Volker Schrader
KI und der Biber

Was ist Deine Arbeit wert, wenn KI alles macht?

Vigilia-Verlag, Kelkheim 2026
ISBN 978-3982819310
160 Seiten, 20 €
(Epub-E-Book: 14 €)

Philosophische Gespräche über KI

Was hätten der Renaissancemaler Lucas Cranach oder die Physik- und Chemiepionierin Marie Curie zu künstlicher Intelligenz zu sagen? Mit solcherlei ungewöhnlichen Fragen beleuchtet Volker Schrader generative KI aus ganz unterschiedlichen Perspektiven.

Menschen aus längst vergangenen Zeiten zum Thema künstliche Intelligenz zu befragen, erscheint auf den ersten Blick nicht gerade sinnvoll. Wer sich aber auf das Gedankenspiel des Kommunikationsexperten Volker Schrader einlässt, kann sich freuen: nicht nur über eine kurzweilige Lektüre, sondern auch über unerwartete Erkenntnisse in Bezug auf den Umgang mit KI. Beispielsweise, wenn Leonardo da Vinci im Interview sagt: „Wissen ist: verstehen, was man nicht versteht. Und dann fragen."

Weil der Autor die Schauplätze seiner fiktiven Gespräche mit Liebe zum Detail beschreibt, fällt es leicht, ihm in die Kunstwerkstatt von Lukas Cranach dem Älteren und ins provisorische Labor von Marie Curie zu folgen. Cranach, dessen Gesellen große Teile seiner Arbeit ausführten, nimmt manchem die Sorge, dass ein Wert nur durch eigene Ausführung entstehen könne. Curie erklärt die Bedeutung von Intuition gegenüber der reinen Datenanalyse.

Nach dem ersten Zwischenfazit geht es in die Natur: Der Biber baut emsig an seinem Damm, auch wenn die Rahmenbedingungen dafür nicht ideal sind. „Einfach mal machen", lautet seine Botschaft. Beim Besuch eines Pilzgeflechts ergründet Schrader die Frage nach der Verantwortung in Systemen, die kein Einzelner mehr allein kontrollieren kann. Mit seinem Besuch der Forscherin Elena im Jahr 2154 wagt der Autor schließlich einen Blick in die Zukunft.

Der Untertitel des Buchs führt ein wenig in die Irre. Die Frage, welchen Wert menschliche Arbeit noch hat, „wenn KI alles macht", steht nicht im Zentrum der Betrachtungen. Für den Autor war sie vielmehr der Motor, der ihn antrieb, sich auf die Suche zu begeben. Die Antworten, die Schrader in seinen fiktiven Gesprächen findet, gehen weit über eine nüchterne Analyse der Arbeitswelt hinaus. Sein Buch kann dem Leser vielmehr eine Ermutigung liefern, die eigene Rolle in der veränderten Arbeitswelt neu zu bestimmen und auf die eigenen, menschlichen Fähigkeiten zu vertrauen. Vielleicht macht er es dann ähnlich wie der Biber, der nicht weiß, wie das Wetter wird oder ob sein Damm letztlich hält – und trotzdem einfach loslegt. *(Dorothee Wiegand/psz@ct.de)*

Lückensucher-Fachfutter

Die Fülle an immer neuen Sicherheitslücken in der wachsenden Softwarewelt macht es Sicherheitspraktikern schwer, mit Netzangreifern Schritt zu halten. Florian Dalwigk vermittelt professionelles Rüstzeug dafür.

Der IT-Sicherheitsexperte und Dozent Florian Dalwigk führt Leser seines dicken Handbuchs systematisch ins Handwerk der Ethical Hacker und die Welt der Cybersicherheit ein.

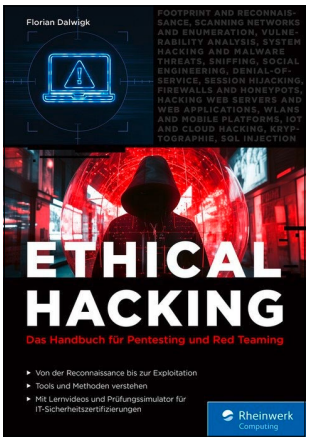
Fachjargon will beherrscht sein; so klärt der Autor wichtige Begriffe gleich am Anfang, informiert über den anerkannten Katalog von Common Vulnerabilities and Exposures (CVE) sowie über verschiedene Angriffstypen. Leser erhalten außerdem einen Überblick über die Rechtslage. Sehr schnell geht es mitten hinein in die Arbeit mit Software: Dalwigk stellt die browsergestützte Lernplattform TryHackMe vor und hilft beim Aufbau eines Hackinglabors auf Basis von VirtualBox und Kali Linux.

Während der Autor die Chronologie typischer Angriffe kapitelweise nachvollzieht, tastet er sich ans Ziel heran, die IT-Umgebung auszuspähen und Aktivitätsspuren im Netz auszuwerten. Er bedient sich zahlreicher Dienste und Suchwerkzeuge und erklärt deren Besonderheiten.

Fürs Scannen von Netzwerken kommen Tools wie hping3, Wireshark, nmap und Metasploit zum Zuge, außerdem KI-Werkzeuge, die Kommandoaufrufe dafür erzeugen. Nach einem Rundflug durch die verschlüsselte und verdeckte Kommunikation mittels Kryptografie und Steganografie hilft Dalwigk schließlich noch, Passwörter zu knacken.

Die gängigsten Sicherheitsprobleme kürt die OWASP-Organisation jährlich in ihrer Top-10-Liste. Einigen davon, beispielsweise SQL-Injections oder Cross-Site-Scripting-Attacken, widmet der Autor eigene Kapitel. Er belässt es auch nicht bei technischen Aspekten, sondern berücksichtigt insbesondere Einfallstore für Social Engineering eingehend.

Jedes Kapitel endet mit Übungsfragen und Lösungen dazu. Online stehen rund 150 Videolektionen und ein Prüfungssimulator zur Vorbereitung auf Zertifizierungsprüfungen zur Verfügung. Das Buch eignet sich daher bestens zum Selbststudium für Leute, die die Suche nach Sicherheitslücken zu ihrem Beruf machen wollen. In seiner Zielrichtung unterscheidet es sich trotz einzelner Überschneidungen vom gleichnamigen Werk desselben Autors, das 2024 bei Eulogia erschien und vorwiegend die Do-it-yourself-Programmierung eigener Werkzeuge mit Python behandelt (Buchkritik: c't 26/2025, S. 166). *(Maik Schmidt/psz@ct.de)*



Florian Dalwigk
Ethical Hacking

Das Handbuch für Pentesting und Red Teaming

Rheinwerk, Bonn 2025
ISBN 978-3836297028
855 Seiten, 50 €
(als Bundle mit E-Book beim Verlag: 50 €; PDF-/Epub-/Kindle-E-Book allein: 50 €)