secorvo
security consulting

Secorvo Security News

Juli 2026

Neue Unübersichtlichkeit

Die beeindruckende Leistungsfähigkeit von KI-Systemen fordert auch die Informationssicherheit heraus. Allerdings gelingt es bisher nicht, die Folgen eindeutig zu bewerten.

So finden KI-Systeme zahlreiche Sicherheitslücken in Software. Aber wem nützt das mehr: Angreifern oder Herstellern? In den vergangenen Monaten rollte eine Monsterwelle von Sicherheitspatches durch die Netze und stopfte tausende bislang unentdeckte Schwachstellen: Bei vielen Produkten waren es zehnmal so viele wie bisher üblich. Sofern wir schneller patchen als Angreifer Exploits ausnutzen: Werden unsere IT-Infrastrukturen nun sicherer?

Doch der Vorfall bei OpenAI und Hugging Face zeigt die andere Seite: Unter Ausnutzung einer unbekannten Schwachstelle gelang einer KI der Ausbruch aus einer Sandbox. Der Fall zeigt, dass KI-Systeme auch eigenständig äußerst komplexe Angriffe konzipieren und durchführen können – und das in kürzester Zeit. Auch diese Angriffe benötigen Sicherheitslücken. Das können aber auch geleakte Zugangsdaten, Fehlkonfigurationen oder konzeptionellen Schwächen eines Schutzmechanismus' sein – Fehler also, die sich auch mit KI-Unterstützung nicht einfach ausschließen lassen. Werden die realen Bedrohungen also eher zunehmen?

Noch ist nicht absehbar, ob Angreifer oder Verteidiger stärker von KI profitieren werden. Das wird nicht zuletzt davon abhängen, wie konsequent Softwarehersteller „Security by Design“ umsetzen. Denn schon eine einzige Schwachstelle kann für einen raffinierten KI-Angriff auf eine IT-Infrastruktur genügen.

Eines steht aber außer Frage: Nachlässigkeit bei Best-Practice-Schutzmaßnahmen wird sich zukünftig weit schneller und zuverlässiger rächen als bisher. Wer nicht zu den Opfern zählen möchte, sollte daher seine Risikobewertungen überprüfen – und, wo nötig, schnellstens bisher aufgeschobene Maßnahmen umsetzen.

Inhalt

secorvo
security consulting

Security News

Domänen und Rechtsräume

Am 01.07.2026 erwirkte der texanische Generalstaatsanwalt Ken Paxton ein Urteil, das Verisign – den US-Betreiber der .com-Registry – verpflichtet, die Domain motherless.com zu sperren. Grund war eine fehlende Altersverifikation; Medienberichten zufolge enthielt die Domäne in großem Umfang Missbrauchsmaterial.

Die Server standen allerdings in den Niederlanden, wo es den Behörden bislang nicht gelungen war, die Server dauerhaft abzuschalten. Erst am 21.07.2026, drei Wochen nach der Sperrung der Domäne, wurden die Server beschlagnahmt. Eine solche Domainsperrung könnte allerdings auch Organisationen drohen, die nach europäischem Recht legal handeln. Wer sich für eine gTLD-Domäne wie .com, .net oder .org entscheidet, begibt sich in die Reichweite von US-Gerichten. Nicht nur theoretisch: Im Rahmen der Operation In Our Sites wurden seit 2010 bereits tausende Domänen auf Grund von Verletzungen geistigen Eigentums beschlagnahmt. Dies sollten Unternehmen bedenken, bevor sie sich für die Nutzung dieser gTLDs, länderspezifischer ccTLDs (wie .by für „Bayern“) oder neuer generischer TLDs wie .app entscheiden.

Bildschirm aus, Sender an

Eine Forschergruppe der Shandong University veröffentlichte zur diesjährigen USENIX-Konferenz vorab ihre Arbeit zu „TrojPix“ vom 16.01.2026. Die Gruppe nutzte ein HDMI-Kabel als Sendeantenne, um Daten aus abgeschotteten Netzen über die Abstrahlung auszuschleusen. Dafür genügte eine Schadsoftware mit Nutzerrechten, die das angezeigte Bild so manipuliert, dass sich die Kodierung des HDMI-Signals und damit die Abstrahlung des Kabels ändert. Die Schadsoftware bettet die Daten in das aktuelle Bild ein, das für das menschliche Auge unverändert bleibt – ein Empfänger mit Richtantenne holt die Daten ab.

Überraschend hoch ist die von den Forschern erreichte Bandbreite von 8,1 Mbit/s – der bisherige Bestwert von BitJabber (2020) betrug 0,3 Mbit/s. Auch die angegebene Reichweite von über 200 m ist bemerkenswert, allerdings nennen die Forscher die auf diese Entfernung erreichte Bandbreite nicht.

Die Messungen sind nur knapp dokumentiert. Für die Risikobetrachtung ist das zweitrangig: Wer besonders schutzbedürftige Systeme betreibt, sollte nicht abwarten, ob sich die Werte bestätigen. Dagegen hilft nur physischer Schutz: ein geschirmter Raum, geplant und geprüft von Fachleuten für Abstrahlsicherheit. Lichtwellenleiter statt Kupferkabel nützt nicht, weil auch Monitor und Grafikkarte senden können. Allerdings setzt der Angriff eine mit Schadsoftware infizierte Maschine voraus.

Patchen in KI-Zeiten

In einem Marketingartikel für Intune Autopatch vom 08.07.2026 wirbt Microsoft für eine schnelle Installation von Updates. Das wichtigste Argument: Schwachstellen würden dank KI schneller entdeckt und ausgenutzt. Der bisher übliche Ansatz, Updates verzögert einzuspielen, sei überholt. Doch gerade Microsoft-Updates haben immer wieder schwerwiegende Probleme verursacht – für viele Administratoren ein guter Grund für Vorsicht.

Natürlich patcht man nicht alle Systeme sofort und zugleich. Sinnvoll ist weiterhin ein stufenweiser Rollout: zuerst Test- und Entwicklungssysteme, bei redundanten Systemen zunächst nur eine Instanz. Manche IT-Abteilungen warten aber eine Woche oder länger mit der Installation oder ziehen das Rollout über mehrere Wochen – das ist heute gefährlich.

Mit den Juli-Updates hat Microsoft die Rekordzahl von 622 Schwachstellen mit CVSS-Werten bis 9.9 behoben, darunter auch Zero-Day-Schwachstellen, die bereits aktiv ausgenutzt wurden. Zu CVE-2026-54121 („Certighost“) z. B. erfolgte die Veröffentlichung der Details zehn Tage nach dem Patch Tuesday – wer seine CA da noch nicht gepatcht hatte, setzte sie einem erheblichen Risiko aus.

Microsoft empfiehlt, reguläre Updates spätestens nach drei Tage zu installieren und das Rollout innerhalb von fünf Tagen abzuschließen. Das sind angemessene Empfehlungen.

Insights für Angreifer

Sich als IT-Administrator lückenlos auf dem Laufenden zu halten, welche sicherheitsrelevanten Patches es für alle genutzten Systeme (OS, Anwendungen, Firmware, etc.) gibt, ist keine einfache Aufgabe. Clouddienste wie Vulmon Alerts können dabei unterstützen: Man trägt ein, welche Software man nutzt, und der Dienst informiert, sobald Updates dafür vorliegen.

Die Nutzung eines solchen Dienstes birgt jedoch ein Risiko: Wird die Datenbank des Anbieters erbeutet, können die darin gespeicherten Angaben für Angriffe genutzt werden, denn die Daten offenbaren, welche Software ein als Angriffsziel ausgewähltes Unternehmen einsetzt.

Seit dem 11.07.2026 bietet Kolja Sagorski, Systemadministrator bei coderei GmbH, die kostenlose Alternative patchletter.com an. Für die Registrierung genügt eine gültige E-Mail-Adresse. Darüber lässt sich das Risiko eines Missbrauchs der Informationen

verringern, wenn man ein anonymes Freemail-Postfach nutzt und die Meldungen von patchletter.com weiterleiten lässt.

Quantensprung

Wie die ANSSI in Frankreich (siehe SSN 6/2026) gibt jetzt auch die US-Regierung Gas: Sie erließ am 22.06.2026 ein Dekret, das die Umstellung auf PQC für Systeme mit hohem Schutzbedarf bis Ende 2030 für die Verschlüsselung und bis Ende 2031 für digitale Signaturen vorschreibt. Zudem sollen Mindestanforderungen an eine Cryptographic Bill Of Materials (CBOM), die auch eine automatisierte Erstellung ermöglichen, formuliert werden.

Diese Entwicklung kündigt sich seit 2024 an. Google gab am 06.02.2026 mit einem Aufruf zum Handeln einen wichtigen Anstoß. Am 25.03.2026 stellte das Unternehmen seinen neuen Zeitplan vor, der eine vollständige Umstellung bis 2029 vorsieht. Cloudflare schloss sich diesem Kurs am 07.04.2026 an. Und Microsoft-CTO Mark Russinovich gab am 30.06.2026 die Zusage, die Einführung von PQC auch bis 2029 zu schaffen.

Noch sind nicht alle kryptografischen Protokolle für PQC standardisiert, aber die Fortschritte sind erkennbar. Die Umstellung auf PQC rückt näher: Alle Unternehmen sollten daher mit den Vorbereitungen beginnen; im ersten Schritt mit einer Kryptografie-Inventur (CBOM).

(Black) HAWK Down

Am 28.07.2026 beschrieb das US-amerikanische KI-Unternehmen Anthropic in einem Blog-Artikel, wie leistungsfähig KI-Modelle inzwischen beim Angriff auf kryptographische Verfahren sind. Betroffen ist unter anderem HAWK, ein gitterbasiertes Verfahren, das die aktuelle Runde 3 des NIST-Wettbewerbs für neue Post-Quanten-Signaturverfahren erreicht hatte. Einen Tag nachdem das Mythos-Modell den Angriff gefunden hatte, zogen es die Autoren zurück. Die notwendige Anpassung der Sicherheitsparameter hätte das Verfahren unattraktiv gemacht.

Die Fähigkeit der jüngsten Generation großer Sprachmodelle, sehr viele mathematische Analysen in ähnlichem Kontext durchzuprobieren, kann zugleich Grund für ein größeres Vertrauen in derzeit genutzte Kryptoverfahren sein: Im Anhang der Veröffentlichung erläutern die Autoren, warum die entdeckte Schwäche das Signaturverfahren Falcon nicht betrifft.

Secorvo News

Teamverstärkung

Begeistern Sie herausfordernde Fragestellungen des Datenschutzes? Für und mit unseren Kunden suchen wir clevere Antworten und Lösungen statt unflexibler, bürokratischer Vorgehensweisen. Möchten Sie uns dabei unterstützen? Dann freuen wir uns auf Ihre Bewerbung!

Qualifikation

Auf unseren Seminaren im kommenden Herbst können Sie Ihr Wissen aktualisieren und anerkannte Zertifizierungen erwerben:

Die T.I.S.P.-Schulung (**28.09.–02.10.2026** und **16.–20.11.2026**) bereitet Sie auf die Prüfung zum TeleTrusT Information Security Professional vor. Für beide Veranstaltungen gibt es noch einige wenige Plätze.

Auf dem Seminar IT Security Insights – T.I.S.P. Update (**19.–20.10.2026**) stellen wir Ihnen aktuelle Entwicklungen in Technik, Recht und Informationssicherheit vor.

Die nach § 38 BSIG verpflichteten Kenntnisse zur Erkennung und Bewertung von Informationssicherheitsrisiken erhalten Geschäftsleitungen in unserer vierstündigen NIS-2-Schulung am **15.10.2026**.

Dank unserer Kooperation mit der andrena objects ag beim Seminar T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (**05.–08.10.2026** und **02.–05.11.2026**) bekommt der Inhalt zusätzlichen Praxisbezug durch 30 Jahre Erfahrung in der professionellen Softwareentwicklung.

Programme und die Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Einfach so abhängen?

Moderne Softwareprojekte nutzen oft hunderte APIs fremder Software-Pakete. Fremdcode kann aber schnell zum Einfallstor für Angriffe werden, daher ist „*Install first, think later*“ keine gute Strategie. Alles selber zu entwickeln allerdings genauso wenig…

Beim kommenden KA-IT-Si-Event am **17.09.2026** zeigt Jana Prechelt (andrena objects ag), welche Abhängigkeiten sinnvoll sind und wie man sie souverän steuert – für robustere, sicherere und besser kontrollierbare Systeme. Anschließend erwartet Sie der Erfahrungsaustausch beim „Buffet-Networking“. Wir freuen uns darauf, Sie bei andrena zu sehen – und empfehlen, wie immer, eine schnelle Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2026	
06.-09.08.	Defcon 34 (DEF CON Communications, Inc., Las Vegas/US)
12.-14.08.	35th USENIX Security Symposium (usenix, Baltimore/US)
17.-20.08.	Crypto 2026 (IACR, Santa Barbara/US)
23.-26.08.	SOUPS 2026 (usenix, Hannover)
24.-25.08.	SAC 2026 (IACR, Ottawa/CA)
24.-25.08.	SAC Summer School (IACR, Ottawa/CA)
September 2026	
09.-10.09.	Annual Privacy Forum 2026 (PLUS, Goethe Universität, Plattform Privatheit, Salzburg/AT)
17.09.	KA-IT-Si-Event „Einfach so abhängen?“ (KA-IT-Si, Karlsruhe)
22.-23.09.	heise devSec 2026 (iX, dpunkt.verlag, heise, Marburg)
23.-25.09.	Datenschutzkonferenz 2026 (DFV, Düsseldorf)
28.09.-02.10.	TeleTrusT Information Security Professional (T.I.S.P.) (Secorvo, Karlsruhe)
29.-30.09.	secIT digital (Heise Medien, virtuell)
29.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt, hybrid)

Fundsache

Das ULD hat auf seiner Webseite eine hilfreiche Handlungsanweisung zum Vorgehen bei Datenpannen veröffentlicht.

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