Strategien für eine wirkungsvolle Cybersicherheit

Braucht es künstliche Intelligenz in der OT-Sicherheit?

Künstliche Intelligenz (KI) scheint heute als Allheilsbringer für den Umgang mit Unsicherheit und Komplexität gehandelt zu werden. Auch Anbieter industrieller Cybersicherheitslösungen proklamieren zunehmend, KI in ihren Lösungen zu verwenden. Dabei ist zum einen nicht alles, was Algorithmen verwendet, KI. Zum anderen stellen Forschungsergebnisse die Effizienz von KI in industriellen Umgebungen infrage. Nicht überall, wo Daten fließen, passt auch KI drauf.

In der Technologiewelt geht nichts mehr ohne KI. Wo Daten fließen, wird KI als Wundermittel versprochen. Auch in der industriellen Cybersicherheit (nachfolgend: OT-Sicherheit) existieren längst Angebote und (nicht sehr transparente) Lösungen. Dabei gibt es bislang ausschließlich Werbeversprechen, Hypothesen und oberflächliche Argumente. Beweise gibt es wenige. Vor allem wird stets der erste Schritt übersprungen: die Frage nach dem Mehrwert von KI in OT-Sicherheitslösungen.

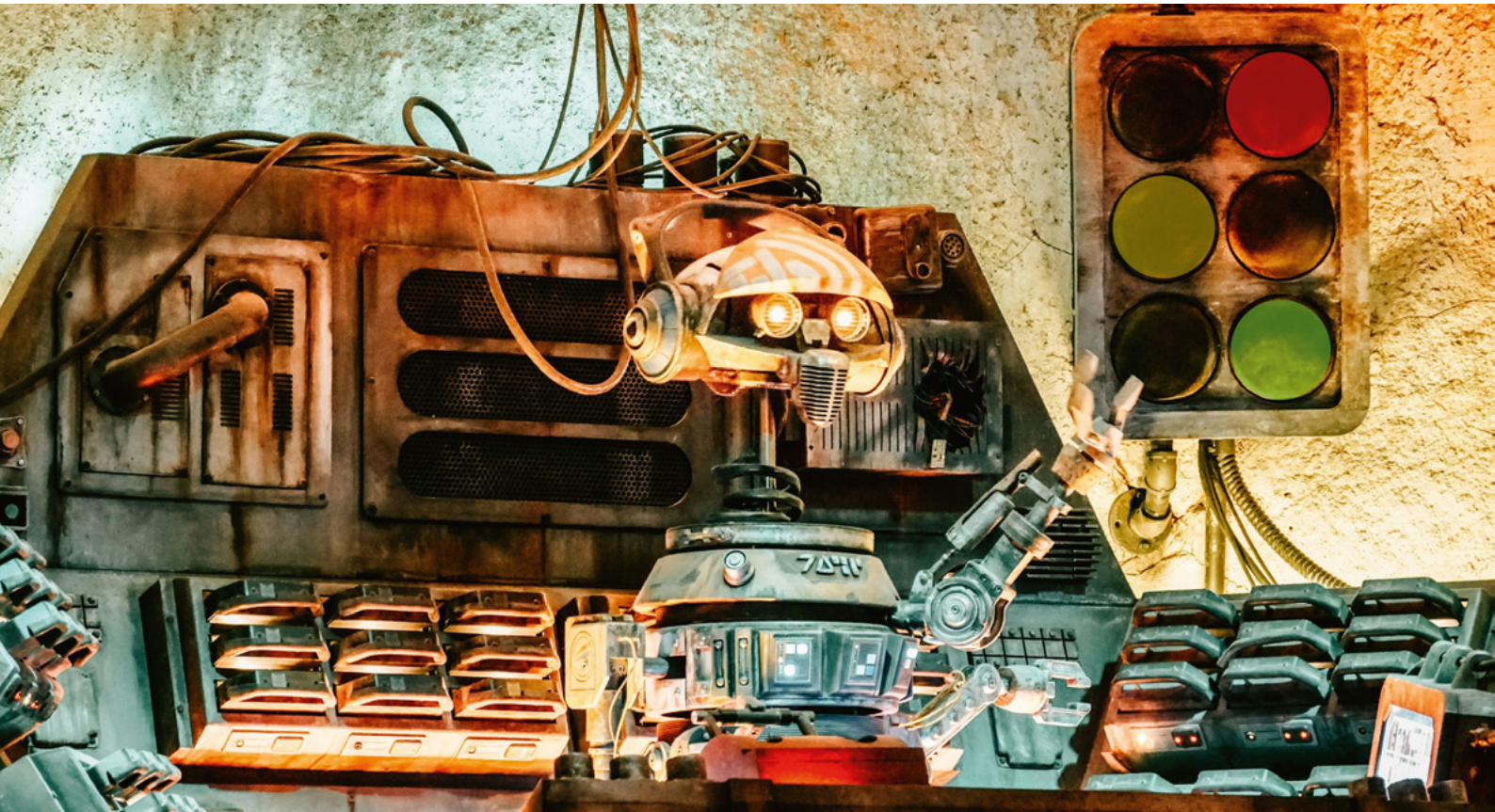
Um zu klären, ob KI die OT-Sicherheit verbessert, sollten Unternehmen sich (und den Anbietern) zwei Fragen stellen:

- Welchen Mehrwert hat KI in der OT-Sicherheit gegenüber anderen Lösungsansätzen?
- Welche Risiken birgt KI für die Stabilität und Verfügbarkeit meiner Prozesse sowie den Arbeitsschutz?

Mehrwert von KI in der OT-Sicherheit

Die Effektivität und Effizienz von KI in der OT-Sicherheit sind tatsächlich noch nicht abschließend geklärt. Das vom Bundesministerium für Bildung und Forschung unterstützte Forschungsprojekt „Hybrid AI Intrusion Prevention for Industrial Control Systems“ (HAIP) [1] erforschte zwischen 2020 und 2023 den Mehrwert von KI für die Anomalieerkennung in indus-

KI-Anwendungen können in der OT-Sicherheit mehr Unsicherheit schaffen Bildquelle: rod-long-_HRi5kBwGh0-unsplash



triellen Umgebungen. Das Forschungsteam kam in ihrem Abschlussbericht zwar zu dem Ergebnis, dass KI die Anomalieerkennung und -bewertung durchaus unterstützen kann. Jedoch lag die Performance und Genauigkeit gleichauf mit und teilweise unter anderen Methoden wie Heuristik, Statistik und Algorithmen, die durch ein Expertenteam definiert wurden.

Das Ergebnis ist nicht verwunderlich für OT-Netzwerke: Die wichtigsten Anomalien sind bereits über statistische und heuristische Methoden zuverlässig identifizierbar, da die OT-Kommunikation deterministisch und repetitiv ist. Die kommunikative Komplexität und Unvorhersehbarkeit der IT fehlen in industriellen Netzwerken. Außerdem fehlen OT-Netzen in der Regel das Datenvolumen und die Datenvariabilität, die KI braucht, um effektiv trainiert zu werden und damit einen Mehrwert durch komplexere Analysen – ohne zu viele falsch-positive Ergebnisse – zu bieten.
Stattdessen können für das OT-Monitoring mit inte-grierter Anomalie- und Angriffserkennung direkt in der OT ressourcenschonendere und genauso effektive Methoden zum Einsatz kommen:

- heuristische Methoden,
- statistische Methoden,
- Algorithmen basierend auf den Tactics, Techniques & Procedures (TTP) des Mitre Att&ck Frameworks für Enterprise und ICS,
- Algorithmen basierend auf Erfahrungswerten und Expertise in der Analyse von Cybervorfällen und OT-Netzwerken.

Gerade in industriellen Umgebungen – in der Fertigung, der Energieversorgung und insbesondere an der Edge von IoT- und IIoT-Netzen – sind die informationsverarbeitenden und -übertragenden Ressourcen eingeschränkt.

Wie das SANS-Institut in einem Beitrag im Mai 2024 anmerkte, gibt es „möglicherweise Aufgaben mit höherer Priorität innerhalb der Entwicklung und der ICS-Sicherheit, die eine höhere Investitionsrendite als die Einführung von KI zum jetzigen Zeitpunkt bieten würden“ [2].

Es gibt drei verbreitete Behauptungen zu KI-Vorteilen in der OT:

1. KI kann schneller die Baseline erstellen

Grundsätzlich kann eine KI unterstützen, um wiederkehrende Muster als Baseline für die Anomalieerkennung zu definieren. Jedoch müssen einige grundlegende Aspekte berücksichtigt werden.

Das Aufwendigste bei der Baseline-Erstellung ist nicht die Auswertung der OT-Kommunikation, sondern der Mitschnitt der OT-Kommunikation. Das Sample muss umfassend genug sein, um möglichst alle legitimen Kommunikationen (und bereits existierenden Auffälligkeiten) abzubilden. Für KI-Anwendungen können Datenvarianz und Datenqualität trotz Vollständigkeit aller Meldungen mitunter zu gering sein, um eine sichere Baseline zu definieren und bestehende Auffälligkeiten herauszufiltern. Das kann die Lernphase stark verlängern und zu fehleranfälligen Baselines führen.

Die fehlende Transparenz gewerblicher KI-Produkte kann zu einer nicht nachvollziehbaren Baseline führen. Nutzende müssen dem Ergebnis blind vertrauen. Die OT-Kommunikation unterscheidet sich stark von Unternehmen zu Unternehmen, von Netzwerk zu Netzwerk. Selbst wenn eine KI zum Einsatz kommt, bleibt das Erfahrungswissen der hiesigen OT-Experten und der jeweiligen Operatoren maßgeblich. In modernen Energieversorgungssystemen gibt es schnellere und kostengünstigere Wege zur Baseline-Erstellung. Die in IEC 61850-Infrastrukturen vorliegende .scd-Datei enthält bereits alle Informationen für eine saubere Baseline.

2. KI verbessert die Erkennung von Schwachstellen und Gefährdungen

Die Stärke von KI liegt darin, aus einer Vielzahl an Daten und Quel-

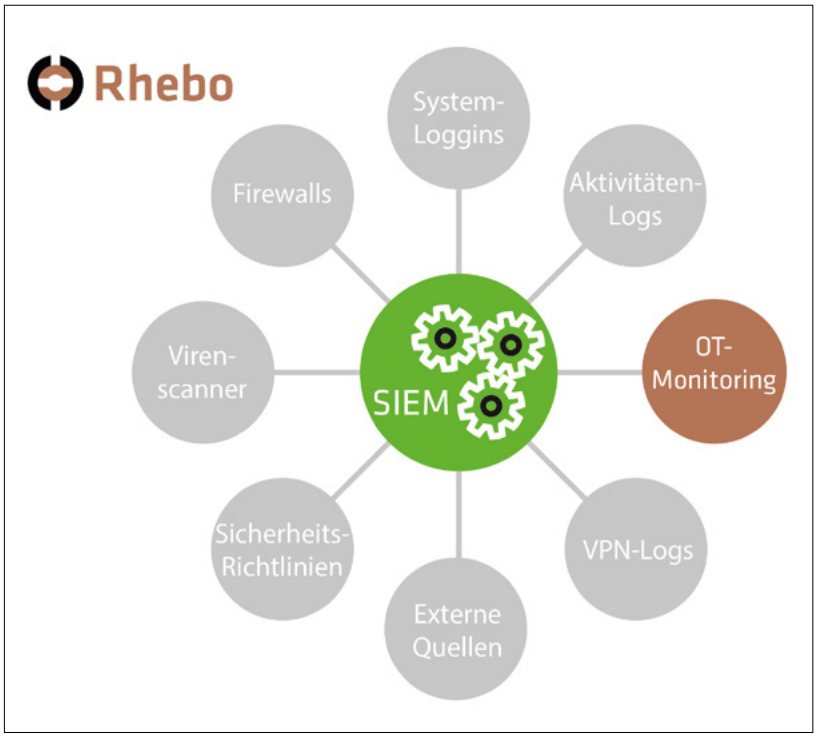


Abbildung1. KI entfaltet ihre Vorteile, wo viele unterschiedliche Datenquellen zusammengeführt werden, im SIEM Quelle: Rhebo

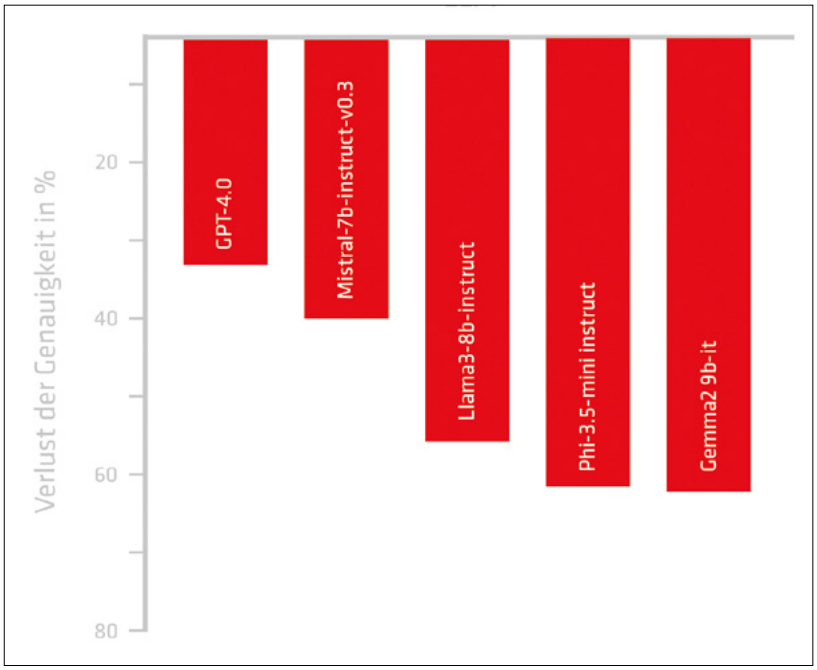


Abbildung 2. Der Genauigkeitsverlust der Ergebnisse liegt bei Aufgaben mit nicht-operativen Inhalten bei den aktuellen Versionen der Large Language Models (LLM) zwischen 32 und 63 % Quelle: [3]

len neue oder bekannte Muster zu erkennen. Der Mehrwert in der OT ist aufgrund der dort vorherrschenden deterministischen, repetitiven Kommunikation jedoch vernachlässigbar und wiegt die Nachteile (siehe unten) nicht auf. Die Gefährdungserkennung durch KI erhält erst in einem zentralen, mehrere Quellen zusammenfassenden Cybersecurity-System Gewicht.

Diese Funktionalität wird in der Regel in einem Security Information & Event Management (SIEM) System geschaffen, durch das auch mehrstufige Angriffe sichtbar werden. In der OT können die wichtigsten und meisten Anomalien jedoch sicher mit heuristischen und statistischen Methoden erkannt werden.

Für die Meldung bekannter Schwachstellen in Firmware-Versionen bedarf es keiner KI. Ein OT-Monitoring, das die in der OT aktiven Systeme samt Firmware-Stand dokumentiert und mit der CVE-Datenbank abgleicht, kann das über einfache heuristische Algorithmen bewerkstelligen.

3. KI kann den Fachkräftemangel überbrücken

KI kann in der Theorie Prozesse automatisieren. In der Praxis der OT ist das jedoch nur bedingt realistisch. Zum einen sind KI-Systeme bislang zu fehleranfällig und intransparent, um ohne engmaschige Kontrolle völlig selbstständig laufen gelassen zu werden. Das bedeutet auch, dass die Verantwortlichen neben dem ohnehin neuen Thema OT-Sicherheit auch in KI-Engineering und -Management fit sein müssen.

In der OT ist eine Automatisierung von Cybersicherheit, wie sie KI verspricht, selten erwünscht, weil falsch-positive Entscheidungen den Arbeitsschutz gefährden und durch fälschlicherweise automatisch heruntergefahrene Anlagen zu Millionenschäden führen können.

KI ergibt eine Ebene höher Sinn

KI kann jedoch im zweiten Schritt – der Integration von OT-Sicherheit in die IT-Sicherheit, insbesondere über ein zentrales SIEM-System – dabei unterstützen, Anomalien besser einzuordnen. Im SIEM werden die Logs und Eventberichte der einzelnen Cybersicherheitskomponenten (Firewalls, Virenscanner, Autorisierungsmechanismen, Anomalieerkennung) zusammengeführt und automatisiert ausgewertet. Erst an dieser Stelle schaffen komplexe Analysen durch KI einen Mehrwert (siehe Abbildung 1).

Ein OT-Monitoring mit Angriffserkennung wird damit zum wichtigen Informationslieferanten für das Gesamt-SIEM eines Unternehmens. Es schafft die lange vermisste Sichtbarkeit in die OT. Anomaliemeldungen und Sicherheitsvorfälle in der OT können an das SIEM per Schnittstelle und verschlüsseltem Syslog im Industriestandard-Format CEF übermittelt werden. Sinnvoll ist zudem eine algorithmische Vorqualifizierung der Sicherheitsevents (etwa nach den Mitre Att&ck Frameworks) durch das OT-Monitoring, um das Datenvolumen für das SIEM handhabbar zu halten.

Risiken der KI für die OT-Sicherheit

Die sichtbarste Form von KI sind derzeit Produkte wie ChatGPT, Gemma und Mistral. Sie sind aufgrund ihrer öffentlichen Nutzbarkeit auch die (einzigen) KI-Produkte, die bislang am besten unabhängig evaluiert werden können. Deshalb sollten die Ergebnisse einer Studie durch ein Forschungsteam bei Apple zu Large Language Models (LLM) bei der Risikoanalyse von KI unbedingt berücksichtigt werden [3].

Das Team untersuchte die Fähigkeiten der KI-Systeme, tatsächlich logisch zu denken und Ableitungen zu erstellen. Das sogenannte Reasoning funktionierte bei den meisten der getesteten Systeme noch sehr gut, solange die Aufgabenstellungen sich stark mit den Trainingsdaten deckten. Als die Forschenden begannen, die Aufgabenstellungen um Informationen zu erweitern, die keinerlei Einfluss auf das Ergebnis haben (sogenannte nichtoperative Informationen), stiegen die falschen Ergebnisse rasch an. Die KI-Systeme konnten also leicht abgelenkt und auf falsche Fährten gesetzt werden, da sie die Inhalte nicht im Sinnzusammenhang verstanden (siehe Abbildung 2). Das ergänzt die irritierenden Erfahrungen vieler Nutzender, in denen ChatGPT und Co. halluzinierten bzw. schlichtweg Falschaussagen getätigt haben.

In der OT-Sicherheit können diese Schwächen dazu führen, dass die Zahl der falsch-positiven Meldungen in der Angriffserkennung steigt, während echte Angriffe durch Verschleierung und Ablenkung nicht erkannt werden. Das kann nicht nur die Prozesse gefährden, sondern auch die Menschen, die an den Anlagen arbeiten.

Hinzu kommt, dass gewerbliche KI-Produkte in der Regel unter dem Deckmantel des Geschäftsgeheimnisses nicht nachvollziehbar sind. Wenn die KI etwas entscheidet, wissen die Nutzenden nicht, wie die KI zu diesem Ergebnis gekommen ist. Im Bereich der Cybersicherheit und erst recht im Bereich der OT-Sicherheit, wo Arbeitsschutz, Stabilität und Verfügbarkeit im Vordergrund stehen, ist eine Blackbox-KI tatsächlich ein No-Go. Ohne Transparenz der KI-Funktionsweise – ohne explainable AI - erhalten die Unternehmen verschleierte Cybersicherheit in einer ohnehin als Blackbox geführten OT.

Literaturhinweise:

[1] Netzwerkdaten verfügbar unter: https://fordatis.fraunhofer.de/handle/fordatis/314?locale=de
[2] https://www.sans.org/blog/ics-ot-cybersecurity-ai-considerations-for-now-the-future-part-i/
[3] Mehrdad Farajtabar et al., GSM-Symbolic: Understanding the Limitations of Mathematical Reasoning in Large Language Models, Apple, Oktober 2024

www.rhebo.com

Autor

Dr. Frank Stummer, Business Development, Rhebo GmbH, Leipzig