Secorvo Security News

Oktober 2025

Alter Wein, neue Schläuche…

Seit drei Jahren diskutiert die EU über die Einführung einer „Chatkontrolle“ – eine Neuauflage der „Kryptodebatte“ der 90er Jahre. Führende Kryptologen warnten damals überzeugend vor den Risiken von Key Escrow und Key Recovery. Weder in den USA noch in Europa kam es zu Beschränkungen von Verschlüsselungslösungen, doch die Debatte riss nicht ab. 2015 nahmen die Autoren daher erneut Stellung.

Um die Verbreitung von Darstellungen sexualisierter Gewalt gegen Kinder zu bekämpfen, sollen Kommunikationsdienste in der EU verpflichtet werden, private Nachrichten auf verdächtige Inhalte zu durchsuchen. Technisch lässt sich eine solche Chatkontrolle ohne Kryptoverbot nur erreichen, wenn Inhalte auf den Endgeräten der Nutzer überprüft werden, bevor sie verschlüsselt sind. Faktisch wäre dies das Ende einer dem vertraulichen Gespräch entsprechenden Kommunikationsform, von dem auch Berufsgruppen wie Journalisten und Anwälte betroffen wären.

Problematisch sind die grundrechtlichen Implikationen einer solchen Maßnahme: Eine anlasslose Überwachung widerspricht fundamentalen europäischen Rechtsprinzipien wie der Unschuldsvermutung, dem Recht auf Achtung der persönlichen Korrespondenz (Art. 8 der Europäischen Menschenrechtskonvention) und dem in Deutschland in Art. 10 Grundgesetz geschützten Telekommunikationsgeheimnis. Sie widerspricht auch der vom EuGH betonten Notwendigkeit der Verhältnismäßigkeit staatlicher Eingriffe in die Privatsphäre.

Kein Zweck, so legitim er sein mag, heiligt jedes Mittel. Eine punktuelle Verbesserung des unzweifelhaft wichtigen Schutzes von Kindern vor Missbrauch darf daher nicht mit anlassloser Massenüberwachung erkauft werden. Die Diskussion wirft eine Grundfrage europäischer Rechtskultur auf: Soll Sicherheit durch den Abbau von Freiheit erkauft werden? Eine EU, die ihre Werte ernst nimmt, muss Wege finden, beides zu schützen – die Sicherheit der Schwächsten ebenso wie die Freiheit aller.

Security News

Zündende Stromquelle

Im zentralen Data Center des National Information Resources Service von Südkorea verursachten am 26.09.2025 Lithium-Ionen-Batterien einen Brand, der über 600 digitale Regierungsdienste lahmlegte und 858 TB Daten vernichtete. Der Vorfall zeigt die Risiken moderner Energieversorgungssysteme: Während USV-Anlagen häufig Blei-Säure-Batterien nutzen, bieten Lithium-Ionen-Batterien durch ihre kompakte

Bauweise Platzvorteile, bergen jedoch ein höheres Brandrisiko. Sie können durch Stöße (thermische Verletzung) oder unsachgemäße Handhabung, etwa einem Vertauschen der Pole, beschädigt werden.

Die Lieferkette der verwendeten Lithium-Ionen-Akkus und seiner Komponenten ist ebenfalls von Bedeutung, denn sie werden zumeist als OEM-Bauteil in USV-Anlagen eingebaut. Weltweit gibt es nur wenige Lieferanten; außerdem sollte bei der Risikoanalyse nicht übersehen werden, dass die Akkusysteme von eingebetteter Software gesteuert werden – dem Battery Management System (BMS). Diese Software sichert die physische Einsatzfähigkeit, übernimmt Zell-Balancing (Ladungsverteilung) und steuert Schutzfunktionen wie Überspannung und Übertemperatur.

In Südkorea wurden zwischen 2018 und 2022 insgesamt 55 USV-Brände registriert; einer davon traf bereits 2022 ein Data Center – nicht auszuschließen, dass einige der Vorfälle extern ausgelöst wurden. Das sollte man nicht unberücksichtigt lassen – zumal in Deutschland die nationale Stromspeicherstrategie gerade mit genau dieser Technik ausgebaut wird.

Alte neue Schwachstellen

Die US-Cybersicherheitsbehörde CISA hat Anfang Oktober 2025 zwölf neue Sicherheitslücken (CVEs) in ihren Known Exploited Vulnerabilities (KEV)-Katalog aufgenommen (siehe SSN 6/2025). Besonders alarmierend: Ein Teil der neuen Einträge stammt aus dem Jahr 2017 oder früher. Das zeigt, dass selbst über zehn Jahre alte Sicherheitslücken weiterhin erfolgreich für Angriffe genutzt werden – weil viele Systeme offenbar jahrelang ungepatcht und damit verwundbar betrieben werden.

Veraltete Software und unzureichendes Schwachstellenmanagement laden Cyberkriminelle ein wie eine offene Balkontüre den Einbrecher. Die oft als „unvermeidbar" dargestellte Nutzung veralteter Systeme sollte von den verantwortlichen CISOs und ISBs kritisch hinterfragt werden – in der Regel wiegt der unsichere Betrieb das Risiko nicht auf.

Timm Thaler lässt grüßen

Am 22.10.2025 wies der hessische Landesdatenschutzbeauftragte darauf hin, dass LinkedIn ab dem 03.11.2025 die Daten von Nutzerinnen und Nutzern für das Training seiner KI-Modelle nutzt, ohne deren Zustimmung einzuholen. Damit folgt das Karriere-Netzwerk den schlechten Vorbildern von Meta, TikTok, Google, Amazon, eBay, X und anderen. Sie alle füttern ihre KIs mit Daten ihrer Nutzer: öffentlichen Posts, Bildern, Sprachdaten, Kaufverhalten etc. Verhindern können Nutzer dies nur, indem sie selbst aktiv werden und in den Einstellungen widersprechen – dann werden zumindest weniger Daten gesammelt.

Wer keine Einwände gegen die Verwendung seiner Daten hat, sollte sie wenigstens nur gegen Entgelt weitergeben. Die App Neon etwa bietet ihren Nutzern bis zu 30 US$ am Tag, wenn sie Sprachdaten aus Telefonaten Neon zum Weiterverkauf zur Verfügung stellen. In Deutschland sind allerdings die Vertraulichkeit des gesprochenen Wortes (§ 201 StGB) und die Regelungen der DSGVO zu beachten: Eine solche Nutzung ist

daher nur zulässig, wenn alle Gesprächspartner wirksam einwilligen und die Weitergabe der Daten transparent im Einklang mit der DSGVO erfolgt.

Security is Not My Problem

Am 24.09.2025 hat Cisco für die auf ihren Switches und Routern verwendeten Betriebssysteme IOS und IOS XE Patches veröffentlicht. Diese beheben eine Schwachstelle im Subsystem für das Simple Network Management Protocol (SNMP), dessen Akronym auch spöttisch als „Security is Not My Problem" interpretiert wird.

In den SSN berichten wir regelmäßig (siehe z. B. SSN 12/2024) über Schwachstellen in Netzwerkgeräten. Meist betreffen sie die webbasierte Administrationsoberfläche. Dabei gerät oft in Vergessenheit, dass es noch andere Admin-Schnittstellen gibt – wie z. B. SNMP. Der Zugriff auf Administrationsschnittstellen sollte grundsätzlich auf die Quelladressen der dafür vorgesehenen Systeme beschränkt werden. Das gilt nicht nur für Webschnittstellen, sondern auch für SSH- und SNMP-Zugänge.

Außerdem sollten veraltete Protokollversionen wie SNMPv1 und SNMPv2 nicht mehr eingesetzt werden – sie bieten keine adäquaten Schutzmechanismen.

Totgesagte leben länger

Microsoft hat den Internet Explorer (IE) durch den Browser Edge ersetzt und den IE im Juni 2022 offiziell für tot erklärt. Ein Teil seines Codes lebt jedoch weiter – z. B. im IE-Modus des Edge-Browsers. Dieser wird von IT-Abteilungen genutzt, um alte Intranet-Anwendungen weiter nutzen zu können. Dafür lassen sich beispielsweise per Gruppenrichtlinie einzelne URLs festlegen, die im IE-Modus geöffnet werden sollen.

Außerdem ließ sich im Edge eine Webseite auf Knopfdruck im IE-Modus zu öffnen – bis Angreifer im August begannen, Benutzer zu verleiten, diesen Knopf zu betätigen, um Schwachstellen im veralteten Code auszunutzen. Microsoft hat daraufhin die Funktion in privaten Installationen abgeschaltet.

IT-Abteilungen müssen selbst aktiv werden – sofern sie die Option nicht schon längst per Gruppenrichtlinie deaktiviert haben. Wie das geht, hat das Edge-Team am 08.10.2025 in einem Blogartikel detailliert beschrieben. Unterstützt wird der IE-Code im Edge-Browser mindestens bis 2029. Wahrscheinlich auch, weil Microsoft ihn nicht ohne Weiteres aus Windows entfernen kann: Zahlreiche WindowsFunktionen greifen weiterhin vielleicht darauf zurück...

Intransparente Zertifikate

Cloudflare, das einen DNS-Dienst mit der IP-Adresse 1.1.1.1 betreibt, berichtete am 04.09.2025 von Zertifikaten, die die kroatische Zertifizierungsstelle (CA) Fina unberechtigt für „1.1.1.1" ausgestellt hatte – eine Abfrage bei crt.sh bestätigt das.

Leider nehmen immer wieder einzelne CAs ihre wichtigste Aufgabe, die Überprüfung der Rechtmäßigkeit des Zertifikatsantrags, nicht mit der nötigen Sorgfalt wahr. Daher hat Google 2013 Certificate Transparency

(CT) eingeführt. Dabei prüfen Browser, ob die Ausstellung eines Zertifikats in einem revisionssicheren öffentlichen Register protokolliert wurde. Außerdem können Domäneninhaber darüber feststellen, wenn eine CA unberechtigt Zertifikate für ihre Domänen ausstellt.

Cloudflare hat nach eigenem Bekunden die CT-Logs für ihre Domänen überwacht. Der Fall zeigt, dass auch eigene IP-Adressen dabei berücksichtigt werden müssen – insbesondere, wenn darüber (wie bei Cloudflare) auch TLS-gesicherte Dienste wie DNS over HTTPS laufen.

Ansichtssache

Schon am 04.09.2025 hat der EuGH über Rechtsfragen zu den Begriffen „personenbezogene Daten" und „Pseudonymisierung" entschieden. Das EuG hatte zuvor die Ansicht vertreten, dass personenbezogene Daten ihren Personenbezug verlieren, wenn eine Stelle den Personenbezug nicht oder nur mit großem Aufwand wiederherstellen kann.

Der EuGH stellte nun ebenfalls fest, dass die Frage des Personenbezugs subjektiv ist. Es komme auf die Perspektive der verantwortlichen Stelle an, die die Daten verarbeitet. Ist kein Personenbezug herstellbar, fallen die Daten nicht unter die Bestimmungen der DSGVO. Konsequenterweise müssten dann aber auch verschlüsselte personenbezogene Daten ihren Personenbezug verlieren, wenn die Verschlüsselung nicht entschlüsselt werden kann – dieses Problem wurde aber vom EuGH nicht betrachtet.

In der Entscheidung stellte der EuGH zudem klar, dass verantwortliche Stellen, die Daten pseudonymisieren, die Betroffenen darüber informieren müssen, bevor sie sie an Dritte übermitteln.

Secorvo News

Teamverstärkung

Michael Schrempp ist Anfang Oktober zu unserem Beratungsteam dazugestoßen. Mit einem Master in IT Security (KIT) bringt er aktuelles und fundiertes Informationssicherheitswissen mit. Herzlich willkommen im Secorvo-Team!

Weiterbildung 2026

Unsere Seminarangebote 2026 – in unseren neuen Räumlichkeiten am Karlsruher Hauptbahnhof – sind online: Freuen Sie sich auf praxisnahe Inhalte und erfahrene Referentinnen und Referenten, die Ihre Kenntnisse in Datenschutz und Informationssicherheit auf den aktuellen Stand bringen.

Seminarübersicht und Online-Anmeldung unter www.secorvo.de/seminare.

Hokus, Pokus, KIdibus

KI wirkt in der Softwareentwicklung magisch: Code, Tests oder Reviews entstehen scheinbar von alleine. Doch gerade dort, wo es besonders zauberhaft erscheint, lohnt ein genauer Blick – vor allem im Hinblick auf Sicherheit und Vertrauen.

Auf dem Jahresabschluss-Event der KA-IT-Si am 11.12.2025 zeigt Peter Wegner (andrena objects), wie sich KI verantwortungsvoll in Entwicklungsprozesse integrieren lässt - im Spannungsfeld zwischen Euphorie und Kontrollverlust.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Hier geht's zur Anmeldung - wir freuen uns auf Sie!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2025	
10.-13.11.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
24.-28.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
Dezember 2025	
03.12.	IT-Sicherheitstag NRW (IHK NRW, Dortmund)
04.-05.12.	CSCML 25 (IACR, CSCML, virtuell)
05.-07.12.	ICSP 2025 (National Institute of Technology Jamshedpur, Rourkela/IND)
08.-11.12.	Black Hat Europe 2025 (Blackhat, London/UK)
08.-12.12.	Asiacrypt 2025 (IACR, Melbourne/AU)
Januar 2026	
19.-21.01.	Omnisecure 2026 (in TIME, Berlin)
27.-28.01.	33. DFN Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT, Hamburg)
Februar 2026	
02.-06.02.	IT-Defense 2026 (cirosec, Würzburg)
18.-19.02.	ID:SMART Workshop 2026 (CAST, Darmstadt)

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, 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

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.