Secorvo Security News

Mai 2025

Beeindruckende Blender

Die Aufregung war nicht zuletzt unter Datenschützern groß, als im vergangenen August Microsofts Copilot den Journalisten Martin Bernklau unter anderem zum verurteilten Kinderschänder erklärte: Er hatte als Gerichtsreporter regelmäßig über Verurteilungen von Straftätern berichtet und war als Autor des veröffentlichten Beitrags namentlich genannt worden.

Die Ursache für diese Falschauskunft ist jedoch keineswegs ein Qualitätsmangel des ChatBots, sondern ein grundsätzliches Missverständnis: Ein Large Language Model (LLM) setzt seine Sätze aus den gelernten Daten nach Wort-Wahrscheinlichkeiten zusammen – und erhebt damit schon konstruktionsbedingt keinen Anspruch auf inhaltliche Richtigkeit. Es ist gewissermaßen ein „Blender mit (Halb-) Wissen, der eloquent formulieren kann" – und daher glaubwürdig erscheint, selbst wenn das vermeintliche Wissen nach Plausibilität geraten ist. Die Glaubwürdigkeit steigt noch durch die große Belesenheit der LLMs: Sie wurden mit mehr Dokumenten angelernt, als ein Mensch im Laufe seines Lebens jemals lesen könnte; daher bleiben sie nur selten eine Antwort schuldig.

Wer korrekte Aussagen sucht, sollte daher Antworten von KI-Chatbots nicht blind vertrauen – sie sind nicht verlässlicher als Äußerungen in „Sozialen Netzwerken", Statements am Stammtisch oder Gerüchte aus der Nachbarschaft. Wer etwas sicher wissen will, muss referenzierte, evaluierte und daher belastbare Quellen konsultieren.

Selbst dann bleibt ein Restrisiko für Falschaussagen. So hatte 1890 der Physiologe *Gustav von Bunge* (1844-1920) den Eisengehalt von Spinatpulver mit 35mg je 100g bestimmt. Doch in frischem Spinat liegt der Eisgengehalt nur bei einem Zehntel dieses Werts. Dennoch hielt sich über Jahrzehnte die Überzeugung, der Verzehr von Spinat sei für den Muskelaufbau besonders förderlich. Generationen von Kindern haben darunter gelitten – lange vor dem ersten LLM.

Security News

Totgesagte leben länger

Die Active Directory Certificate Services (ADCS) sind inzwischen 25 Jahre alt. Da es jahrelang keine Neuerungen gab und notwendige Schwachstellen-Fixes eher lieblos in das User Interface integriert wurden, kursierte seit einer Weile die Befürchtung, dass Microsoft das Windows-Feature über kurz oder lang aufgeben würde – auch wenn die Einführung von Certificate Based Authentication in Entra ID 2022 ADCS-Anwendern etwas Hoffnung gemacht hatte.

Nun hat die neue Produktmanagerin Tanya Jha am 20.04.2025 auf dem Windows Server Summit mehrere funktionale Erweiterungen angekündigt. Auch Post-Quanten-Kryptographie (PQC) wird ADCS unterstützen: In einem Blogartikel erläuterte die leitende Produktmanagerin Aabha Thipsay am 19.05.2025, dass ML-KEM und ML-DSA sowohl in die Windows-Krypto-Bibliothek CNG als auch in ADCS implementiert werden. Auch die optionalen ADCS-Komponenten wie CEP/CES, NDES und OCSP-Responder sowie der Intune Certificate Connector sollen PQC-fähig werden. Offenbar ist bei Microsoft angekommen, dass zahlreiche Kunden die On-Premise-AD-Dienste noch länger benötigen: Nach einer LinkedIn-Umfrage von Linda Taylor, AD-Entwicklerin bei Microsoft, wollen 36% der Unternehmen die Dienste sogar „für immer" nutzen.

Regen und Traufe

In ihrem Tätigkeitsbericht vom 12.05.2025 für 2024 berichtet die Landesdatenschutzbeauftragte Brandenburg, dass es bei öffentlichen Stellen immer wieder durch Briefkastensprengungen zur Offenlegung von personenbezogenen Daten aus Schreiben kommt – und empfiehlt, die Briefkästen in die Gebäude oder ins Mauerwerk zu verlegen. Das wirkt etwas kurz gesprungen: Auch die Vernichtung personenbezogener Daten ist ein (ggf. sogar meldepflichtiger) Datenschutzvorfall. Dagegen hilft nur zügige Digitalisierung – aus Datenschutzgründen.

Copilot als Geheimnisfinder

Nicht nur Schwachstellen, sondern auch zu großzügige Berechtigungen können vertrauliche Informationen preisgeben. Das britische Unternehmen Pen Test Partners beschrieb am 07.05.2025, wie Microsofts KI Copilot die Suche nach solchen Daten in Sharepoint unterstützt: Zwar respektiert Copilot vergebene Berechtigungen, doch hinterlassen die Suchabfragen wenige Spuren. Wer Copilot um eine inhaltliche Zusammenfassung interessanter Dateien bittet, kann so einen protokollierten Zugriff umgehen. Wird SharePoint gar für vertrauliche Daten genutzt – direkt oder über Teams –, muss man die Zugriffsrechte im Auge behalten und sollte gegebenenfalls die Nutzung von Copilot einschränken.

Untergeschoben

Wenn Motherboard- oder Rechnerhersteller unter Windows mit mehr oder weniger sanftem Druck ihre eigene Treiberverwaltung installieren, erzeugt das bei Anwendern zusätzlichen Verwaltungsaufwand. Microsoft bietet daher an, herstellerspezifische Treiber über Windows Update auszuliefern.

Das ist zu begrüßen: Da jede Treiberinstallation hohe Berechtigungen braucht, ist jeder Update-Mechanismus auch ein Sicherheitsrisiko. Aktuelles Beispiel: Im ASUS DriverHub (Patch vom 09.05.2025) wurden zwei hoch kritische Schwachstellen (CVSS-Bewertungen 9,4 und 8,4) entdeckt, über die Anwender sich bspw. von einer manipulierten Webseite eine Remote Code Execution mit Admin-Rechten einfangen können, wie der neuseeländische Sicherheitsforscher Mr. Brush am 07.04.2025 herausgefunden hatte.

Sichere Logins im Königreich

Das britische Zentrum für Cybersicherheit (NCSC) kündigte am 06.05.2025 auf ihrer CYBERUK-Konferenz an, dass in öffentlichen Einrichtungen die SMS-basierte Zwei-Faktor-Authentifikation durch Passkeys ersetzt wird. Neben der Vereinfachung des Anmeldevorgangs soll damit ein besserer Schutz vor Phishing erreicht werden. Der National Health Service, der in der Vergangenheit wiederholt Opfer von Cyberangriffen wurde, soll zu den ersten Nutzern gehören. Um an der weiteren Entwicklung von passwortlosen Anmeldeverfahren mitwirken zu können, ist das NCSC außerdem der FIDO-Alliance beigetreten.

Auch das BSI teilt die Überzeugung des NCSC und empfiehlt schon seit 2024 die Nutzung von Passkeys. Doch bei der Umsetzung hinkt Deutschland hinterher.

Armer Mann aus Nebraska

Mit dem Angriff auf das npm-Modul „rand-user-agent" erhält die Reihe auffälliger Kompromittierungen in der Software-Lieferkette einen neuen Vertreter: Über die „RATatouille" getaufte Attacke gelang es Angreifern, einen Remote-Access-Trojaner (RAT) in die beliebte Bibliothek einzuschleusen. Rund eine Woche blieb der Angriff unentdeckt, bis Aikido Security ihn am 06.05.2025 öffentlich machte. Ursache war nach Recherchen von BleepingComputer ein Maintainer-Token ohne Zwei-Faktor-Authentifizierung.

Der Angriff zeigt beispielhaft, wie anfällig Software-Lieferketten sind. Wer Software anderer nutzt, muss inzwischen auf deren Sicherheit und die der Repositories vertrauen, denn eine Kontrolle ist bei der Vielzahl von Abhängigkeiten in moderner Software nahezu unmöglich. Die Verantwortung verlagert sich dadurch aber nicht auf Dritte.

Künftig bringt von KI-Systemen erzeugter Quelltext neue Herausforderungen: Eine am 03.04.2025 publizierte Untersuchung der University of Texas zeigt, dass große Sprachmodelle häufig unsichere Abhängigkeiten vorschlagen – und diese oft ohne Prüfung übernommen werden. So wird aus vermeintlicher Produktivitätssteigerung eine neue Angriffsfläche. Wer den armen Mann aus Nebraska von xkcd kennt, den wundert das nicht.

Arbeitnehmerdatenschutz

Am 28.01.2025 und am 08.05.2025 hat das Bundesarbeitsgericht (BAG) zwei Urteile mit Datenschutzbezug gefällt. Im ersten Fall hatte ein Arbeitgeber seinen Arbeitnehmern die Entgeltnachweise digital zur Verfügung gestellt. Dafür dürfen die Daten nach Auffassung des BAG im Rahmen einer Auftragsverarbeitung an einen Dienstleister übermittelt werden.

In einem zweiten Fall entschied das BAG, dass eine Datenübermittlung innerhalb eines Konzerns zwar rechtmäßig war. Doch war in einer Betriebsvereinbarung festgelegt, welche Daten an einen Dienstleister übermittelt werden durften. Dieser erhielt jedoch mehr Daten als zur Zweckerfüllung erforderlich. Das Gericht erkannte den Betroffenen einen Schadensersatzanspruch von 200 € im Einzelfall zu. Damit folgte es der Entscheidung des EuGH vom 19.12.2024, nach der sich

eine Betriebsvereinbarung an den Maßstäben der DSGVO messen lassen muss.

Randnotiz: Zur Legitimation einer Übermittlung von Personaldaten innerhalb eines Konzerns ist das berechtigte Interesse in der Regel nicht ausreichend, da es angemessenere Mittel wie beispielsweise mandantenfähige Systeme gibt, die keine konzernweiten Datenübermittlungen erfordern.

Secorvo News

Teamzuwachs

Seit Anfang Juni verstärkt Dr. Alexander Koch unser Team. Er ist Informatiker mit den Schwerpunkten Kryptologie und Informationssicherheit und hat über kryptografische Protokolle promoviert.

Secorvo Seminare

Wie Sie Public Key Infrastrukturen erfolgreich aufbauen und nutzen, zeigt Ihnen unser Kollege Hans-Joachim Knobloch vom **23. bis 26.06.2025**. Und 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. Wer sich für einen Cyber-Angriff wappnen will, sollte einen Vorfall-Experten im Haus haben. Vom **14. bis 16.10.2025** bilden wir Sie nach dem Curriculum des BSI dazu aus.

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

Divide et Impera

Nach der Maxime „teile und herrsche“ haben nicht nur die Römer Gallien unterworfen. Netzwerksegmentierung ist auch ein zentrales Schutzkonzept zur Begrenzung der Auswirkungen von Cyber-Angriffen. Und das nicht erst seitdem „Zero Trust“ durch die Dörfer getrieben wird: Wirksame Segmentierungen haben schon bei vielen Unternehmen die Ausbreitung von Ransomware begrenzen können. Auf dem nächsten KA-IT-Si-Event am **26.06.2025** zeigt Paul Blenderman (Secorvo), was bei der Segmentierung zu beachten ist – technisch und konzeptionell –, um einerseits die Funktion der Dienste und erforderliche Zugriffe nicht einzuschränken und andererseits Angreifern den Weg durchs Netz mit möglichst vielen Barrieren zu versperren.

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

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 über aktuelle 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. Hier geht's zum Programm und zur Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2025	
02.-04.06.	Entwicklertag 2025 (VKSI, GI, ObjektForum, Karlsruhe)
02.-04.06.	DuD 2025 (COMPUTAS, Potsdam)
04.-05.06.	Security Forum Congress 2025 (Security Forum, Barcelona/ES)
23.-26.06.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
23.-26.06.	23rd International Conference on Applied Cryptography and Network Security (fordaysec, München)
26.06.	Teile und herrsche (KA-IT-Si, Karlsruhe)
30.06.-04.07.	10th IEEE European Symposium on Security and Privacy (IEEE, Venedig/IT)
Juli 2025	
14.-19.07.	PETS 2025 (The George Washington University, Washington, DC/US, hybrid)
17.07.	15. Tag der IT-Sicherheit (Cyber-Forum, IHK, KA-IT-Si, Karlsruhe)
22.-25.07.	DFRWS USA 2025 Conference (DFRWS, Chicago/US, hybrid)

Fundsache

Ein herausforderndes Spiel: Beim Reverse Turing Test von Catmanmcgee gewinnt, wer sich in einem Chat mit drei KIs erfolgreich als weitere KI ausgibt. Der Quelltext kann eingesehen werden.

Impressum

Secorvo Security News – ISSN 1613-4311

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