Secorvo Security News

August 2024

Halluzinierte Wirklichkeit

Alter Wein in neuen Schläuchen – danach klingt die aktuelle KI-Euphorie, zumindest in den Ohren derjenigen, die die zahlreichen KI-Wellen der vergangenen 40 Jahre miterlebt haben. Neu ist allerdings die beeindruckende Leistungsfähigkeit heutiger Sprachmodelle. Da vergisst man leicht, dass sie wenig anderes liefern als eine Prognose für das nächste Wort. Dass wir einer auf Wort-Wahrscheinlichkeiten basierenden Ausgabe einen Sinn beimessen, verrät vielleicht mehr über unser eigenes Denken als über die KI.

„Wissen" in unserem bisherigen Verständnis besitzt ein Sprachmodell allerdings nicht: Ein Wikipedia-Eintrag und oft auch eine Internet-Recherche sind in der Regel zuverlässiger als die Antwort eines Chatbots. Etwas zugespitzt ist ein KI-Chatbot ein Dilettant, der sich gut ausdrücken kann – ein Blender.

Was aber macht ein Blender, wenn er nicht mehr weiter weiß? Er „ergänzt" seine Ausführungen auf der Grundlage seines Halbwissens kreativ. Bei einem Chatbot nennt man das „Halluzinieren": Namen, Daten und Fakten niedrigerer Wahrscheinlichkeiten werden hinzugefügt. Das Ergebnis hat dann bestenfalls noch am Rande etwas mit der Wirklichkeit zu tun – ist aber hübsch formuliert.

Sprachmodelle werden derzeit vorwiegend wie ein „Orakel" zu allen möglichen Themen befragt. Die Ergebnisse werden meist separat verarbeitet – im Kopf, in Dokumenten, in Datenbanken. Genau hier liegt die eigentliche Gefahr: „Halluzinierte" oder auch nur „nicht ganz richtige" Ausgaben finden zunehmend Eingang in Überzeugungen und seriöse Dokumente: Presseartikel, Studien, Datenbanken.

Darunter finden sich auch Angaben über Personen. Art. 14 DSGVO verpflichtet Verarbeiter, Betroffene über die Verarbeitung personenbezogener Daten zu informieren, die nicht direkt bei diesen erhoben wurden – damit wird Datenschutz zum Chatbot-Korrekturfilter. Hilfreich. Solange er nicht missachtet wird.

Security News

Ferngesteuerte Kraftwerke

Forscher vom niederländischen Institut DIVD haben am 12.08.2024 gleich sechs Schwachstellen in den Gateways des amerikanischen Photovoltaik-Giganten Enphase publiziert. Die Gateways verbinden die PV-Anlagen mit der Cloudplattform des Herstellers. Schon am 17.04.2021 hatte das DIVD in einem GitHub-Repository ein Administrator-Passwort für die Cloudplattform des chinesischen PV-Herstellers SolarMan gefunden, und am 07.08.2024 berichtete Bitdefender über

eine Schwachstelle in der Authentifizierung der Solar-Man-Cloudplattform.

Das Problem ist gravierend: Die Web-Oberflächen liefern nicht nur hübsche Grafiken über die Produktion der Paneele, sondern können die Anlagen aus der Ferne steuern oder neue Firmware einspielen. Angriffe auf die Anlagen eines Herstellers könnten das Stromnetz empfindlich stören, denn solche Cloud-Server steuern Millionen von PV-Anlagen – das Äquivalent von dutzenden Kraftwerken, wie Bert Hubert in seinem Blog argumentiert. Während für konventionelle Kraftwerke strenge Vorschriften gelten, werden diese Plattformen hingegen wie simple Geburtstagskalender behandelt.

Undifferenzierte Integration

Microsoft-Forscher berichteten am 29.07.2024 von einer Schwachstelle in VMware ESXi, die bereits von Ransomware ausgenutzt werde: Integriert man das System in ein Active Directory (AD), gewährt die Software implizit einer AD-Gruppe „ESX Admins" volle Administratorrechte auf dem Hypervisor. VMware hat die Schwachstelle mittlerweile geschlossen (CVE-2024-37085).

Die Sicherheitslücke konnte ausgenutzt werden, weil viele IT-Abteilungen die Administration ihrer Infrastruktur wie eine beliebige Büro-Anwendung in das produktive AD integriert haben. Das ist keine gute Idee: Will man die Virtualisierung, die Storage-Systeme, die Switches und Router in ein AD integrieren, gehören sie in eine separate, rein administrative Domäne, die vom produktiven Forest netzwerktechnisch und logisch getrennt ist. Das kann man mit dem Konzept einer „Bastionumgebung" kombinieren, wie von Microsoft ausführlich beschrieben.

Reanimierte Sicherheitslücke

Qualys Labs hat am 01.07.2024 berichtet eine bereits 2006 geschlossene Schwachstelle in OpenSSH entdeckt zu haben, die durch eine Überarbeitung des Codes versehentlich erneut eingebaut wurde. Die wiederauferstandene Schwachstelle wurde „RegreSSHion" getauft, da im Entwicklungsprozess nicht sichergestellt wurde, dass einmal behobene Fehler durch spätere Änderungen nicht abermals implementiert werden. Solche Regressionstests sollten gerade bei sicherheitsrelevanten Softwareprojekten Standard sein.

Mitverantwortung

Die Rechtbank Amsterdam hat am 07.06.2024 erstinstanzlich entschieden, dass für Tracking-Cookies verantwortlich ist, wer sie entwickelt, Webseitenbetreibern zur Verfügung stellt und im Zuge dessen auch Vereinbarungen über die Datenschutzbestimmungen trifft. Diese Unternehmen legen fest, welche personenbezogenen Daten zu welchen Zwecken und mit welchen Mitteln verarbeitet werden. Eine Abwälzung der Verantwortung für die Einholung einer wirksamen Einwilligung auf die Webseitenbetreiber sei nicht rechtskonform.

Microsoft, LinkedIn und Xandr wurde daher untersagt, Tracking Cookies zu verwenden, wenn keine ausdrück-

liche Einwilligung der Betroffenen vorliegt. Diese Auffassung ist konsequent und folgt den Vorgaben des EuGH (Urteil zu IAB Europe vom 07.03.2024). Webseitenbetreiber und Urheber von Cookies müssen im Zweifel gemeinsam dafür Sorge tragen, dass der Einsatz rechtmäßig erfolgt.

KRITIS-Prüfungen neu geregelt

Am 19.08.2024 hat das BSI die überarbeiteten Grundsätzlichen Anforderungen im Nachweisverfahren (GAiN) veröffentlicht. Darin wird die Durchführung von KRITIS-Prüfungen nach § 8a (3) BSIG verbindlich geregelt. Überraschende Neuerungen finden sich nicht; die konkretisierten Anforderungen zur Gestaltung von Geltungsbereich (N.DG.01) und Netzplan (N.DG.02) dürften für Betreiber der wichtigste Aspekt sein und möglicherweise Handlungsbedarf erzeugen. Eine gute Zusammenfassung der Änderungen findet sich bei OpenKRITIS.

Patientendatenschutz

Den Schutz von Patientendaten fordert nicht nur das Datenschutzrecht, sondern auch das Patientengeheimnis, dessen Verletzung nach § 203 StGB strafbewehrt ist. Einzelne gesetzliche Krankenkassen kümmert das offenbar wenig – sie lassen sich bei Beratungsterminen von Versicherten nebulöse (und damit rechtsunwirksame) Einwilligungen zur „Verarbeitung von medizinischen Informationen“ unterzeichnen, mit denen sie dann Diagnosen und Berichte von Ärzten und Krankenhäusern anfordern. Eine solche Weitergabe kann ohne die explizite Entbindung von der ärztlichen Schweigepflicht durch den Patienten eine Straftat sein.

Die Datenschutz-Aufsichtsbehörde Hessen setzte dieser Praxis bei einer besonders offensiven Krankenkasse nach einer Datenschutz-Beschwerde von Secorvo am 09.07.2024 ein Ende. Weitere Beschwerden sind derzeit bei anderen Datenschutz-Aufsichtsbehörden in Bearbeitung.

Fatales Update

Es wurde in allen Medien berichtet: Ein fehlerhaftes Update von CrowdStrike für das EDR-Produkt Falcon führte am 19.07.2024 bei geschätzt 8,5 Millionen Windows-Rechnern dazu, dass die Systeme ständig abstürzten – viele schon bevor sie ein korrigiertes Update herunterladen konnten. Zahlreiche Kunden benötigten bis zu zwei Tage, um die betroffenen Systeme manuell instand zu setzen. Der Vorfall verursachte Ausfälle an Flughäfen, bei Banken und in Krankenhäusern. Fitch Ratings schätzte am 22.07.2024 allein den versicherten Schaden auf einen mittleren bis hohen einstelligen Milliardenbetrag.

Der Tenor der Nachrichten war, dass das Sicherheitsprodukt selbst zu einem Sicherheitsproblem geworden sei. Diese Bewertung greift jedoch zu kurz, denn unabhängige Tests zeigen, dass Falcon einen effektiven Schutz vor Angriffen bietet - eine Wiederherstellung nach einem erfolgreichen Angriff dürfte wesentlich länger als 1-2 Tage dauern und einen viel höheren Schaden verursachen.

Allerdings hat das Update-Verfahren – wie CrowdStrike am 06.08.2024 selbst einräumte – erhebliche Schwächen. Auch Microsoft sieht sich in der Mitverantwortung und kündigte am 27.07.2024 an, die Antimalware-Hersteller besser dabei zu unterstützen, dass sie nur in seltenen Fällen auf Kernel-Prozesse zugreifen müssen, damit Programmfehler nicht das Betriebssystem in Mitleidenschaft ziehen.

Secorvo News

Weiterbildung

Im Herbst 2024 erwarten Sie vier Zertifizierungs- und Fachseminare bei Secorvo. Das Seminar Vorfall-Experte (BSI) vom **15. bis 17.10.2024** bereitet Sie auf die Zertifizierung durch das BSI vor. Auf dem PKI-Seminar vom **04. bis 07.11.2024** lernen Sie von unseren PKI-Experten alles Erforderliche von den Grundlagen bis zu Planung und Betrieb Ihrer eigenen PKI.

Möchten Sie Teil der über 2.000 Mitglieder starken T.I.S.P.-Community werden? Das gelingt mit unserem T.I.S.P.-Seminar vom **11. bis 15.11.2024** und der anschließenden Zertifikatsprüfung.

Beim T.P.S.S.E.-Seminar vom **25. bis 28.11.2024**. dreht sich alles um die Entwicklung sicherer Software. Auch diese Qualifikation können Sie mit einer Zertifizierung abschließen. Sichern Sie sich durch eine schnelle Buchung den Frühbucherrabatt. Wir freuen uns auf Ihre Anmeldung.

Software ist sicher.
Und die Erde eine Scheibe.

Der Cyber Resilience Act (CRA) legt Herstellern von Software und Open Source Communities strenge Regeln zur IT-Sicherheit ihrer Produkte auf. Zu den Anforderungen der EU-Verordnung an „Produkte mit digitalen Elementen" zählen die Erstellung einer Cybersicherheitsrisikobewertung und die Bereitstellung von Sicherheitsupdates.

Verstöße können mit bis zu 15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes geahndet werden.

Beim KA-IT-Si-Event am **12.09.2024** gibt Markus Toran (Secorvo) einen Überblick über die gesetzlichen Regelungen, erläutert, worauf sich Hersteller, Open Source Communities und Verbraucher einstellen müssen und diskutiert, wie praktikabel und effektiv die Vorgaben sein werden.

(Der ursprünglich für diesen Tag vorgesehene Vortrag von Frau Professorin Volkamer muss verschoben werden – wird aber nachgeholt).

Anschließend erwartet Sie natürlich der Erfahrungsaustausch beim „Buffet-Networking". Wir freuen uns auf Sie in der „Church" im CyberForum – und empfehlen wie immer eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2024	
04.-05.09.	Annual Privacy Forum 2024 (ENISA, DG Connect and Karlstad University, Karlstad/SWE)
11.-12.09.	secIT digital (Heise Medien, virtuell)
12.09.	KA-IT-Si-Event „Software ist sicher. Und die Erde eine Scheibe.“ (KA-IT-Si, Karlsruhe)
19.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
19.-20.09.	37. Kryptotag (GI, Nürnberg)
25.-26.09.	heise DevSec 2024 (iX, heise Security, dpunkt.Verlag, Köln)
Oktober 2024	
14.-18.10.	ACM CSS 2024 (ACM SIGSAC, Salt Lake City/US)
15.-17.10.	Vorfall-Experte (BSI) (Secorvo, Karlsruhe)
22.10.	Swiss Cyber Storm 2024 (Swiss Cyber Storm, Bern/CH)
22.-24.10.	it-sa 2024 (itsa 365, Nürnberg)
November 2024	
04.-07.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
05.-07.11.	24. IDACON 2024 (WEKA Akademie, München)
11.-15.11.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Paul Blenderman, Robert Eitel, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

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