Künstliche Intelligenz in der OT-Sicherheit

Vertrauen statt Verunsicherung

Die Entwicklung künstlicher Intelligenz (KI) hat inzwischen auch den Bereich der OT-Sicherheit (Operational Technology) erreicht. Allerdings unterscheiden sich die Ansätze deutlich. Während viele Anbieter KI-Funktionen hastig in ihre Produkte integrieren, setzen andere zunehmend auf einen Ansatz, der Datenschutz, industrielle Anforderungen und menschliche Expertise in den Mittelpunkt stellt.

Ein Kommentar von:
Kai Thomsen
Director of Global Incident Response Services
Dragos
www.dragos.com

Je weiter sich KI-Anwendungen entwickeln, desto stärker entscheidet der verantwortungsvolle Umgang mit Transparenz und Vertrauen über nachhaltige Akzeptanz. Ziel ist es, KI so einzusetzen, dass Sicherheitsteams schneller und präziser reagieren können, ohne den Menschen als zentrale Instanz der Analyse zu verdrängen.

Leitgedanken

Drei Leitgedanken prägen den modernen Einsatz von KI in der OT-Sicherheit:

1. **KI stärkt die menschliche Analyse, sie ersetzt sie nicht.**
   Künstliche Intelligenz soll Fachkräfte nicht verdrängen, sondern ihre Arbeit gezielt verstärken. Speziell entwickelte Werkzeuge unterstützen Analysten dort, wo Geschwindigkeit, Skalierbarkeit und Wiederholbarkeit gefragt sind.
2. **Daten und Fachwissen bilden die gemeinsame Grundlage.**
   KI liefert dann die besten Ergebnisse, wenn sie auf hochwertigen, umfangreichen Daten und tiefem Fachwissen basiert. Erst die Verbindung strukturierter Informationen mit erfahrungsbasiertem Wissen ermöglicht fundierte Analysen und präzise Entscheidungen.
3. **Datenhoheit und Datenschutz sind unverzichtbar.**
   Die Verantwortung über die Daten liegt stets bei der jeweiligen Organisation. Ein transparenter Umgang mit Trainings- und Betriebsdaten sowie klare Entscheidungsfreiheit bei deren Nutzung schaffen Vertrauen und sichern die Integrität des Systems.

Zusammen bilden sie das Fundament für einen verantwortungsvollen Einsatz von KI.

Die Wissenslücke zwischen IT- und OT-Sicherheit

Ein zentrales Problem der Branche ist die fehlende Brücke zwischen IT- und OT-Sicherheitskompetenz. IT-Systeme basieren in der Regel auf standardisierten Plattformen mit etablierten Schutzmechanismen. Industrielle Systeme hingegen sind oft proprietär, mehrere Jahrzehnte alt und nicht für regelmäßige Updates ausgelegt. Während Vertraulichkeit und Verfügbarkeit in der IT im Fokus stehen, haben Sicherheit und Stabilität des laufenden Betriebs in der OT Vorrang. Schon kleinste Eingriffe in industrielle Steuerungssysteme können erhebliche Auswirkungen auf Anlagen und Menschen haben.

Diese Unterschiede erschweren es IT-Sicherheitsfachkräften, in OT-Umgebungen wirksam zu handeln. Gleichzeitig wächst der Bedarf an qualifizierten OT-Sicherheitsanalysten rapide. Laut Branchenanalysen wird der gezielte Einsatz von KI entscheidend sein, um diesen Fachkräftemangel zu überbrücken und die Resilienz cyber-physischer Systeme zu erhöhen.

Wissenslücke mit KI überbrücken

Ein auf Analysten ausgerichteter KI-Ansatz kann IT-Sicherheitskräfte dabei unterstützen, sich schneller in OT-Systeme einzuarbeiten und fundierte Entscheidungen zu treffen. Künstliche Intelligenz erleichtert den Zugang zu sicherheitsrelevanten Informationen über natürliche Sprachschnittstellen. So lassen sich OT-spezifische Bedrohungen und Schwachstellen schneller identifizieren und besser einordnen.

Gleichzeitig liefert KI gezielte Handlungsempfehlungen zur Analyse komplexer Angriffsvektoren und industrieller Protokolle. Sie strukturiert sicherheitsrelevante Zusammenhänge und beschleunigt dadurch den Entscheidungsprozess. Durch den direkten Zugriff auf hinterlegte Fachinformationen und Bedrohungsdatenbanken erweitert sie das vorhandene Wissen und macht es unmittelbar nutzbar. Darüber hinaus steigert KI die Effizienz der Sicherheitsarbeit. Sie setzt automatisch Prioritäten, bewertet Alarme und verkürzt dadurch die Reaktionszeiten bei Sicherheitsvorfällen erheblich.

Insgesamt wird KI damit zu einem Werkzeug, das vorhandenes Fachwissen gezielt ergänzt, neue Kompetenzebenen erschließt und sicherere, effektivere Arbeitsprozesse ermöglicht.

Die Zukunft der OT-Sicherheit

Die Verbindung von Künstlicher Intelligenz und OT-Sicherheit eröffnet neue Möglichkeiten, Kompetenzlücken zu schließen und sicherheitsrelevante Herausforderungen gezielter zu bewältigen. Dabei darf technologischer Fortschritt nicht zulasten von Transparenz, Fachwissen oder Datenschutz gehen. Entscheidend ist nicht die schnelle Umsetzung technischer Trends, sondern ein Ansatz, der die besonderen Anforderungen industrieller Systeme berücksichtigt und sich in bestehende Abläufe integrieren lässt.

Abgestimmtes Zusammenspiel

Eine wirksame Nutzung von KI setzt spezialisierte Werkzeuge voraus, die menschliche Expertise gezielt ergänzen und den Zugang zu sicherheitsrelevantem Wissen erleichtern. Die Zukunft der OT-Sicherheit liegt nicht in vollständiger Automatisierung, sondern im abgestimmten Zusammenspiel von Mensch und Maschine. Nur so lässt sich die Resilienz industrieller Systeme langfristig stärken. ◄