IT-MARKT

netzmedien

IT-MARKT.CH | DIE INFO-DREHSCHEIBE FÜR DEN SCHWEIZER IT-CHANNEL | N° 08 2025

PRO-AV KONKRET

Cybersecurity

Die Ransomware-Bande Akira greift vermehrt Schweizer Unternehmen an und findet fast täglich ein Opfer.

Seite 10

Event

Die IT-SA 2025 hat die Messlatte höher gelegt. Schweizer Aussteller sagen, wie sie die Messe erlebt haben.

Seite 15

Marktübersicht

Wie Unternehmen die beste Security-Lösung für ihre spezifischen Anforderungen finden, zeigt die Marktübersicht.

Seite 28

« Rechnen Sie damit, dass Sie irgendwann gehackt werden! »

Paul Such, Swiss Post Cybersecurity. Ab Seite 20

Podium

Experten diskutieren im Podium darüber, wie viel künstliche Intelligenz die Cyberabwehr heutzutage erfordert.

Seite 30

Was Kunden wollen

Sensirion hat bei der Zusammenarbeit mit IT-Partnern klare Vorstellungen: massgeschneiderte KI und Security.

Seite 40

15 Jahre IT-MARKT

BILD: REALSTOCK1 - STOCK.ADOBE.COM

So viel KI braucht die Cyberabwehr

Wird sich künstliche Intelligenz (KI) künftig komplett im Alleingang um die Cybersecurity kümmern? Vermutlich nicht. Aber da auch die Gegenseite KI nutzt, ist sie schon heute integraler Bestandteil der IT-Security geworden. Wie viel KI die Cyberabwehr braucht, sagen Experten von Arctic Wolf, Check Point, Eset, FHNW, Fortinet, G Data, OST, Palo Alto Networks, PXL Vision und Trend Micro. Interviews: Coen Kaat

Michael Born
CEO, PXL Vision

Wie viel KI braucht die Cyberabwehr?
Michael Born: Eine effiziente und effektive Cyberabwehr ist heute ohne KI nicht mehr denkbar. Grundsätzlich verbessert KI die Sicherheit in den verschiedensten Bereichen. Wie viel KI letztlich sinnvoll ist, kann je nach Anwendungsfall und Bedrohungspotenzial variieren.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
Besonders nützlich ist KI, wenn menschliche Fähigkeiten an ihre Grenzen stossen, etwa aufgrund mangelnder Konzentration, Ermüdung, subjektiver Wahrnehmung oder schierer Datenmengen. Insbesondere bei der kontinuierlichen Analyse grosser Datenströme, dem Erkennen subtiler Anomalien und dem Identifizieren verdächtiger Muster kann KI wesentlich schneller und konsistenter agieren als ein Mensch. KI wird zudem besonders relevant, wenn auch die Angreiferseite KI nutzt, um Sicherheitsmechanismen gezielt auszutricksen, etwa durch das Fälschen von Ausweisdokumenten oder das Generieren täuschend echter Deepfake-Bilder. In solchen Fällen ist ein rein manuelles Vorgehen nicht mehr ausreichend.

Wo sind die blinden Flecken der KI?
Wenn es um Kontext, Kreativität oder ungewohnte Situationen geht, die ein menschliches Verständnis erfordern. KI trifft Entscheidungen ausschliesslich auf Basis des Gelernten und besitzt weder Intuition noch Kontextverständnis. Daher müssen Sicherheitsalgorithmen sorgfältig entworfen werden. Zudem kann KI einfache Unstimmigkeiten oder völlig neue Angriffsmuster übersehen, wenn diese ausserhalb ihrer Trainingsdaten liegen.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
Eine rein KI-gesteuerte Abwehr wäre fahrlässig, da Maschinen ohne menschliches Urteil weder Kontext noch Prioritäten verlässlich bewerten können. Am wirksamsten ist daher eine Kombination aus Mensch und Maschine: Die KI analysiert schnell, während Menschen Frameworks definieren und bei Bedarf steuernd oder korrigierend eingreifen.

Elier Cruz
Global Enterprise Security Architect, Check Point Software Technologies

Wie viel KI braucht die Cyberabwehr?
Elier Cruz: Die Cyberabwehr hängt heute mehr denn je von KI ab. Mit exponentiell zunehmenden Bedrohungen – allein in der Schweiz stiegen die Angriffe im ersten Quartal 2025 um 113 Prozent – ist KI inzwischen eine entscheidende strategische Komponente und nicht nur ein Werkzeug. KI lässt sich in alle vier Phasen des adaptiven Sicherheitszyklus integrieren: Vorhersage, Prävention, Erkennung und Reaktion. Ziel ist es nicht nur, Bedrohungen schneller zu erkennen, sondern sie proaktiv zu verhindern.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
KI ist besonders effektiv bei der Automatisierung repetitiver Aufgaben, der Analyse grosser Datenmengen und der Erkennung komplexer Angriffsmuster in Echtzeit.

Wo sind die blinden Flecken der KI?
KI ist keine magische Lösung. Ihre Modelle verhalten sich oft wie Blackboxes – undurchsichtig und schwer zu interpretieren. Ausserdem kann KI durch manipulierte Daten (Data Poisoning) oder gezielte Fehlinformationen getäuscht werden. Die Wirksamkeit von KI hängt stark von der Qualität ihrer Daten ab – schlechte Daten führen zu schlechten Entscheidungen. Daher ist es entscheidend, dass KI-Governance mit Standards und Best Practices übereinstimmt.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
KI ersetzt die Cybersecurity nicht, sie verbessert sie. Menschliche Expertise bleibt unverzichtbar, insbesondere für strategische Bewertungen und die Bewältigung neuer Bedrohungen. KI hilft, repetitive Aufgaben zu automatisieren, aber qualifizierte Fachkräfte werden weiterhin benötigt – insbesondere bei der Implementierung von Agentic AI. Der anhaltende Fachkräftemangel in der Cybersecurity besteht fort; KI mildert ihn, beseitigt ihn aber nicht.

Alle Interviews finden Sie auch online
it-markt.ch

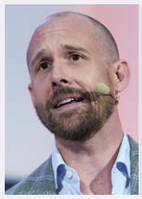
Michael Schröder
Head of Product Marketing, Eset Deutschland

Wie viel KI braucht die Cyberabwehr?
Michael Schröder: So viel, wie sinnvoll nötig, ohne Hype! Im Zuge der heutigen Bedrohungslage wird der Einsatz von KI-Werkzeugen vor allem im Hinblick auf die zielgerichteten, perfiden Methoden, die Vielzahl der Angriffe/Vektoren und die zeitkritische Komponente der Analyse immer wichtiger. Wir brauchen KI überall dort, wo sie Menschen unterstützt und in ihrem Alltag entlastet. Der Alltag von IT-Entscheidern ist vollgepackt mit täglichen Ereignissen, Compliance und gesetzlichen Anforderungen. Alles, was sie und ihr Team befähigt, effektiver zu arbeiten und sich auf wesentliche Tasks zu konzentrieren, ist sinnvoll.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
Immer dort, wo sie den Menschen zweckgebunden unterstützt, Zeit einspart sowie fehlende Ressourcen oder Kompetenzen ergänzen kann. Besonderes Augenmerk liegt auf der Zusammenführung und Interpretation von Analyseergebnissen. Hier ist KI zukünftig ebenso unverzichtbar wie in der aktiven Betrachtung von Ereignissen.

Wo sind die blinden Flecken der KI?
Unbeaufsichtigtes Lernen bei KI und deren Modellen halte ich für extrem kritisch. Hier benötigen wir die menschliche Expertise, um die richtigen Reaktionen für MDR-Services abzuleiten, aber auch, um die Fehlertoleranz (False Positives) niedrig zu halten. Letztlich darf KI allein nicht die einzige Entscheidungsgrundlage sein. Vielmehr soll sie immer nur einen Baustein in einer vielschichtigen Strategie darstellen. Denn es gibt schon heute Angriffe mittels etwa «Prompt Injection», um hier neue Angriffsvektoren zu schaffen.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
Tatsächlich gibt es Marktbegleiter, die diese Thematik gern als Werbe-Claim nutzen und vermitteln: KI könne zukünftig einen Grossteil der Mitarbeitenden ersetzen. Ich persönlich glaube nicht an diese These – haben wir doch heute bereits einen regelrechten Mangel an Fachkräften und kaum freie Ressourcen für Projekte. Ich sehe immer wieder in Projekten, wie weit wir von einem optimalen Stand der IT-Sicherheit in Unternehmen und Behörden entfernt sind, und hoffe vielmehr darauf, dass wir nun eine Chance bekommen, diese Missstände aufzuarbeiten. Im Übrigen teilen viele Koryphäen in Forschung und Lehre die Einschätzung, dass KI weiterhin ein Werkzeug bleibt und dass wir Szenarien wie eine «Superintelligenz» noch lange nicht zu fürchten haben. Schon allein die explodierenden Energiekosten für diesen Wettlauf im Verhältnis zur «zahlenden Kundschaft» stehen in keinem Verhältnis.



Andy Weiss
Regional Vice President for Switzerland & Austria, Palo Alto Networks

Wie viel KI braucht die Cyberabwehr?
Andy Weiss: Lassen Sie es mich anhand von Zahlen verdeutlichen: Im vergangenen Jahr hat unsere Plattform täglich 2,3 Millionen neue, zuvor unbekannte Angriffe erkannt. Inzwischen ist die Zahl auf 8,9 Millionen gestiegen. Angesichts dieser Dynamik ist klar, dass Unternehmen ohne den Einsatz von KI und Automatisierung kaum noch mit der Geschwindigkeit der Angreifer Schritt halten können.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
Aktuell können Analysten nur ungefähr die Hälfte aller generierten Alarme im Security Operations Center (SOC) bearbeiten, da für die restlichen Meldungen die Kapazitäten fehlen. Hier kann agentenbasierte KI Abhilfe verschaffen, indem sie wiederkehrende Aufgaben übernimmt, Alarme kategorisiert, Kontextinformationen anreichert und erste Untersuchungsschritte einleitet. Gleichzeitig eröffnen KI-Technologien grosse Chancen, etwa in Form von schnellerer Erkennung von Bedrohungen, geringeren Fehlalarm-Quoten oder tieferen Einblicken in das Netzwerkverhalten.

Wo sind die blinden Flecken der KI?
Der Erfolg KI-basierter Sicherheitslösungen steht und fällt mit der Datenqualität. Daher sind umfangreiche Trainingsdaten unerlässlich, die das gesamte Spektrum möglicher Bedrohungsszenarien und Angriffsmuster abbilden. Diese Datenbasis ermöglicht es, KI-Systeme zu entwickeln, die sowohl präzise Vorhersagen treffen als auch effektive Abwehrmassnahmen einleiten können.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
Durch KI ändern sich die Aufgaben von Sicherheitsteams. Anstatt der weniger beliebten und zeitintensiven Aufgaben wie der Analyse von Alarmen nach dem Schema «False Positive» und «True Positive» übernehmen sie nun komplexere Themen und treffen finale Entscheidungen. Das Ziel ist eine autonome SOC-Plattform, die von menschlicher Expertise geleitet wird und fortlaufend dazulernt.

Benjamin Zulliger
CISO, Fachhochschule Nordwestschweiz

Wie viel KI braucht die Cyberabwehr?
Benjamin Zulliger: KI ist in der Cyberabwehr zu einer guten Unterstützung geworden. Angreifer nutzen bereits massiv KI-gestützte Tools für Phishing, Malware-Entwicklung und automatisierte Angriffe. Wer jetzt nicht mit der Integration von KI in seine Sicherheitsstrategie beginnt, wird bald einem exponentiellen Aufholbedarf gegenüberstehen.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
Besonders wertvoll ist der Einsatz von KI zur Unterstützung der Endbenutzer bei der Phishing-Erkennung. Wir ermutigen unsere Studierenden und Mitarbeitenden aktiv, KI zu nutzen, um verdächtige E-Mails zu analysieren und deren Legitimität zu beurteilen. Dabei ist es jedoch empfehlenswert, eine geschlossene KI-Instanz zu verwenden, um den Datenschutz zu gewährleisten und sensible Unternehmensdaten nicht an externe Dienste zu übermitteln.

Wo sind die blinden Flecken der KI?
KI hat einen wesentlichen blinden Fleck: Sie basiert zurzeit noch primär auf bestehendem Wissen und historischen Daten, was ihre Fähigkeit einschränkt, völlig neue Angriffstechniken oder Zero-Day-Exploits zu erkennen. Deshalb bleibt die Kombination aus KI-gestützter Analyse und menschlicher Expertise unverzichtbar, um auch neuartige Bedrohungen zu identifizieren.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
Zum Glück wird KI in naher Zukunft nicht die komplette Cybersecurity übernehmen. Sie kann unterstützen, erzählt aber auch in vielen Fällen Unsinn oder täuscht sich. Da die IT-Landschaften komplexer werden und die Angriffe in Vielfalt und Raffinesse zunehmen, braucht die Cyberabwehr mehr, nicht weniger qualifizierte Mitarbeitende. KI ist ein kraftvolles Werkzeug zur Effizienzsteigerung, ersetzt aber nicht das kritische Denken, die Kreativität und die Entscheidungskompetenz menschlicher Sicherheitsexpertinnen und -experten.

Sebastian Schmerl
RVP Security Services EMEA, Arctic Wolf

Wie viel KI braucht die Cyberabwehr?
Sebastian Schmerl: Künstliche Intelligenz ist heute unverzichtbar, um der Geschwindigkeit und Komplexität moderner Angriffe standzuhalten. Sie hilft, Millionen von Ereignissen in Echtzeit zu analysieren und Muster zu erkennen, die für Menschen kaum erfassbar wären. KI-gestützte Systeme reduzieren täglich Milliarden von Telemetriedaten auf nur noch wenige relevante Warnungen – das entlastet Security-Teams und beschleunigt Reaktionen erheblich. Entscheidend ist jedoch das richtige Mass: KI unterstützt, ersetzt aber nicht die menschliche Urteilsfähigkeit.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
Besonders effektiv ist KI bei der frühen Erkennung und Priorisierung von Bedrohungen. Sie hilft, Fehlalarme zu minimieren und verdächtige Aktivitäten schneller zu verifizieren. Auch in der Automatisierung von Routineaufgaben – etwa beim Schwachstellen- oder Log-Management – bringt sie enorme Effizienzgewinne. Richtig eingesetzt schafft sie Freiräume, damit sich Security-Experten auf komplexe Analysen und strategische Entscheidungen konzentrieren können.

Wo sind die blinden Flecken der KI?
KI erkennt Muster, aber keine Absichten. Sie kann also technische Anomalien identifizieren, nicht aber menschliches Fehlverhalten oder bewusste Täuschung. Unser Human Risk Report 2025 zeigt, dass viele Mitarbeitende KI-Tools wie ChatGPT im Arbeitsalltag nutzen – häufig ohne die Sicherheitsrichtlinien ihres Unternehmens zu kennen. Genau hier liegen die Grenzen: Ohne Schulung, klare Prozesse und menschliche Kontrolle bleibt jedes Modell anfällig für Fehlinterpretationen.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
KI übernimmt keine Verantwortung – sie ist ein Werkzeug. Menschen bleiben essenziell, um Ergebnisse zu interpretieren, Prioritäten zu setzen und ethische Grenzen zu wahren. Die Zukunft liegt in hybriden Teams, in denen Technologie Routinearbeiten übernimmt und automatisiert und IT-Fachkräfte strategische Entscheidungen treffen. So entsteht echte Cyberresilienz – durch das Zusammenspiel von KI und menschlichem Urteilsvermögen.

Stefan Züger
Director Systems Engineering, Fortinet Schweiz

Wie viel KI braucht die Cyberabwehr?
Stefan Züger: KI ist Fluch und Segen zugleich. Sie transformiert Branchen und steigert die Effizienz, birgt aber ohne wirksame Governance Risiken wie Verstösse gegen Vorgaben, Datenmissbrauch und Reputationsschäden. Gleichzeitig revolutioniert KI das Vorgehen von Cyberkriminellen: Sie beschleunigen ihre Operationen massiv und investieren mehr Zeit in Planung und Aufklärung für gezieltere, verheerendere Angriffe. Um dieser Bedrohungslage zu begegnen und Cybersecurity-Operationen zu vereinfachen, ist KI ein unverzichtbarer Eckpfeiler moderner Verteidigungsstrategien.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
Dort, wo Sicherheitsteams an ihre Grenzen stossen. Analysten werden täglich mit Tausenden Alerts überflutet. GenAI filtert das Rauschen, korreliert Ereignisse und hebt kritische Bedrohungen hervor. Statt roher Logs erhalten sie klare Zusammenfassungen mit Schweregrad und Auswirkung – das beschleunigt die Reaktionszeit erheblich. KI-gestützte Systeme identifizieren zudem Zero-Day-Exploits in Echtzeit, die traditionelle Tools übersehen würden, decken Shadow-AI auf und unterstützen bei Risikobewertung sowie Compliance. Kurz: Teams werden schneller, präziser und können sich auf strategisch relevante Bedrohungen konzentrieren.

Wo sind die blinden Flecken der KI?
Vielen Nutzern fehlt das Fachwissen für sicheren KI-Einsatz, das zeigt unser aktueller Skills Gap Report. 76 Prozent der befragten Unternehmen erlitten 2024 neun oder mehr Cyberangriffe – trotz KI-Nutzung. Gleichzeitig sinkt die Bereitschaft, Mitarbeiterzertifizierungen zu finanzieren. Dieser Mangel an Expertise und Governance – fehlende Prozesse, Rollen und Weiterbildung – ist das grösste Hindernis für effektive Cybersecurity mit KI.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
Nein – qualifiziertes Personal ist wichtiger denn je. KI automatisiert Routinen und beschleunigt Analysen, ersetzt aber nicht strategische Entscheidungen und Governance. Fortinets Skills Gap Report zeigt: 48 Prozent der Organisationen fehlt KI-Expertise, 47 Prozent können Tools ohne Fachkräfte nicht effektiv nutzen. Ohne geschultes Personal vergrössern KI-Lösungen sogar Schwachstellen. Das ist kritisch, da 49 Prozent befürchten, dass Angreifer KI für intensivere Attacken nutzen. Die Arbeit verändert sich: Fachkräfte konzentrieren sich auf Überwachung, Risikomanagement und KI-Sicherheit. Human Capital bleibt essenziell.

Christian Thiel
Studiengangsleiter Wirtschaftsinformatik MSc, Ostschweizer Fachhochschule

Wie viel KI braucht die Cyberabwehr?
Christian Thiel: So viel, wie messbar Nutzen bringt – und niemals ohne Governance. In der Praxis bedeutet das, KI gezielt dort einzusetzen, wo Volumen und Geschwindigkeit menschliche Kapazitäten übersteigen: bei der Triage von Alarmen, der Anreicherung von Kontextdaten, der Mustererkennung in Netzwerk- und Log-Daten oder der Phishing-Abwehr. Der Grundsatz bleibt «Human-in-the-Loop»: Die KI entlastet und beschleunigt, aber der Mensch trifft die finale Entscheidung. Etablierte Rahmenwerke wie das NIST AI RMF – National Institute of Standards and Technology Artificial Intelligence Risk Management Framework – oder die Norm ISO/IEC 42001 sorgen dafür, dass Risiken wie Daten-Drift, mangelnde Erklärbarkeit und Transparenz von Anfang an mitgedacht und durch kontinuierliches Monitoring und Red-Teaming beherrschbar bleiben. Kurz gesagt: punktuell hochautomatisieren, aber immer mit klaren Zielen, Metriken und Leitlinien.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
Der grösste Nutzen zeigt sich in der gesamten Abwehrkette, von der Prävention bis zur Reaktion. Konkret sind das Bereiche wie E-Mail- und Phishing-Abwehr: Analyse von Texten, Bildern und Audiodateien, um Social Engineering und sogar Deepfake-Indizien zu erkennen; Anomalie- und Verhaltenserkennung – UEBA User and Entity Behavior Analytics –: Identifikation von untypischem Nutzer- oder Systemverhalten, das auf laterale Bewegungen im Netzwerk oder missbrauchte Privilegien hindeutet; SOC-Automatisierung: KI dedupliziert Alarme, reichert sie mit Kontext zu Assets, Schwachstellen und Bedrohungsdaten an, fasst komplexe Fälle für Analysten zusammen und steuert automatisierte Reaktions-Playbooks – SOAR Security Orchestration, Automation, and Response –; Threat Intelligence & Hunting: Abgleich riesiger Datenmengen mit bekannten Angriffsmustern – etwa «MITRE ATT&CK», eine global zugängliche Wissensdatenbank über Taktiken und Techniken von Angreifern, basierend auf realen Beobachtungen – und Unterstützung bei der hypothesenbasierten Suche nach unbekannten Bedrohungen; oder Secure Coding & DevSecOps: KI-gestützte Überprüfung von Code, Infrastructure-as-Code (IaC) und Konfigurationen sowie die intelligente Priorisierung von Schwachstellen. Voraussetzung für all das sind saubere Datenpipelines und eine solide Zero-Trust-Architektur.

Wo sind die blinden Flecken der KI?
Die grösste Schwachstelle ist, dass die Logik der KI selbst zum Angriffsziel wird. Dieses Feld nennt sich Adversarial Machine Learning und umfasst Risiken, die in Frameworks wie «MITRE ATLAS» – Adversarial Threat Landscape for Artificial-Intelligence Systems – und den «OWASP»-Top-10 für LLMs dokumentiert sind. Dazu gehören Prompt-Injection und Datenvergiftung – Data Poisoning –, bei denen Angreifer Modelle durch manipulierte Eingaben oder Trainingsdaten gezielt in die Irre führen oder Hintertüren einbauen. Weitere blinde Flecken sind Daten- und Modell-Drift, bei denen Modelle über die Zeit an Präzision verlieren, sowie Halluzinationen, bei denen die KI Fakten erfindet, was im Sicherheitskontext fatal ist. Hinzu kommen Risiken in der Supply-Chain durch unsichere Drittbibliotheken und die ungesteuerte Nutzung von Shadow-AI durch Mitarbeitende, die unklare Datenflüsse und Datenschutzrisiken schafft.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
Nein, die Vorstellung einer vollautomatisierten Cyberabwehr ist eine Illusion. KI verlagert die Arbeit von repetitiven Level-1-Aufgaben hin zu hochkomplexer Level-2/3-Analyse, Engineering, Governance und proaktivem Threat-Hunting. Die Rollen ändern sich fundamental: SOC-Analysten werden zu Automations- und Playbook-Designern und neue Profile wie AI-Security-Engineers, Model-Risk-Manager und spezialisierte Red-Teams für KI entstehen. Personell bedeutet das: Wir brauchen gleich viel oder sogar mehr Kompetenz, aber anders verteilt. Eine vollautomatisierte Abwehr ohne menschliche Aufsicht, strategische Weitsicht und ethische Kontrolle ist in sicherheitskritischen Umgebungen weder realistisch noch verantwortbar. Der Mensch bleibt die letzte Instanz für Kontext, Kreativität und kritische Entscheidungen.

Cornelia Lehle
Head of Sales DACH,
G Data Cyberdefense

Wie viel KI braucht die Cyberabwehr?
Cornelia Lehle: Es ist weniger eine Frage der Quantität als vielmehr eine Frage der Qualität. Denn der Einsatz von Large Language Models, kurz LLM, hat Vor- und Nachteile. Den Effizienzgewinnen stehen häufig ungenaue, unzuverlässige oder fehlerhafte Ergebnisse entgegen. Und noch immer haben die Trainingsdaten einen entscheidenden Einfluss auf die Ergebnisse. Wer also sein Modell mit minderwertigen Daten füttert, erhält am Ende falsche oder ungenaue Ergebnisse. Das hilft bei der IT-Sicherheit keinem weiter.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
Die grosse Stärke von KI-basierten Systemen ist die schnelle Verarbeitung grosser Datenmengen. Es gibt in der Malware-Analyse viele sinnvolle und hilfreiche Einsatzgebiete für KI. Der Einsatz als Filter, der auf grossen Datenmengen basiert, oder die Priorisierung von Aufgaben erleichtert Malware-Fachleuten die Arbeit. Dem steht aber entgegen, dass KI Fehler macht. Die mangelnde Präzision erschwert den Einsatz von KI in Bereichen, wo akkurate Ergebnisse erforderlich sind, wie etwa bei der Analyse des Codes. Die abschliessende Entscheidungs- und Interpretationshoheit sollte daher immer beim Menschen liegen.

Wo sind die blinden Flecken der KI?
KI, die den Code erklärt, zum Beispiel bei Virustotal für Powershell-Skripte, finde ich nicht hilfreich. In der Regel kennt KI den Kontext nicht, in dem diese Skripte aufgerufen und verwendet werden. So können legitime Skripte ohne Kontext tatsächlich bösartig aussehen, weil die Aktionen, die Administratoren durchführen, mitunter den Aktionen von Eindringlingen sehr ähnlich sind. Es kommt immer darauf an, wer etwas benutzt und warum. Eine LLM-basierte Erklärung, die nun ein Verstehen dieser Skripte besser zugänglich machen soll, erreicht dabei eher das Gegenteil. Diese Erklärungsansätze erzeugen für Malware-Analysten unnötige Arbeit, da mehr vermeintliche False-Positive- und False-Negative-Meldungen auflaufen, die ein Mensch dann erst einmal ansehen und widerlegen muss.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
Ich gehe nicht davon aus, dass künstliche Intelligenz in naher Zukunft unsere gesamte Cybersecurity übernehmen kann und wird. Denn die Anzahl der Angriffsversuche wird nicht nur steigen, sondern auch weiterhin an Komplexität gewinnen. Deswegen braucht es weiterhin einen prüfenden Blick von menschlichen Experten, um Fehler zweifelsfrei auszuschliessen. Es bleibt noch viel zu tun, bis Maschinen die Aufgabe der Menschen übernehmen können. Ein ganzheitlicher Ersatz für menschliche Analysten und Analystinnen wird KI meiner Meinung nach nicht werden.

Richard Werner
Security Advisor,
Trend Micro

Wie viel KI braucht die Cyberabwehr?
Richard Werner: KI ist heute bereits ein integraler Bestandteil jeder IT-Sicherheitsarchitektur. Sie entfaltet ihre Stärken dort, wo grosse Datenmengen in kürzester Zeit analysiert oder wiederkehrende Aufgaben automatisiert werden müssen. Bei umfassenden Analysen ist sie unverzichtbar. Für Unternehmen bedeutet der Einsatz von KI präzisere Beurteilungen bei gleichzeitiger Kosteneinsparung.

Bei welchen Aufgaben bietet KI den grössten Nutzen?
Unternehmen sind zunehmend aufgefordert, ihr Cyber-Sicherheitsrisiko zu managen. Jede Unternehmensführung sollte das Geschäftsrisiko eines Cybervorfalls beurteilen. Schliesslich verantwortet sie mit Budget und Personal, wie viel zur Absicherung dieses Risikos getan wird. Risiken zu berechnen, in den richtigen Kontext zu stellen und für Menschen verständlich zu erklären, wird eine der Hauptaufgaben von KI werden.

Wo sind die blinden Flecken der KI?
Der wichtigste Punkt ist und bleibt, dass KI keine Verantwortung im juristischen Sinne übernehmen kann. Sie kann lediglich die Entscheidungsfindung von Menschen unterstützen. Auf technischer Ebene ist festzustellen, dass eine KI stark von ihren Trainingsdaten abhängig ist. Eine auf IT-Sicherheit spezialisierte KI kann beispielsweise nur mit den verfügbaren Angriffsmustern trainiert werden. Neue Attacken, sogenannte Zero Days, sind deshalb auch für eine KI nur schwer identifizierbar.

Übernimmt die KI nun die komplette Cybersecurity? Wie viele Mitarbeitende braucht es jetzt noch in der Abwehr?
KI wird viele der aktuellen Herausforderungen von Cyber-Sicherheitsabteilungen lösen und unter anderem genauere Risikoeinschätzungen und schnellere Reaktionszeiten ermöglichen. Sie wird auch mittelständische Unternehmen dazu befähigen, fortschrittliche Cyber-Sicherheitsoperationen durchzuführen. Insgesamt wird KI die Arbeit aktueller Cybersicherheitsabteilungen stark vereinfachen, aber nicht überflüssig machen.