Mehr Sicherheit für Industrienetze

Intelligente Angriffserkennung durch KI-basierte Analyse

Kai-Oliver Detken

Industrienetze unterscheiden sich stark von typischen Unternehmensnetzwerken. Sie werden in Energieerzeugungsanlagen betrieben, benötigen eine 100% Verfügbarkeit und nutzen andere Protokolle wie zum Beispiel Modbus. Zudem sind sie auf große Zeitspannen ausgelegt und beherbergen daher oftmals veraltete Betriebssysteme, Software-Zustände et cetera Dies war sicherheitstechnisch kein Problem, solange diese Netze nicht mit dem Internet in Berührung kamen. Durch geforderte Fernzugriffe von Service-Technikern ist diese Abschottung nicht mehr möglich. Daher ist es auch in Industrienetzen notwendig eine Anomalie-Erkennung zu etablieren, um die Cybersicherheit auf einem hohen Niveau zu halten. KI-Algorithmen sollen dabei helfen aus der Alarmmenge eine sinnvolle Risikoabschätzung zu generieren.

Prof. Dr.-Ing. Kai-Oliver Detken studierte Informationstechnik an der Universität Bremen und promovierte im Fachbereich Informatik. Heute ist er Geschäftsführer der DECOIT GmbH & Co. KG, doziert an der Hochschule Bremen und arbeitet als freier Autor im IT-Umfeld

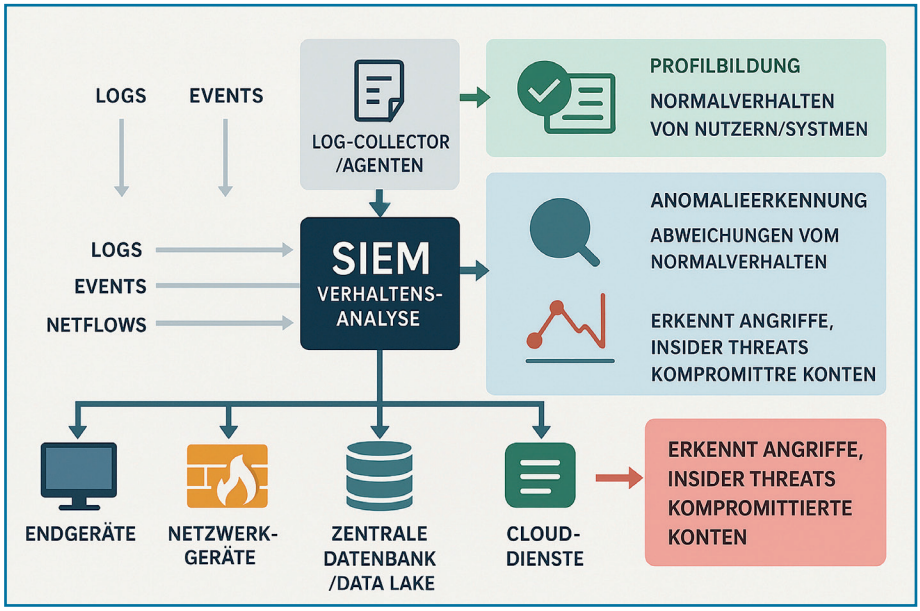

Abbildung 1: SIEM-Systeme der zweiten Generation werden oftmals mit dem Attribut „Künstliche Intelligenz" beworben, die nach verschiedenen Ansätzen funktionieren

Das industrielle Internet der Dinge (IIoT) wächst weltweit rasant und verspricht einen Mehrwert bei reduzierten Kosten für verteilte Anwendungen. IIoT-Anwendungen reichen von Smart Metering und Smart Grid über autonomes Fahren, Smart Traffic, Smart Home und Smart Building bis hin zur Industrie- und Prozessautomatisierung.

Die Vernetzung von Milliarden kleiner, ressourcenbeschränkter und kosteneffizienter eingebetteter Systeme stellt jedoch eine große Herausforderung für die Informationssicherheit dar, nicht nur für die Sicherheit und die Privatsphäre von Personen, Geräten und Systemen, sondern auch für die funktionale Sicherheit des Systems. Gelingt es einem Angreifer, ein System zu kompromittieren, kann er auch die Kontrolle über das System übernehmen. Dies ist besonders kritisch, wenn im System nicht nur sensorische (überwachende) Geräte, sondern auch aktive und sicherheitsrelevante Anwendungen (Regelung durch Aktoren) eingesetzt werden.

Systeme zur Angriffserkennung

Herkömmliche IT-Netze werden bereits seit vielen Jahren unter anderem mit Intrusion Detection Systemen (IDS) oder Intrusion Prevention Systemen (IPS) geschützt. Seit einigen Jahren sind auch Security Information and Event Management (SIEM)-Systeme im Einsatz, die möglichst viele geeignete Technologien (wie Intrusion Detection and Prevention, Asset-Management, Log-Analyse) umfassend miteinander kombinieren. Allerdings stehen solche SIEM-Systeme bislang nicht oder nur sehr eingeschränkte für den Einsatz in industriellen IoT-Netzen und -OT-Netzwerken zur Verfügung. Dies ist umso kritischer, als dass diese immer häufiger die Einfallstore für Angreifer darstellen.

Um beliebe Anomalien erkennen zu können und nicht nur veröffentlichte Schwachstellen der Hersteller, müssen Si-

cherheitsüberwachungssysteme intelligenter werden. So werden SIEM-Systeme der zweiten Generation oftmals mit dem Attribut „Künstliche Intelligenz“ beworben, die nach verschiedenen Ansätzen funktionieren (siehe Abbildung 1).

Die statistische Zeitreihenanalyse ist in vielen kommerziellen Produkten und Open-Source-Bibliotheken zu finden. Sie arbeitet aber nur auf vorab definierten Metriken und nummerischen Werten. So könnte man beispielsweise festlegen, welcher Netzwerkverkehr normal ist , um dann bei Überschreitung dieses Wertes einen Alarm auszulösen. Warum dieser Wert überschritten wurde, wird dabei nicht hinterfragt. Das statische Regelwerk ist bei bekannten SIEM-Herstellern wie IBM QRadar SIEM, OSSEC oder McAfee Enterprise Security SIEM integriert. Hier wird versucht eine sog. „Threat Intelligence“ umzusetzen, indem Honeypots, statische Analysen über verschiedene Kunden und Postings im Darknet einbezogen werden. Dazu ist die permanente Anbindung des SIEM-Systems an die Kundensysteme notwendig. Bei der Verhaltensanalyse wird zunehmend auch Maschinelles Lernen (ML) eingesetzt. Diese Technik kommt bei SIEM-Herstellern der zweiten Generation, wie IBM QRadar UBA, LogRhythm UEBA (inzwischen aufgekauft durch Exabeam), HPE ArcSight UBA, Splunk und DarkTrace Enterprise zum Einsatz. Die verwendeten Lernverfahren nutzen dabei ausgewählte Metriken zu einzelnen Datenfeldern der Events (zum Beispiel Authentifizierungsvorgänge und Aktivitäten in Applikationen), deren zeitliche Entwicklung und Korrelation betrachtet werden. So können beispielsweise vermehrte Login-Versuche auf einer Datenbank erkannt werden.

Anomalie-Erkennung durch ML

Im Bereich der Anomalie-Erkennung bei IDS-Systemen kommen bereits seit Jahrzehnten Maschinelles Lernen (ML) zum Einsatz. Waren es zunächst symbolische Verfahren, wie zum Beispiel Support Vector Machines,

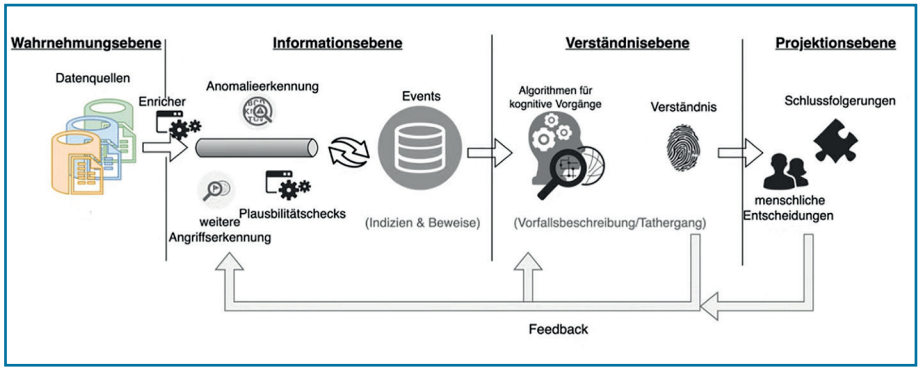

Abbildung 2: So wird der der gesamte Prozess zur Wahrnehmung einer Anomalie durch verschiedene Ebenen (Wahrnehmungs- bis Projektionsebene) unterteilt

Knearest neighbor oder Bayes‘sche Verfahren, werden jetzt auch vermehrt subsymbolische Deep-Learning-Verfahren, wie zum Beispiel Generative Adversarial Network, Recurrent Neural Network, Artificial Neural Network oder hybride Kombinationen zur Analyse des Netzverkehrs und dessen Verhalten verwendet. Zum Trainieren solcher Netze kommen vermehrt auch Active-Learning-Ansätze zum Einsatz, bei der ein menschlicher Experte weitere Bewertungen vornimmt. Intrusion-Response-Systeme (IRS) reagieren manuell (passiv) oder automatisch (aktiv) auf solche gemeldeten Angriffe mit entsprechenden Maßnahmen. Die Zuordnung von Angriffen zu erforderlichen Gegenmaßnahmen erfolgt entweder regelbasiert oder assoziativ unter Einbeziehung der durch die Maßnahmen beobachteten Systemänderungen. Ein aktives System reagiert automatisch auf Ereignisse und bietet daher eine kurze Reaktionszeit und damit kleineres Zeitfenster, in dem der Angreifer aktiv sein kann. Umgekehrt kann es aber bei Fehlalarme signifikante Kosten verursachen, so dass eine zuverlässige Erkennung bösartiger Angriffe Voraussetzung für den automatischen Einsatz eines IRS ist. Für das Verständnis eines Angriffs und dessen Meldung an Partnerakteure ist es wichtig, das Vorgehen des Angreifers zu verstehen. Die Root-Cause-Analysis ist eine Methodik zur Identifikation von initialen Ereignissen und deren kausale und temporale Beziehungen bzw. Wirkketten zu auftretenden Feh-lern, die bisher hauptsächlich im Qualitätsmanagement und im Safety-Bereich zum Einsatz kommt. Typischerweise konstruieren solche Techniken deterministische oder probabilistische Modelle, die auf dem zugrunde liegenden Domänen- beziehungsweise Systemwissen und der Historie des beobachteten Systems aufbauen und mit deren Hilfe sich die Verwundbarkeit eines Systems zum Beispiel mit Hilfe von Markov-Modellen oder simulationsbasierten Verfahren (zum Beispiel Monte-Carlo-Simulation) abschätzen lässt.

Abbildung 2 zeigt, wie der gesamte Prozess zur Wahrnehmung einer Anomalie durch verschiedene Ebenen (Wahrnehmungs- bis Projektionsebene) unterteilt wird. Am Anfang stehen die Rohdaten, die erst einmal mit Zusatzinformationen (zum Beispiel IP-/MAC-Adressen) angereichert werden müssen. Daraus folgt durch Deep-Learning-Algorithmen eine erste Anomalie-Erkennung, die parallel automatisiert auf Plausibilität überprüft wird. Anschließend wird ein Vorfall bzw. Event erzeugt und dieses an weitere Algorithmen für kognitive Vorgänge weitergegeben, damit am Ende eine menschliche Entscheidung über diesen Vorfall getroffen werden kann. Stellt der Analyst fest, dass es sich nicht um eine Anomalie handelt, sondern um eine bekannte Störung oder einen Ausnahmefall, kann er über ein Feedback-Mechanismus dies an die Anomalie-Erkennung zurückgeben. Dadurch wird bei dem nächsten ähnlichen Vorfall kein Event mehr erzeugt. Für diese menschlich Entscheidung muss daher ein Bezug zu den Ausgaben der Systeme hergestellt werden

können, was nicht immer möglich ist.

Daher werden durch den ML-Einsatz erst einmal die Ausgabe von Falschmeldungen erhöht, da exakte Werte für Metriken nicht erkannt werden können und eine hohe Variabilität des realistischen, gutartigen Verkehrs existiert. Beides erschwert das Auffinden stabiler Muster. Hinzu kommt, dass gute Datensätze und eine solide Bewertungsmethodik oftmals nicht vorhanden sind. Auch reale Anwendungen zum Erkennen von Netzwerk-Anomalien fehlen bislang. Sicherheitsanalysten von Security Operations Center (SOC), die permanent mit Sicherheitsvorfällen zu tun haben, benötigen weitere Unterstützung bei der Korrelation von Daten aus heterogenen Quellen, um sich einen ganzheitlichen Überblick verschaffen zu können. Erst dann können laterale Bewegungen und Bedrohungen zwischen Hosts erkannt werden.

Forschungsprojekt KISTE

Das Forschungsprojekt KISTE (https://kiste-project.info) mit einer Laufzeit von Juli 2024 bis Juni 2026 hat sich zum Ziel gesetzt einen automatisierten KI-Analysten in einer OT-Umgebung zu entwickeln, wie die Abbildung 3 zeigt. Es beinhaltet ein KI-gesteuertes System, das die Cybersicherheitsabläufe verbessert:

- Analyse von Warnmeldungen: Der KI-Analyst überwacht kontinuierlich die Warnmeldungen des SIEM-Systems und unterscheidet mithilfe von maschinellem Lernen zwischen falsch positiven Meldungen und echten Bedrohungen.
- Ursachenanalyse: Nach der Erkennung einer echten Bedrohung führt das System eine Ursachenanalyse durch. Dabei werden die Ursprünge der Bedrohung zurückverfolgt, ihre Auswirkungen verstanden und die ausgenutzten Schwachstellen identifiziert.
- Bewertung des Schweregrads der Bedrohung: Der automatisierte Analytiker bewertet den Schweregrad der Bedrohung auf der Grundlage der potenziellen Auswirkungen auf den Geschäftsbetrieb, der Sensibilität der betroffenen Daten und des Sicherheitsstatus der Organisation.
- Automatische Reaktion: Je nach Bedrohungsstufe leitet das System automatische Reaktionen ein. Diese können von der Aktualisierung von Firewall-Regeln bis zur Isolierung gefährdeter Systeme reichen. Wichtig ist, dass die Entscheidungen des SIEM-Systems in der OT ein Gleichgewicht zwischen der Abschwächung der Bedrohung und der Aufrecht-erhaltung der Geschäftsprozesse und Sicherheit herstellen.
- Automatische Erstellung von Cyber Threat Intelligence (CTI): Für identifizierte reale Bedrohungen erstellt das System automatisch CTI-Feeds. CTI-Plattformen erstellen Bedrohungsmeldungen, die von internen SIEM-Systemen eingelesen werden können (sog. Threat Feeds). Die Hauptidee dahinter ist, dass Informationen über Angriffsszenarien mit anderen SIEM-Systemen geteilt werden können.
- Benutzerbenachrichtigung: Das System informiert die relevanten Akteure über die Bedrohung, einschließlich der Analyse und der Vorschläge für weitere Maßnahmen. Zum Beispiel Empfehlungen zur Behebung von Schwachstellen oder zur Änderung von Sicherheitsrichtlinien.
- Lernen und Anpassen: Das KI-System muss kontinuierlich aus jedem Vorfall lernen. Dieses Lernen sollte durch menschliche Feedbackschleifen und die kontinuierliche Aktualisierung der Bedrohungsdatenbank erreicht werden.

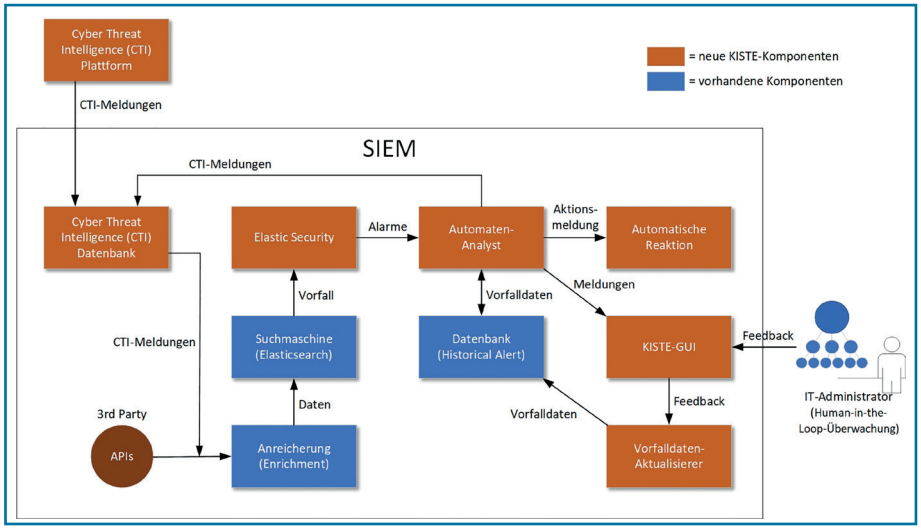

Abbildung 3: Das Forschungsprojekt KISTE hat sich zum Ziel gesetzt, einen automatisierten KI-Analysten in einer OT-Umgebung zu entwickeln (Grafiken: Detken)

Solch ein System ist allerdings noch in der Forschung. Es wird gerade im OT-Bereich noch dauern bis man automatisierten Reaktionen zustimmt, da hier die Verfügbarkeit immer vor der IT-Sicherheit eingeordnet wird.

Fazit

Maschinelles Lernen (ML) steckt nach wie vor in den Kinderschuhen. Bestehende Forschungsansätze gelangen oftmals nicht die Praxis, weil eine semantische Lücke zwischen der Ausgabe von Systemen, die in der Regel auf der Basis einzelner Datensätze arbeiten, und den Erwartungen des Analysten, der die Ausgabe verstehen muss, besteht. Es bleibt daher schwierig einen Angreifer und seine Beweggründe hinter einer Attacke zu identifizieren, da die Zuordnung der Daten problematisch ist. Die SIEM-Systeme der dritten Generation werden diese Lücke in der Zukunft versuchen zu schließen. In OT-Netzen wird der Einsatz von Automatismen allerdings immer problematisch sein.