Cybersecurity
KI verändert die Bedrohungslandschaft, aber nicht die Bedrohung selbst

Künstliche Intelligenz verändert, wie Angriffe ablaufen. Die Grundkategorien der Cyberbedrohungen bleiben dabei gleich, doch ihre Reichweite, Geschwindigkeit und Wirkung nehmen zu.

Künstliche Intelligenz sorgt in der Cybersicherheit für Besorgnis. In Medienberichten ist häufig von «neuen» Gefahren die Rede, von lernenden Schadprogrammen und täuschend echten Phishing-Mails. Tatsächlich hat sich an den eigentlichen Bedrohungen aber nichts verändert. Die Ziele von Angreifern sind dieselben – Informationen stehlen, Systeme stören oder Vertrauen untergraben. Hinzugekommen ist ein neues Werkzeug. KI wirkt wie ein Verstärker: Sie beschleunigt bekannte Angriffe, macht sie glaubwürdiger und schwerer erkennbar (vgl. «Natural Language Processing», S. 58). Um die Bedrohungslage richtig einzuordnen, lohnt sich ein Blick auf die zentralen Begriffe.

Was Bedrohungen wirklich sind

In der Sprache der Sicherheitsnormen bezeichnet eine Bedrohung ein potenzielles Ereignis, das Schaden verursachen kann. Eine Bedrohung ist also nicht der Angriff selbst, sondern die Möglichkeit, dass etwas Schlimmes geschieht. Erst wenn eine Bedrohung auf eine Schwachstelle trifft, wird sie zu einem Angriff. Der Angriff ist die Handlung, mit der jemand versucht, eine Bedrohung umzusetzen – etwa durch das Versenden einer Phishing-Mail. Das Werkzeug schliesslich ist das Mittel, das Angreifer verwenden, um den Angriff durchzuführen: Schadsoftware, Botnetze oder KI-gestützte Text- und Bildgeneratoren.

Die bekanntesten Bedrohungskategorien sind seit Jahren dieselben: Manipulation von Menschen durch Social Engineering, Schadsoftware, Angriffe auf Netzwerke und Systeme, Blockaden durch DDoS-Attacken sowie Datenabfluss durch Fehlverhalten oder böswillige Insider. Jede dieser Kategorien beschreibt, was gefährdet ist – Vertraulichkeit, Integrität oder Verfügbarkeit – und auf welchem Weg der Schaden entstehen kann. Diese Systematik hat sich bewährt, weil sie stabil bleibt, auch wenn sich Technologien verändern. Organisationen der Cyberabwehr bewerten Risiken weiterhin nach ihrem Ursprung, anstatt auf technische Trends zu reagieren. Eine Phishing-Mail bleibt eine Täuschung, egal ob sie von einer betrügerischen Person oder von einer KI formuliert wurde. Entscheidend ist, bei der Abwehr darauf zu setzen, dass die Täuschung als solche erkannt wird. Ein Fokus auf KI als Werkzeug der Täuschung lenkt von den wesentlichen Aspekten ab und spielt den Angreifern in die Hände.

Warum KI keine neuen Gefahren schafft, aber alte verstärkt

Nach aktuellem Stand der Forschung – und darin sind sich Fachleute einig – entstehen durch KI keine neuen Bedrohungskategorien. KI ändert weder die Grundprinzipien der Informationssicherheit noch die Schutzziele. Sie kann aber Angriffe automatisieren, personalisieren und skalieren. Der Unterschied liegt also nicht in der Art der Gefahr, sondern in ihrer Dynamik.

Beim Social Engineering verrieten sich gefälschte Mails oft durch fehlerhafte Sprache oder unpassende Formulierungen. KI kann diese Schwächen beseitigen. Täuschend echte Nachrichten im Stil des Vorgesetzten oder realistische Deepfake-Anrufe erhöhen die Wahrscheinlichkeit, dass Mitarbeitende darauf reagieren. Aber verstehen wir den Kern der Bedrohung, dann ist die Abwehr klar: Wir müssen verifizieren, mit wem wir kommunizieren (vgl. «Elektronische Identität», S. 32). Ähnlich im Bereich Schadsoftware: KI kann bekannten Schadcode verändern, um ihn schwerer erkennbar zu machen. Doch die Bedrohung bleibt gleich – Systeme kompromittieren, Daten verschlüsseln, Geld erpressen.

Insgesamt erhöht KI die Geschwindigkeit von Angriffskampagnen und erschwert die Erkennung. Auch wenn die Einstiegshürden ziemlich sicher sinken, ist für gezielte Angriffe auf lange Sicht trotzdem ein hohes Mass an Verständnis über die angegriffenen Systeme notwendig. Gleichzeitig steht KI auch der Verteidigung zur Verfügung – etwa für die automatisierte Erkennung von Anomalien in Netzwerken oder das frühzeitige Entlarven gefälschter Inhalte.

Unsere Empfehlungen

1. Verständnis schaffen
Schulen Sie Führungskräfte und Mitarbeitende gezielt in der Unterscheidung von Bedrohung, Angriff und Werkzeug. Nur wer die Konzepte versteht, kann Risiken richtig bewerten.

2. Resilienz stärken
Bestehende Schutzmassnahmen – insbesondere im Bereich Awareness, Patchmanagement und Notfallvorsorge – bleiben wirksam, müssen aber konsequenter umgesetzt werden.

3. KI verantwortungsvoll nutzen
Prüfen Sie, wie KI-Tools selbst zur Erkennung und Abwehr von Angriffen beitragen können. Legen Sie klare Regeln für deren Einsatz fest.

Mehr Informationen

Kontaktmöglichkeiten
und weitere Informationen
zu Cybersecurity:
bfh.ch/ipst/cyber-security

Kontakt

Prof. Dr. Sebastian Höhn
Dozent

sebastian.hoehn@bfh.ch
T +41 31 848 44 26