Secorvo Security News

Juni 2025

Von Genie bis Wahnsinn

KIs versprechen, Sicherheitslücken schneller und gründlicher zu finden als der Mensch. Oft aber liegen sie völlig daneben. Erst kürzlich strapazierte ein offensichtlich KI-generierter Schwachstellenbericht von hackerone die Geduld von Daniel Stenberg, dem Entwickler von curl. Bereits 2023 hatte er mit unseriösen Berichten über die angebliche Schwachstelle CVE-2020-19909 zu kämpfen; jetzt muss er sich gegen automatisierte Meldungen von KI-halluzinierten Schwachstellen wehren. Die Sisyphusarbeit, falsche Alarme richtig zu stellen, kostet inzwischen nicht nur Open-Source-Autoren regelmäßig mehr Zeit als mancher echte Fehler.

Über ein Gegenbeispiel berichtete Sean Heelan im Mai 2025. Er wollte lediglich prüfen, ob das o3-Modell von OpenAI seine zuvor manuell entdeckte Use-after-Free-Schwachstelle CVE-2025-37778 erkennt. Auch dabei kam es zur Halluzination von False Positives – doch mitten im Leistungsvergleich stieß o3 auf eine bisher unbekannte echte Lücke in der Abmelderoutine (CVE-2025-37899), die sich ebenfalls aus der Ferne ausnutzen lässt. Das Ergebnis war allerdings nur deshalb hilfreich, weil Heelan jede Ausgabe genau prüfte: KI als Lupe, nicht als Autopilot.

Das unbedachte Verlassen auf die Ergebnisse digitaler Werkzeuge hat traurige Analogien in der realen Welt: 2022 folgte ein Autofahrer blind den Anweisungen einer Navigations-App und stürzte von einer seit Jahren gesperrten Brücke zwanzig Meter in die Tiefe. Wer – insbesondere KI-basierte – Assistenzsysteme nutzt, sollte jede Ausgabe sorgfältig verifizieren, bevor er dem Ergebnis traut.

KI verstärkt sowohl Genialität als auch Irrtum; zur Unterscheidung bleibt Prüfen Pflicht. Nur wer jede Fundstelle verifiziert, trennt Mehrwert von Rauschen. Assistiert die Maschine dem Menschen statt ihn als Autopilot zu ersetzen, spart sie Nerven und Budget – und Halluzinationen werden nicht zur Katastrophe.

Security News

Danebengepickt

Der US-amerikanische Softwarehersteller OASIS beschrieb am 28.05.2025 eine Schwachstelle in der OneDrive-Dateiauswahl (File Picker). Webanwendungen wie ChatGPT können darüber auf Dateien im OneDrive-Speicher des Anwenders zugreifen. Dafür muss die Anwendung allerdings für den gesamten OneDrive-Speicher des Benutzers berechtigt werden. Zwar werden die Nutzer um Zustimmung gebeten, doch der Hinweis macht den Umfang des gewährten Zugriffs nicht deutlich.

Böswillige Webanwendungen können das ausnutzen - und auch gutwillige Anwendungen können Probleme schaffen, wenn sie die ihnen im Namen des Nutzers gewährten Authentication Token nicht sicher speichern. Außerdem sieht das Verfahren vor, dass Refresh-Token ausgestellt werden können, die der Anwendung fortlaufend Zugriff auf die Nutzerdaten gewähren. Entra-Administratoren sollten die Einstellungen der Benutzereinwilligung bei Webanwendungen daher weitestmöglich einschränken.

Geschwärzte Fenster

Am 09.06.2025 kündigte Microsoft an, dass Teams ab August das Erstellen von Screenshots in Besprechungen unterbinden kann, indem es das Teams-Fenster schwärzt. Dazu nutzt es eine API, die unter Windows (SetWindowDisplayAffinity), macOS, iOS und Android verfügbar ist. Auf anderen Systemen und im Browser bleibt dem Teilnehmer nur der Ton.

Natürlich lässt sich damit nicht verhindern, dass ein Teilnehmer z. B. mit der Handykamera eine Aufnahme macht. Auch lassen sich die Daten weiterhin im Kernelmodus abfangen oder etwa aus dem GPU-Speicher auslesen. Aber das Verfahren erschwert es auch, das System aus der Ferne auszuspähen.

Signal gab am 21.05.2025 bekannt, dass sein Messenger nun ebenfalls Screenshots abwehrt – zunächst allerdings nur unter Windows. Damit soll verhindert werden, dass das umstrittene Windows-Feature Recall die Chats mitliest.

Finger her!

Der Bundesgerichtshof hat am 13.03.2025 entschieden: Liegt ein richterlicher Durchsuchungsbeschluss vor, dürfen Polizei und Staatsanwaltschaft das Entsperren eines Geräts mit biometrischen Merkmalen (Fingerabdruck, Gesicht, Iris) erzwingen. Neben einem Durchsuchungsbeschluss ist hierfür immer auch der Vorwurf einer schweren Straftat erforderlich, wie die Verbreitung und der Besitz von Anleitungen zu sexuellem Missbrauch von Kindern.

Der Grundsatz „Nemo tenetur se ipsum accusare“ verbietet, dass jemand gezwungen wird sich selbst zu belasten. Wer den Zugriff von Strafverfolgungsbehörden verhindern will, sollte auf das biometrische Entsperren verzichten. Unter iOS lässt sich die biometrische Erkennung sogar per Notrufmodus deaktivieren: Fünfmaliges Drücken der Seitentaste genügt. Bei Android hilft ab Version 9 der Sperrmodus: Einschalttaste gedrückt halten, dann auf das Schloss-Symbol tippen. Nur ein Code – Zahlenkombination oder Muster – schützt wirksam vor behördlichem Zugriff, da hier kein Zwang ausgeübt werden darf und Beschuldigte sich nicht selbst belasten müssen.

Konzertierte Updates

Bereits 2005 war der in „Microsoft Update“ umgetaufte Update-Dienst um die automatische Aktualisierung von Microsoft-Anwendungen erweitert worden; und seit einigen Jahren bietet Microsoft Treiberherstellern an, ihre Updates via Windows Update zu verteilen (SSN 05/2025). Am 27.05.2025 kündigte

Microsoft nun an, Drittanbietern die Nutzung von Windows Update auch für die Aktualisierung ihrer Anwendungen zu öffnen.

Linux-Systeme nutzen für Updates seit Jahren Package-Manager, iOS und Android setzen auf App-Stores – ein Konzept, das nun auch Microsoft für die sogenannten Modern Apps übernommen hat.

Tatsächlich ist es wenig sinnvoll, wenn jeder Hersteller seine eigene Updatelösung entwickelt. Für die Anwender sind die unterschiedlichen Abläufe und Meldungen verwirrend; zudem ist es nervenraubend, wenn notwendige Neustarts nicht in ein gemeinsames Wartungsfenster fallen. Solange Microsoft keine Fehler unterlaufen, sinkt mit der Zahl der Update-Lösungen auch das Risiko von Supply-Chain-Angriffen.

Drei Roadmaps, ein Weckruf

Die PQC Coalition, ein Zusammenschluss der US-amerikanischen MITRE Corporation und zehn weiteren Organisationen, hat am 16.05.2025 einen Fahrplan für die Umstellung auf Post-Quanten-Kryptographie (PQC) vorgestellt. Am 11. und 23.06.2025 haben die EU und Kanada nachgezogen. Sie machen damit deutlich, wie dringend es ist, die Migration in Gang zu setzen. So sollen die EU-Mitgliedsstaaten bis Ende 2026 erste Schritte unternehmen; bis Ende 2030 müssen die kritischen Infrastrukturen umgestellt haben.

Die EU und Kanada sind sich einig, dass die Umstellung in den meisten Systemen innerhalb der nächsten zehn Jahre, d. h. spätestens 2035 abgeschlossen sein soll. Flexibler zeigt sich die PQC Coalition: Sie schlägt ein modulares Vorgehen vor und setzt auf Eigenverantwortung.

Ob Vorschrift oder Empfehlung – eines ist allen drei Ansätzen gemeinsam: Wer jetzt nicht plant und sehr bald die wichtigsten Use-Cases (wie digitale Signaturen von Firmware-Updates) angeht, wird später unter Druck improvisieren müssen. Denn die Frage nach der Migration ist kein „Ob", sondern ein „Wann" (siehe SSN 01/2025). Und es tut sich bereits etwas: Der monatliche „Stand der Migration" der PQC Coalition zeigt: Die Umstellung auf Protokoll- und Anwendungsseite hat schon begonnen.

Schwachstellen-Quartett

Das NIST hat am 19.05.2025 mit CSWP 41 eine neue Schwachstellen-Kategorie eingeführt: Likely-Exploited Vulnerabilities (LEV). Anders als der EPSS-Score, der die Wahrscheinlichkeit für eine Ausnutzung in den nächsten 30 Tagen prognostiziert, schaut LEV in die Vergangenheit: Durch wahrscheinlichkeitstheoretische Betrachtungen berechnet LEV eine Untergrenze für die Wahrscheinlichkeit, dass eine Schwachstelle schon ausgenutzt wurde – auch wenn das noch nicht nachgewiesen ist.

Damit schließt LEV die Lücke zwischen CISA-KEV – einem Katalog bestätigter Ausnutzungen – und dem Prognose-Werkzeug EPSS. Zusammen mit dem CVSS, der nach wie vor eine einfache Basismetrik für Schwachstellen beschreibt und dank Environmental-Metriken unternehmensspezifisch justiert werden kann, entsteht so erstmals ein konsistenter Vier-

Felder-Ansatz: KEV erzwingt Sofortmaßnahmen, LEV ergänzt weitere Maßnahmen, EPSS unterstützt die kurzfristige Priorisierung und zum Schluss bilden ein CVSS-Basiswert und der zugehörige Vektor die Grundlage für eine individuelle Betrachtung, wenn es noch Diskussionsbedarf gibt.

Angesichts der überwältigenden Menge von Schwachstellen (CVEs) und Produkten (CPEs) ist ein effektives Patch-Management heute nur noch mit Werkzeugunterstützung zu bewältigen. Für LEV gibt es noch keine Tools, doch kann es sich lohnen, die Kategorie auch jetzt schon bei der Priorisierung und Bewertung von Schwachstellen zu berücksichtigen.

Kontrolle ist besser

Die Bundesbeauftragte für den Datenschutz und Informationsfreiheit hat am 10.06.2025 ein 45 Mio. Euro schweres Bußgeld gegen Vodafone verhängt. Denn Vodafone hatte Auftragsverarbeiter nicht ausreichend überwacht: Shopbetreiber, die Verträge mit Vodafone vermittelt haben, nutzten Kundendaten, um in deren Namen (und ohne deren Wissen) weitere Verträge abzuschließen. Es ist Aufgabe des Verantwortlichen dafür zu sorgen, dass die von ihm oder in seinem Auftrag verarbeiteten Daten geschützt bleiben – diese Verantwortung kann nicht delegiert werden.

Außerdem hatte Vodafone ein Verfahren bei eSIMs verwendet, das dem Grundsatz „Privacy and Security by Design“ nicht ausreichend gerecht wurde. Auch diesbezüglich gilt: Die verantwortliche Stelle trägt die Verantwortung, dass geeignete technische und organisatorische Maßnahmen zur Gewährleistung einer sicheren Datenverarbeitung ergriffen werden. Das Bußgeld ist ein wichtiges Signal, dass sich DSGVO-Compliance auszahlt.

Secorvo News

Teamzuwachs

Seit kurzem verstärken Liza Trace und Julian Wahl mit ihren Erfahrungen und Kenntnissen in forensischen Analysen, Audits, Sicherheits- und Datenschutzmanagement das Secorvo-Beratungsteam. Herzlich willkommen!

Secorvo Seminare

Nach der Sommerpause bereiten Sie die Autoren des T.I.S.P.-Buchs 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. Das Seminar IT Security Insights am **07. und 08.10.2025** bietet Aktuelles für IT-Sicherheitsverantwortliche aus der Praxis.

Übrigens: Alle unsere Seminare sind als Weiterbildungen für die T.I.S.P.-Re-Zertifizierung anerkannt (zur Anmeldung).

15. Tag der IT-Sicherheit

Am **17.07.2025** bietet Ihnen der Tag der IT-Sicherheit bei der IHK Karlsruhe zum 15. Mal die Möglichkeit, sich

zu aktuellen IT-Sicherheitsthemen zu informieren. Beate Bube, Präsidentin des Landesamts für Verfassungsschutz Baden-Württemberg hält die Keynote.

Lernen Sie interessante IT-Sicherheits-Start-Ups kennen und nutzen Sie in der Network-Pause die Gelegenheit zum Erfahrungsaustausch mit Teilnehmern und Referenten. Anmelden können Sie sich noch bis zum 10.07.2025.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2025	
14.-19.07.	PETS 2025 (PETS Board, Washington D.C./US)
17.07.	15. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, Karlsruhe))
22.-25.07.	DFRWS USA 2025 Conference (DFRWS, Chicago/US)
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)

Fundsache

Mit der überarbeiteten Handreichung Stand der Technik bietet TeleTrusT einen aktualisierten und – trotz des inzwischen beachtlichen Umfangs von 140 Seiten – kompakten und strukturierten Überblick über die Best Practices in der IT-Sicherheit.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Ion Barza, Paul Blenderman, Kai Jendrian (Editorial), Hans-Joachim Knobloch, Dr. Alexander Koch, 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