1 Der Vormarsch von KI schafft neue Angriffsvektoren

Cyberkriminelle vervielfachen ihre Angriffsfläche durch KI ...

Künstliche Intelligenz revolutioniert verschiedenste Branchen weltweit. Doch gleichzeitig bietet sie auch für Cyberkriminelle nie dagewesene Möglichkeiten. Angreifende nutzen KI als Angriffsvektor für ausgeklügelte Cyberangriffe, zum Beispiel in Form von realistischen Deepfakes. Gleichzeitig erstellen sie mit ihrer Hilfe großangelegte Phishing-Kampagnen, die mit weniger Ressourcen zu größeren Gewinnen führen. Laut World Economic Forum wurde **beim Handel mit Deepfake-Tools im Darkweb zwischen Q1 2023 und Q1 2024 ein globaler Zuwachs von 223 Prozent festgestellt**.[1] Die Folgen dieses Anstiegs zeigen sich jetzt in der Realität. Erst kürzlich fiel der CEO der weltweit größten Werbe-Holding WPP einem extrem ausgeklügelten Multi-Channel-Deepfake-Angriff zum Opfer.[2] Dabei imitierten die Angreifenden mittels Voice-Cloning seine Stimme und gelangten damit an das Geld und die persönlichen Daten von Mitarbeitenden.

KI ist jedoch nicht mehr nur ein Tool, um in Organisationen einzudringen – sie vergrößert jetzt auch deren Angriffsfläche. Viele Organisationen setzen inzwischen zur Optimierung ihres Geschäftsbetriebs eigene, intern entwickelte KI-Tools ein, wie beispielsweise zur Prozessautomatisierung und zur Analyse sensibler Daten. Vielen dieser Tools fehlen jedoch die nötigen Schutzmechanismen, was sie zu einer großen Schwachstelle macht. Wenn Cyberkriminelle Zugriff auf solche Tools erlangen, können sie sensible Informationen freilegen, Schwachstellen aufspüren und Sicherheitssysteme unbemerkt umgehen – mit verheerenden Folgen für die Organisation.

... und lassen die Abwehrmechanismen von Organisationen hinter sich zurück

Laut unserer globalen Kundenumfrage rechnen 91 Prozent der Teilnehmenden damit, dass Bedrohung und Intensität KI-basierter Cyberangriffe in den nächsten drei Jahren zunehmen werden. Auch die Komplexität der Angriffe steigt – etwa durch **Verschleierungsstrategien, bei denen beispielsweise der Ursprung und die Absicht eines Angriffs mittels KI verborgen wird**.

91 Prozent der Sicherheitsexpertinnen und -experten in unserer globalen Umfrage halten es für entscheidend, solche Angriffe zu erkennen. Doch nur 26 Prozent schätzen ihre eigene Fähigkeit dazu als „hoch“ ein. KI kann selbst einen wichtigen Beitrag zur Lösung leisten – etwa durch Mitarbeitertraining mit smarten Simulationen, die zentrale Zusammenführung von Security-Alerts oder automatisierte Code-Korrektur. Mit ihrer rasanten Entwicklung ist KI nicht nur ein zunehmendes Risiko, **sondern kann auch entscheidend dazu beitragen, den Schutz von Organisationen zu stärken**.

> Wir sollten Künstliche Intelligenz nicht nur zur Bekämpfung ihrer Gefahren einsetzen, sondern sie auch nutzen, um uns durch gezieltes Training auf mögliche Szenarien vorzubereiten.

Frank Schätzing
Science-Fiction-Bestsellerautor

1 **World Economic Forum (2025).** Global Cybersecurity Outlook.
2 **New York Post (2024).** CEO of WPP, world's biggest advertising agency, falls victim to elaborate deepfake scam.