreativität nie etwas Abstraktes ist, sondern sich wesentlich aus der individuellen Erfahrung und Emotionalität eines Künstlers speist. Wenn hinter einem Werk kein erlebendes, emotionales Subjekt mehr steht, werden dann Literatur, Malerei, Musik oder Poesie noch dieselbe Bedeutung für uns haben?

Die technische Sicherheitsanalyse von Software und Infrastrukturen, vielleicht sogar die Entwicklung und Analyse von kryptografischen Verfahren und Protokollen werden wir künftig KIs überlassen können. Wenn es allerdings um die Bewertung von Risiken, die Übernahme von Verantwortung oder die Überzeugung von Mitarbeitern zur Einhaltung von Sicherheitsregeln geht, bleibt der Mensch unverzichtbar. Denn „Werte“ und „Verantwortung“ sind für ein LLM nur Begriffe. Wenn es dagegen verstößt, hat es nichts zu verlieren.

Security News

Nur ein Beispiel…

Am 10.09.2026 schilderte Simon Weber von Machine Spirits gegenüber heise online, wie sein Team im Frühjahr schwere Sicherheitslücken (CVSS bis 9.1, critical) in drei quelloffenen Clients (von fbeta, Oviva und Med United) für die elektronische Patientenakte (ePA) fand. Ein Angreifer hätte Gesundheitsdaten mitlesen oder bei der Übertragung verändern können. Alle gefundenen Lücken sind mittlerweile geschlossen, Angriffe sind nicht bekannt.

Die von der gematik bereitgestellte Beispielbibliothek lib-vau für den Kanal zum Aktensystem führt nur zwei von sechs vorgeschriebenen Serverprüfungen aus. Med United übernahm diese Bibliothek, ohne die fehlenden Prüfungen zu ergänzen. Oviva baute die Prüfung selbst zwar nach, verwarf aber das Ergebnis. Zwar erwähnt die Dokumentation der lib-vua fehlende Zertifikatsprüfungen; ausdrücklich abgeraten vom Produktiveinsatz hat die gematik aber erst nach Meldung der Lücken am 21.05.2026.

Wer Beispielcode übernimmt, übernimmt auch dessen Schwachstellen. Sicherheit gehört deshalb von Beginn an in Entwurf, Code und Tests. Wer digitale Gesundheitsanwendungen entwickelt, muss schon heute Informationssicherheit, Verifizierung und Validierung berücksichtigen (Anhang I Nr. 17.2 der Medizinprodukteverordnung). Ab 11.12.2027 fordert der Cyber Resilience Act (CRA) für fast alle anderen Produkte mit digitalen Elementen Security by Design (Art. 13 Abs. 1) und Sorgfalt bei Fremdkomponenten (Art. 13 Abs. 5). Darauf bereiten wir in unserem T.P.S.S.E.-Seminar vor.

Echte Daten, falsches Vertrauen

Am 21.10.2026 hat die EU-Kommission ein Verfahren gegen Booking.com wegen eines möglichen Verstoßes gegen das Gesetz über digitale Dienste eingeleitet. Schon im Frühjahr und Sommer gab es Hackerangriffe auf Schnittstellen von Buchungssystemen zu Booking.com, bei denen Buchungsdaten (Unterkunft, genauer Reisezeitraum etc.) erbeutet wurden. Immer mehr Gäste erhalten seitdem – vor allem via WhatsApp – Phishing-Nachrichten, in denen die Buchungsdaten als Vertrauensanker missbraucht werden. Dadurch steigen die Chancen der Angreifer, tatsächlich Zahlungsdaten zu erhalten. Auch die Datenschutzaufsichtsbehörden warnen bereits vor solchen Nachrichten.

Auch wenn einzelne Angaben in (Phishing-)Nachrichten stimmen, sollten Empfänger bei finanziellen Forderungen zunächst direkten Kontakt zur Unterkunft aufnehmen – und erst zahlen, wenn sie den Absender und die Korrektheit der Forderung geprüft haben.

Vier gewinnt

Am 17.10.2026 meldete der Sicherheitsforscher „Wayne“, dass sich die privaten Schlüssel von acht in der Common CA Database (CCADB) der Browser-Hersteller gelisteten CA-Zertifikate trivial rekonstruieren lassen: Statt 384 zufälliger Bit, wie es die elliptische Kurve „P-384“ vorsieht, hatten sie höchstens 8 Bit; der kleinste war die „Zufallszahl“ 4.

Nach Angaben der betroffenen CA eMudhra Ltd. in einem Bugzilla-Ticket seien die Schlüsselpaare am 30.04.2025 in einem zertifizierten Hardware Security Module (HSM) erzeugt worden. Ein Fehler beim anschließenden Test von verschlüsseltem Export und Re-Import habe zusätzlich die unsicheren Schlüsselpaare erzeugt, die man irrtümlich für Zertifikatsanträge verwendet habe.

Diese Darstellung prüft derzeit die KPMG. Sie wirft kein gutes Licht auf eMudhras PKI-Betrieb: Das zweite Schlüsselpaar hätte spätestens im Juni 2025 auffallen können, als ungültige Sperrlisten-Signaturen gemel-

det wurden, die mit den Original-Schlüsseln erzeugt worden waren: Sie passten nicht zu den unsicheren Schlüsseln in den Zertifikaten. eMudhra signierte sie mit letzteren neu, ohne die Ursache zu erkennen (siehe die Antwort auf Frage Q8).

eMudhra steigt nun aus dem Geschäft mit öffentlichen TLS-Zertifikaten aus. Nutzer aktueller Browser sind geschützt: Die CA-Zertifikate sind gesperrt, Mozilla und Chrome haben zudem der Root-CA das Vertrauen entzogen. Vorsicht ist bei Software mit veraltetem CA-Bündel ohne Sperrinformationen geboten (Testseite). Inzwischen prüft Chrome alle in der CCADB offengelegten CA-Zertifikate automatisiert auf schwache Schlüssel. Im CA/Browser Forum wird diskutiert, diese Prüfung ab 2027 auch für CAs verpflichtend zu machen und die Regeln für die Schlüsselerzeugung zu verschärfen.

Team: Toll, ein anderer machts

Die norwegische Datenschutzbehörde Datatilsynet verhängte am 12.10.2026 gegen den zu Microsoft gehörenden Werbeanbieter Xandr ein Bußgeld in Höhe von 8,6 Mio. €. Xandr war an der automatisierten Vermarktung von Werbeflächen der Dating-App Grindr beteiligt. Die Behörde stufte bereits die Information, dass eine Person Grindr nutzt, als besonders schützenswertes personenbezogenes Datum ein. Für die Verarbeitung solcher Daten gelten strenge Anforderungen an die ausdrückliche Einwilligung.

Die Datenschutzkonferenz hat diese in ihrem aktualisierten Kurzpapier Nr. 20 zusammengefasst (siehe SSN 9/2026).

Die Datenschutzbehörde sah Grindr und Xandr in der gemeinsamen Verantwortung für die Verarbeitung. Daher müsse Xandr selbst sicherstellen, dass die erteilten Einwilligungen auch die Datenverarbeitung abdecken, die Xandr zu eigenen Zwecken vornimmt. Die von Grindr eingeholte Einwilligung schloss diese nicht ein. Die Verantwortung für die eigene Verarbeitung lässt sich eben nicht auf andere abwälzen.

Registrarmacht

Am 06.10.2026 veröffentlichte Google in seinem Security Blog, dass Angreifer die Registry-Betreiber der Top-Level-Domains von Ghana, Sierra Leone und Amerikanisch-Samoa kompromittieren konnten. Sie erschlichen sich darüber gültige TLS-Server-Zertifikate für Webseiten namhafter Organisationen, wie google.as.

Die Zertifizierungsstellen gehen davon aus, dass nur der Domäneninhaber Kontrolle über seinen DNS-Bereich hat. Ein Registry-Betreiber hat aber natürlich dieselben Möglichkeiten. Besonders perfide: Die klassische Schutzmaßnahme gegen falsche Zertifikatsausstellung, CAA mit DNSSEC und ACME-Accountbindung (SSN 06/2026), greift hier nicht: Ein kompromittierter Registry-Betreiber kann alle DNS-basierten Schutzmechanismen umgehen, indem er die Einträge selbst anpasst. Auch Registrar- und Registry-Locks sind in diesem Fall wirkungslos. Dennoch sollte man nach Wiedergewinnung der Kontrolle über das DNS eine ACME-Accountbindung konfigurieren, um vom Angreifer via

ACME erhaltene, noch gültige Zertifikate und Nachweise zu invalidieren.

Eine andere Schutzmaßnahme, Certification Transparency Logging, greift aber weiterhin: Alle gängigen Browser fordern inzwischen, dass ausgestellte Zertifikate in öffentlichen Logs publiziert werden. Unternehmen sollten in diesen Logs automatisiert nach Zertifikaten für ihre Domäne suchen, um damit solche fälschlich ausgestellten Zertifikate zu erkennen und sperren zu lassen.

Nicht jedes Anonym ist anonym

Das Gesundheitsforschungsunternehmen IQVIA Solutions Italy S.r.l. bot gemeinsam mit der italienischen Gesellschaft für Allgemeinmedizin (SIMG) rund 800 hausärztlichen Praxen eine kostenlose Lizenz für ihre Praxissoftware an. Im Gegenzug mussten diese regelmäßig anonymisierte Patientendaten an IQVIA übermitteln. Das Unternehmen fasste diese Daten zusammen und nutzte sie für Beobachtungsstudien und medizinische Auswertungen. Doch die vermeintlich anonymen Daten waren nicht immer anonym. Die SIMG entdeckte in gut 3.000 Datensätzen Angaben, anhand derer sich einzelne Personen unmittelbar identifizieren ließen. So waren vor allem Freitextfelder bei der Anonymisierung unverändert übernommen worden.

Bei der Prüfung durch die italienische Datenschutzaufsichtsbehörde Garante Privacy berief sich IQVIA auf den relativen Personenbezug: Zwar könnten die behandelnden Ärzte ihre Patienten anhand der Daten identifizieren; für IQVIA seien die Daten jedoch anonym. Die Aufsichtsbehörde erkannte diesen Grundsatz an, ließ ihn aber nicht als Entlastung gelten.

IQVIA war maßgeblich an der Datenverarbeitung beteiligt und damit kein unbeteiligter Empfänger. Das Unternehmen hätte deshalb die Wirksamkeit der Anonymisierung sorgfältig prüfen müssen. Stattdessen hatte es pseudonymisierte Daten ohne gültige Rechtsgrundlage verarbeitet. Zudem fehlten eine ausreichende Information der betroffenen Personen, eine Datenschutz-Folgenabschätzung und ein Löschkonzept. Am 02.10.2026 erging ein Bußgeldbescheid an IQVIA über 7 Mio. €: Pseudonymität genügt für die Befreiung von den Pflichten der DSGVO nicht.

Secorvo News

Little brother is watching you

Wie Personen über die von WLAN-Access-Points ausgesandten WLAN-Signalen erkannt werden können, stellt Dr. Thorsten Strufe, Professor für IT-Sicherheit am KIT und Honorarprofessor für Datenschutz und Netzwerksicherheit an der TU Dresden auf dem letzten diesjährigen KA-IT-Si-Event am **03.12.2026** vor.

Mit seiner Forschungsgruppe ist es ihm gelungen, die unverschlüsselte Beamforming Feedback Information (BFI), mit denen Router die WLAN-Übertragung optimieren, für die Identifikation und Wiedererkennung von Menschen zu missbrauchen. Diese Untersuchungen haben im vergangenen Jahr große öffentliche Resonanz hervorgerufen.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Hier geht es zur Anmeldung.

Seminare 2027

Auch im kommenden Jahr bieten wir Ihnen praxisnahe Schulungen und fundiertes Expertenwissen rund um die Informations- und IT-Sicherheit. Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz.

November 2026	
10.-11.11.	T.I.S.P./T.P.S.S.E. Community Meeting (TeleTrusT, Berlin)
10.-12.11.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
15.-19.11.	ACM CSS 2026 (ACM SIGSAC, Den Haag/NL)
16.-20.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-26.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-25.11.	13. DFN-Konferenz Datenschutz (DFN-CERT, Hamburg)
Dezember 2026	
02.12.	secIT Thementag (heise, virtuell)
03.12.	KA-IT-Si-Event „Little brother is watching you" (KA-IT-Si, Karlsruhe)
03.-04.12.	10th CSCML 2026 (IACR, CSCML, Beer-Sheva/IL)
07.-10.12.	Black Hat Europe 2026 (Blackhat, London/UK)
07.-11.12.	Asiacrypt 2026 (IACR, Hongkong/CN)
08.12.	IT Sicherheitsrechtstag NRW (IHK NRW, Duisburg)

Fundsache

Ein sehr übersichtlich gestalteter Leitfaden zum Thema Löschen findet sich auf der Webseite des Landesdatenschutzbeauftragte von Sachsen-Anhalt.

Impressum

Secorvo Security News – ISSN 1613-4311

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

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

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.