Verlagsbeilage, August 2025

Special
Künstliche Intelligenz in Angriff und Verteidigung

‹kes›
Die Zeitschrift für Informations-Sicherheit

Impressum

DATAKONTEXT GmbH

Augustinusstraße 11 A
50226 Frechen (DE)
Tel.: +49 2234 98949–30,
redaktion@datakontext.com,
www.datakontext.com

Geschäftsführer: Dr. Karl Ulrich

Handelsregister:
Amtsgericht Köln, HRB 82299

Anzeigenleitung: Birgit Eckert
(verantwortlich für den Anzeigenteil)
Tel.: +49 6728 289003, anzeigen@kes.de

Satz: Dirk Hemke (SatzPro), Krefeld;
Markus Miller (Satz + Bild), München

Druck: QUBUS media GmbH,
Beckstraße 10, 30457 Hannover

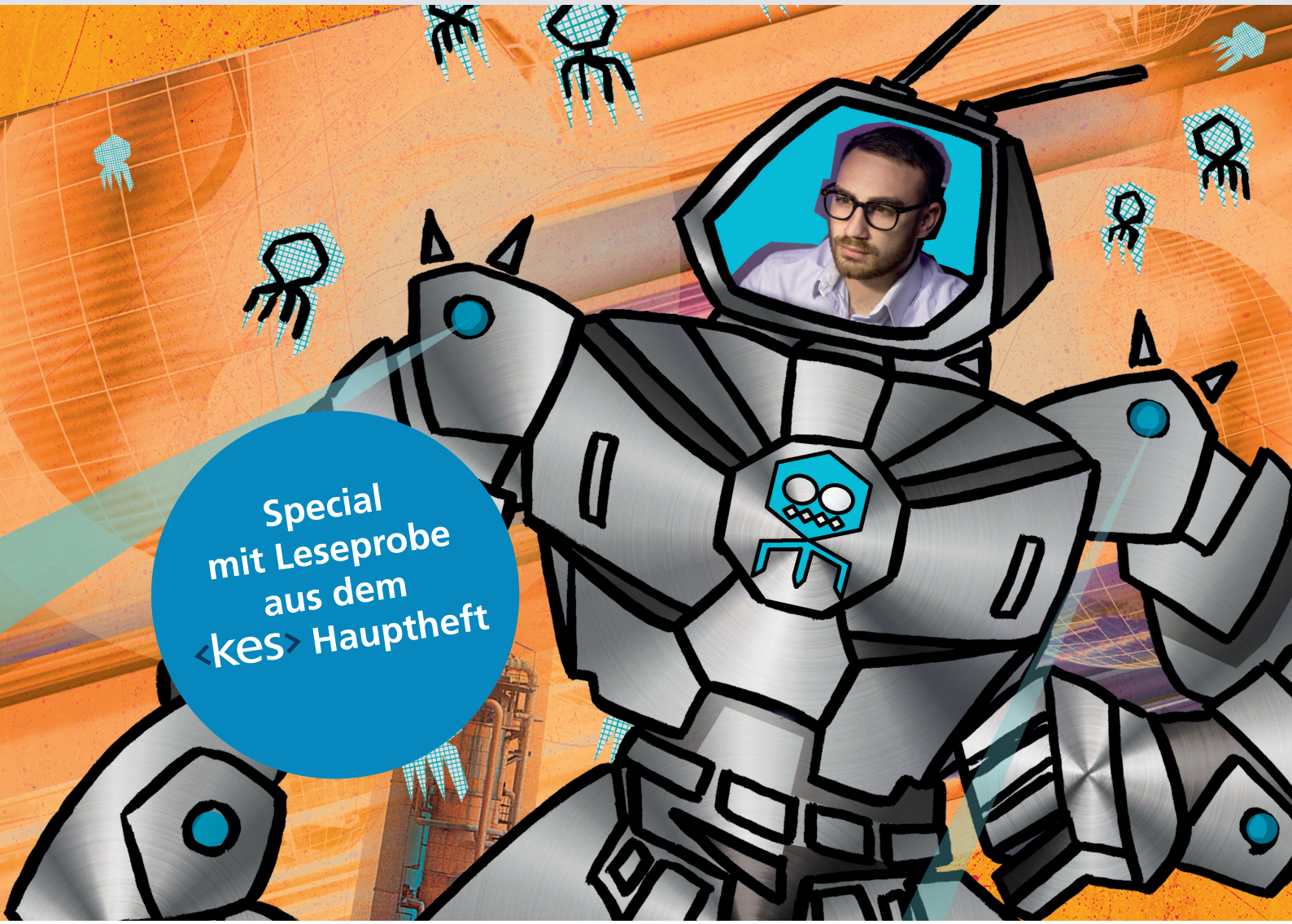


Bild: Andreas Heller, www.hellergrafik.de (Foto: Freepik.com)

Bild: nateejindakum/stock.adobe.com

Keine Angst vor Kollege KI

Künstliche Intelligenz sicher, effizient und nachhaltig im Unternehmen einführen

Künstliche Intelligenz (KI) verspricht Effizienzgewinne und das Ende leidiger Routinearbeit. Doch um KI erfolgreich einzuführen, muss die Vorbereitung stimmen. Qualität und Auswahl der Daten sollten im Vordergrund stehen und betriebliche Gremien wie Betriebsrat und Datenschutz früh eingebunden werden.

Von Elmar Török, SITS Deutschland GmbH

Es wird häufig missverstanden: KI verbessert eben nicht die Datenqualität. Im Gegenteil, die künstliche Intelligenz ist auf eine saubere Datenbasis angewiesen, um vernünftige Ergebnisse zu erzielen. Doch in vielen Unternehmen sind die Datenhygiene zusammen mit einer gepflegten Rechte- und Ablagestruktur seit Langem vernachlässigte Pflichtübungen. Tenant-Hygiene, wie das Thema oft genannt wird, ist aufwendig, zäh und bringt zunächst keine direkt messbaren Erfolge. Das ändert sich mit der Einführung von künstlicher Intelligenz. Arbeitet die KI mit unvollständigen, inkonsistenten oder veralteten Daten, führt das zu fehlerhaften oder unbrauchbaren Vorhersagen. Wenige Aktivitäten haben eine so große positive Wirkung auf den Erfolg der KI-Einführung wie eine umfassende Datenbereinigung mit dem Ziel, die Qualität zu verbessern. Eine wichtige Aufgabe im Vorfeld ist dabei, die Kriterien für Qualität festzulegen. Das kann normalerweise nur der Datenbesitzer – und der ist häufig nicht definiert, zumindest nicht offiziell. Oft beginnen Tätigkeiten wie die Identifikation und Korrektur von Datenfehlern, die Entfernung von Duplikaten und die Harmonisierung der Datenformate mit der Suche nach einem Verantwortlichen.

Neben der Datenqualität spielt auch die Datenmenge eine entscheidende Rolle. KI-Systeme, besonders solche, die auf maschinellem Lernen basieren, benötigen große Datenmengen, um Muster zu erkennen und robuste Vorhersagen zu treffen. Doch eine möglichst große Datenmenge bedeutet nicht automatisch, dass die Daten auch nützlich sind. Alte oder irrelevante Daten können die Modellgenauigkeit beeinträchtigen und zu Verzerrungen führen. Es ist daher notwendig, nicht nur die Datenmenge zu betrachten, sondern auch deren Aktualität und Relevanz zu überprüfen. Ein Modell, das beispielsweise auf veralteten Kundendaten basiert, kann keine aktuellen Marktentwicklungen abbilden und liefert potenziell unbrauchbare Prognosen.

Aufbewahrung und Löschung über Richtlinien umsetzen

Eine Lösung, um der KI nur aktuelle Daten zur Verfügung zu stellen, ist ein individuelles Aufbewahrungs- und Löschkonzept für die Organisation. Zum einen müssen darin rechtliche Vorgaben zur Mindestaufbewahrungsdauer berücksichtigt werden. Zum anderen ist es notwendig, Daten, die als nicht mehr relevant kategorisiert wurden, entweder zu löschen oder zumindest aus dem Zugriff der KI zu entfernen. Das kann über ein Staging mittels Backup oder über eine Archivierung umgesetzt werden.

Ein weiterer essenzieller Schritt vor der Einführung von KI besteht darin, sensible und kritische Daten zu identifizieren und entsprechend zu kennzeichnen. Welche das sind, muss jede Organisation individuell im Rahmen

eines Klassifizierungsprojekts herausfinden. Daten mit einem Label zu versehen, das die Kritikalität beschreibt, wird unter anderem von der Datenschutzgrundverordnung gefordert. Aber auch der IT-Sicherheitsstandard ISO 27001 fordert die Klassifizierung von Daten mithilfe technischer Maßnahmen. Nur wenn klar ist, welche Daten schützenswert sind, können diese auch mit den notwendigen Mitteln geschützt werden.

KI treibt die Einführung von Datenklassifizierung

Organisationen haben den Aufwand für eine Datenklassifizierung bisher oft gescheut. Häufig existiert zwar eine Datenklassifizierungsrichtlinie, die Mitarbeiter kennen sie aber nicht oder wenden sie nicht an. Nun sorgen künstliche Intelligenz und die hohe Attraktivität von KI-Tools für einen Nachholeffekt. In vielen Unternehmen werden jetzt die meist ohnehin vorhandenen Werkzeuge für die Datenklassifizierung abgestaubt und Einführungsprojekte gestartet. Moderne Tools ermöglichen es, Daten entweder automatisch zu kategorisieren oder durch eine nahtlose Integration in die täglichen Produktivitätstools wie Word, Excel, PowerPoint und E-Mail schnell und unkompliziert manuell einzuordnen.

Untrennbar damit verbunden ist das Rollen- und Rechtekonzept. In vielen Organisationen werden moderne Kollaborationstools ohne Governance verwendet. Jeder darf Speicherbereiche erstellen und Dateien oder ganze Ordnerstrukturen für einzelne oder für die Organisation freigeben. So entstehen unkontrollierte Informationssammlungen, auf die jeder Zugriff hat – auch die KI. Denn künstliche Intelligenz im Unternehmen arbeitet immer im Benutzerkontext. Worauf Anwender Zugriff haben, darauf hat auch die KI Zugriff. Existieren keine klaren und durchsetzbaren Regeln für Dateifreigaben, werden die Ergebnisse der KI-Anfrage auch Informationen enthalten, die möglicherweise nicht für den Benutzer gedacht waren.

KI und die Rolle von Datenschutzbeauftragten und Betriebsrat

Ein KI-System einzuführen, ist nicht nur eine technische, sondern auch eine rechtliche und ethische Herausforderung. Datenschutzbeauftragte und Betriebsräte spielen dabei eine zentrale Rolle, da sie die Interessen der Mitarbeiter vertreten und die Einhaltung datenschutzrechtlicher Vorschriften überwachen. KI-Systeme haben das Potenzial, große Mengen personenbezogener Daten zu analysieren, zu verarbeiten und sogar Verhaltensmuster zu erkennen. Dies kann erhebliche Risiken für die Privatsphäre der Mitarbeiter erzeugen. Um das Vertrauen in die Technologie zu stärken und um für Transparenz bei den einzuführenden Tools zu sorgen, muss der Bereich Datenschutz frühzeitig, am besten schon in der Planungsphase, eingebunden werden. So können der Datenschutzbeauftragte oder sein Vertreter sicherstellen, dass geeignete Datenschutzmaßnahmen getroffen werden. Dazu zählen unter anderem die Implementierung von Privacy-by-Design- und Privacy-by-Default-Prinzipien sowie die regelmäßige Überprüfung der Systeme auf Datenschutzkonformität.

Schnelle und transparente Kommunikation zahlt sich auch beim Betriebsrat aus. Das Gremium ist nach dem Betriebsverfassungsgesetz immer dann zu beteiligen, wenn die Möglichkeit zur Überwachung von Mitarbeitern besteht. KI-Systeme sind in der Lage, Unmengen von Daten zu korrelieren und Analysen daraus zu erstellen. Ohne Governance-Leitlinie und die technischen Maßnahmen, um sie durchzusetzen, ließen sich Analysen missbrauchen. Der Betriebsrat stellt sicher, dass genau diese Regeln zur Governance definiert und implementiert werden.

Klarheit bei der KI-Nutzung

Die Einführung von KI ist ein dynamischer Prozess, der kontinuierlich überwacht werden muss. Moderne Tools zur Verwaltung von KI-Produkten können deren Nutzung meist sehr detailliert abbilden. So erfahren die Projektverantwortlichen, welche Teile der KI-Unterstützung besonders gut ankommen und wo noch mehr Information und eventuell auch Hilfestellung notwendig sind. Darüber hinaus können die Monitoring-Tools dabei helfen, den Missbrauch von KI zu erkennen. Im Idealfall lassen sich darüber auch Regeln vorgeben, welche Daten verwendet werden dürfen und was passieren soll, wenn Anfragen an die KI gestellt werden, die sich nicht mit den ethischen und rechtlichen Vorgaben der KI-Richtlinie vereinbaren lassen. Oft sind solche Anfragen nicht böswillig gemeint, sondern nur eine Folge von mangelnder Information oder einer falschen Erwartungshaltung der Mitarbeiter. Neben den Tools, um die Nutzung zu überwachen, ist also auch eine klar formulierte Richtlinie mit den Dos and Don'ts der KI-Nutzung unbedingt erforderlich.

Fazit und Ausblick

Die Einführung von KI im Unternehmen erfordert weit mehr als die bloße Implementierung von Technologien. Sie muss strategisch geplant und unter Berücksichtigung ethischer und rechtlicher Vorgaben umgesetzt werden. Datenschutzbeauftragte und Betriebsräte übernehmen eine wichtige Rolle, indem sie die Interessen der Mitarbeiter schützen und die Einhaltung von Datenschutzrichtlinien überwachen. Aber auch durch umfassende Schulungen, kontinuierliches Monitoring und transparente Kommunikation kann die Implementierung von KI optimal gestaltet werden. Langfristig wird es entscheidend sein, die Systeme regelmäßig zu überprüfen und die Mitarbeiter aktiv einzubeziehen. ■

KI in der Verteidigung

Von reaktiver zu proaktiver Cybersecurity

Künstliche Intelligenz wird unverzichtbar, um wachsende Security-Herausforderungen zu meistern und KI-basierte Software-Architekturen abzusichern. Eine wichtige Rolle spielen dabei KI-Agenten.

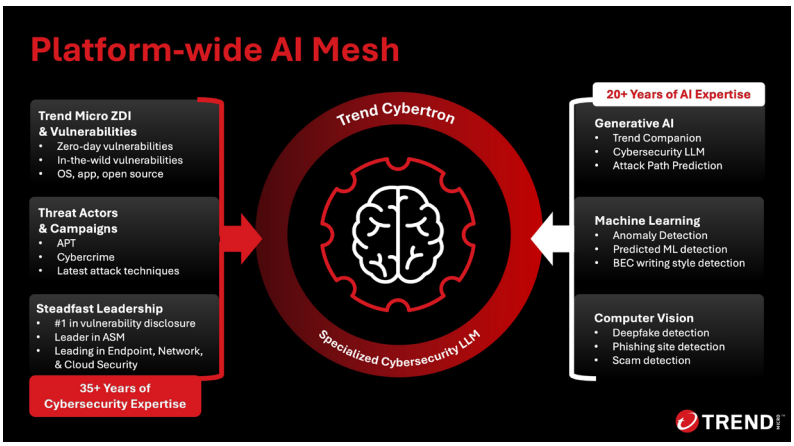
Von Richard Werner, Trend Micro

Cyberkriminalität ist ein globales Geschäft und die Angreifer sind heute keine Einzeltäter mehr, sondern in einer hochprofessionellen Schattenindustrie organisiert. Sie nutzen Cloud-Ressourcen und As-a-Service-Angebote, was sie zu effizienten und weltweit vernetzten Akteuren macht. Neben monetär motivierten Cybercrime-Organisationen sehen wir – bedingt durch die angespannte geopolitische Lage – verstärkt auch staatlich gesponserte Gruppierungen, die das Ziel verfolgen, die Gesellschaft zu destabilisieren. IT- oder IT-Security-Teams sind mit einer wachsenden Angriffsfläche und einer Flut an Warnmeldungen konfrontiert, die es erschwert, kritische Indikatoren zu erkennen. Dazu kommen neue regulatorische Anforderungen. Künstliche Intelligenz (KI) bietet ihnen verschiedene Unterstützungs- und Automatisierungsmöglichkeiten.

LLMs als Übersetzer

In der Praxis kommen in der Cybersicherheit zwei Arten von KI-Modellen zum Einsatz. Zum einen gibt es die traditionelle, kategorisierende KI, die überall dort benutzt wird, wo es um Datenanalyse und die Auswertung von Sicherheitsinformationen geht. Zum anderen gibt es generative KI, die aus bestehenden Informationen beziehungsweise Daten Neues erstellt. Hierunter fallen Large Language Models (LLMs), die sich in der Cybersicherheit besonders dafür eignen, technische Informationen in natürliche Sprache und verständliche Anweisungen zu übersetzen.

Insgesamt unterstützen beide Kategorien dabei, komplexe Angriffsflächen im Blick zu behalten, Risiken zu bewerten, Schwachstellen proaktiv zu schließen und im Ernstfall schnell zu reagieren. In Trend Micro XDR korreliert und analysiert KI etwa die Warnmeldungen sämtlicher angeschlossener Security-Systeme. So werden False Positives minimiert und Mitarbeiter sehen in einer zentralen Konsole auf einen Blick, ob die IT-Umgebung angegriffen wird und welche Systeme betroffen sind. Maschinelles Lernen kann Anzeichen für Cyberangriffe verhaltensbasiert erkennen und auch bisher unbekannte Bedrohungen aufdecken – im Gegensatz zu traditionellen, patternbasierten Verfahren. Außerdem kommen Machine Learning, Deep Learning und Computer Vision beispielsweise zum Einsatz, um Phishing-Mails herauszufiltern oder Deepfakes als ungebetene Gäste in Videokonferenzen zu identifizieren. LLMs übernehmen währenddessen die Rolle des Übersetzers und helfen Mitarbeitern dabei, komplexe technische Informationen leichter zu verstehen und schnell die richtigen Handlungsempfehlungen zu finden.



Trend Micro AI Mesh mit Cybertron-Kern, verbindet Vulnerabilitäts-Management, Bedrohungserkennung und KI-Technologien für Cybersicherheit. (Bild: Trend Micro)

Spezialisierte KI-Agenten

Aktuell geht die Branche den nächsten Entwicklungsschritt hin zu spezialisierten KI-Agenten, die wie virtuelle Security-Mitarbeiter selbstständig Aufgaben übernehmen und sich ins Team integrieren. Die Integration einer proaktiven

Cybersecurity-KI bedeutet dabei wesentlich mehr als ein Chatbot-Interface. Konkret beinhaltet sie die Sammlung spezialisierter LLM-Modelle, Datensätze, Machine Learning, Sprachverarbeitung sowie KI-Agenten, die mit umfassender Sicherheitsexpertise in den Feldern Bedrohungsanalyse und Schwachstellenforschung trainiert wurden.

Es gibt dabei einen wichtigen Unterschied zwischen rohen LLMs und den um sie herum aufgebauten KI-Agenten: Basismodelle wie GPT-4o von OpenAI oder Sonnet, Opus und Haiku von Anthropic sind rohe LLMs, die in der Lage sind, Benutzeranfragen zu beantworten. Im Gegensatz dazu bauen LLM-gesteuerte KI-Agenten wie ChatGPT und Claude auf diesen Basismodellen auf, um komplexere Systeme mit Funktionen wie Codeausführung, Speichererhaltung und Internet-Browsing-Fähigkeiten zu schaffen. Teamarbeit beinhaltet in diesem Kontext also einen LLM-gesteuerten KI-Agenten, der ein System aus vielen miteinander verbundenen Modulen ist.

Ein Beispiel für spezialisierte Cybersecurity-KI-Agenten sind sogenannte „Cybersecurity Digital Twins“. Solche KI-Agenten erstellen eine virtuelle Simulation der individuellen IT-Umgebung, die kontinuierlich mit Daten des Originalobjekts oder -systems aktualisiert wird. In dieser können die Aktivitäten realer Angreifer imitiert und die Risikoexposition in Echtzeit berechnet werden. Dabei lernen die Agenten dynamisch dazu. Auf diese Weise können Sicherheitsverantwortliche ihre Verteidigungsstrategie durch eine unbegrenzte Anzahl von Tests an einer Simulation kontinuierlich validieren und optimieren – ganz ohne Ressourcen des aktiven Security-Systems zu verbrauchen oder Störungen zu verursachen. Dank der durch KI-Agenten gewonnenen Fähigkeit, Aktionen von Angreifern vorherzusehen, können Unternehmen mit einem proaktiven Security-Ansatz schneller sein als ihre Gegner.

KI-Architekturen erfordern eine dynamische Absicherung

KI-Workloads sind nicht mehr CPU-zentriert, sondern GPU-basiert. Sie führen neue Architekturschichten ein, sind datengetrieben und verändern sich kontinuierlich. Auch die Cybersicherheit muss sich daher dynamisch ausrichten und KI-Modelle, den Datenfluss sowie deren Infrastrukturen laufend überwachen. So lassen sich neue, KI-spezifische Risiken wie Data Poisoning oder Adversarial Attacks mindern, die darauf abzielen, KI-Modelle zu kompromittieren oder sensible Daten zu extrahieren. Wichtig ist, Sicherheit in alle Ebenen der KI-Infrastruktur zu integrieren und die gesamte Lieferkette zu berücksichtigen – von der Hardware über die Cloud-Umgebung und Schnittstellen zu Drittsystemen bis zum Foundation-Modell und Nutzerinterface. Die Voraussetzung dafür schafft eine integrierte, KI-gestützte Cybersecurity-Plattform wie Trend Vision One.

Die intelligente Security-Schaltzentrale

Ein Plattformansatz stellt sicher, dass sämtliche Security-Systeme und KI-Agenten nahtlos interagieren und auf die bestmögliche und aktuelle Datenbasis zugreifen können. Alle sicherheitsrelevanten Informationen laufen einheitlich auf einer Plattform zusammen und Sicherheitsprozesse werden zentral gemanagt. Das reduziert die Komplexität in der Administration erheblich und schafft umfassende Transparenz über Aktivitäten, Risiken und Bedrohungen in der gesamten IT-Umgebung. Trend Vision One basiert auf einer agentischen KI-Architektur, die als eine der Kernkomponenten einen Cybersecurity Digital Twin bereitstellt. Das intelligente Cyber-Gehirn hinter der Plattform ist Trend Cybertron, ein speziell für die Cybersecurity entwickeltes LLM. Dieser Ansatz in Kombination mit der umfassenden Abdeckung von E-Mail-, Netzwerk-, Endpunkt- und KI-Sicherheitsdomänen macht eine einheitliche Security-Plattform zu einem unverzichtbaren Bestandteil moderner Sicherheitsarchitektur in Unternehmen.

Trend Cybertron wird auch als Open-Source-Lösung bereitgestellt, sodass Sicherheitsforscher auf der ganzen Welt von dem spezialisierten KI-Modell profitieren und daran mitwirken können. Typische Anwendungsfälle für die Open-Source-Lösung sind unter anderem die Verbesserung bestehender Security-Tools mit fortschrittlichen KI-Funktionen, die Entwicklung zugeschnittener Sicherheitsanwendungen mit spezifischen Cybersecurity-Modellen und die Integration in DevSecOps-Pipelines zur automatischen Sicherheitsbewertung.

Die Zukunft ist proaktiv und KI-gestützt

Die goldene Regel der Cybersicherheit bleibt: Während sich Bedrohungslandschaften, IT-Infrastrukturen und Software-Architekturen weiterentwickeln, muss auch die Security Schritt halten. Reaktive Cybersicherheit ist schon lange nicht mehr zeitgemäß. Mit einer proaktiven Sicherheitsstrategie, die das Potenzial von KI-Agenten ausschöpft, können Unternehmen Risiken vorausschauend mindern und auch künftige Herausforderungen meistern. Entscheidend für die Wirksamkeit ist ein einheitlicher Plattformansatz, der Security-Daten, -Systeme und -KI-Modelle zusammenführt und zentral steuert. So lassen sich die nötige Transparenz, Effizienz und Voraussicht erzielen, um mit der Verteidigung proaktiv den wachsenden Anforderungen zuvorzukommen. ■

rubrik

HACKER SIND HARTNÄCKIG.

SIE AUCH?

Rubrik bringt Sie schnell wieder auf Kurs.

Ihr Unternehmen, Ihr Ruf und Ihre Karriere. Gesichert.

rubrik.com/de

Die handhabbare KI-Revolution

LOTL-Angriffe gezielt mit KI und Nutzerprofilen abwehren

KI und Machine Learning tragen wesentlich zur Erkennung und Abwehr von Gefahren bei. Doch Security-Teams kämpfen oft mit einer Flut unstrukturierter Alarme. Erst durch Verfahren wie das automatisierte Clustering von Nutzertypen wird KI praxisnah: Es zeigt, welche Tools an Endpunkten genutzt werden, und erlaubt so gezielte Sicherheitsregeln. So lässt sich der legitime vom missbräuchlichen Einsatz von Systemtools bei Living-off-the-Land-Angriffen klar unterscheiden.

Von Daniel Daraban, Bitdefender

Cyberkriminelle nutzen bei sogenannten Living-off-the-Land-(LOTL)-Attacken legitime Systemtools wie PowerShell, um ihre Angriffe vorzubereiten und durchzuführen. Diese Taktiken spielen besonders bei komplexen und gezielten Attacken eine große Rolle: Laut einer Analyse von Bitdefender, die auf 700 000 sicherheitsrelevanten Ereignissen aus Telemetriedaten im Frühjahr 2025 basiert, setzen 84 Prozent aller schwerwiegenden Cyberangriffe auf LOTL-Mechanismen.

Dennoch ist der überwiegende Teil der PowerShell-Nutzung legitim. Daher muss künstliche Intelligenz (KI) den legitimen vom missbräuchlichen Einsatz grundsätzlich unterscheiden. Eine automatisierte Nutzeranalyse leistet zusätzliche Hilfe, um effiziente Sicherheitsrichtlinien abzuleiten, die das Verhalten und die Bedürfnisse der jeweiligen Anwender berücksichtigen.

Klassische Verhaltensanalysen stoßen an Grenzen

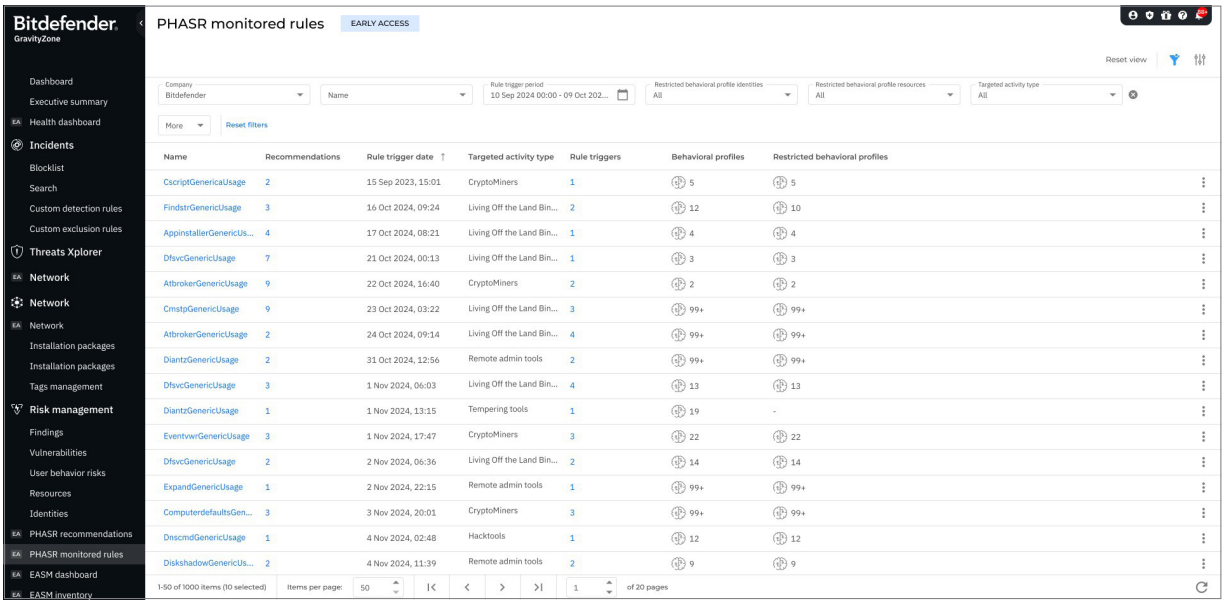
Ein ungefilterter formaler Verhaltensreport auf Basis von KI und Machine Learning liefert keine praxisnahe Grundlage für eine wirksame Abwehr. Wenn jede Nutzeraktivität isoliert und ohne Kontext bewertet wird, resultiert daraus eher ein Alarmchaos statt echter Hilfe. Die Folge ist eine Vielzahl von Regeln und Warnungen, die Administratoren prüfen und dokumentieren müssen – selbst dann, wenn sie letztlich bewusst ignoriert werden. Hinzu kommt, dass der Einsatz von Tools je nach Endpunkt und Mitarbeiter stark variieren kann und sich pauschal kaum einheitlich bewerten lässt.

Auch berücksichtigt eine formale Verhaltensanalyse weder Industriekontexte noch die Geschäftsprozesse im jeweiligen Unternehmen. KI-Modelle bleiben für sich generisch. Angreifer können eine darauf basierende Abwehr umgehen, indem sie ihrerseits vereinfachte Benutzermuster nachahmen. Besonders bei gezielten Angriffen eruieren sie die Arbeitsweise der vorhandenen Sicherheitssoftware. Im nächsten Schritt identifizieren sie die effektivsten Verhaltensmuster legitimer Tools, mit denen sie sich am effizientesten und so lange wie möglich oder nötig tarnen können.

Dynamische, zugeschnittene Regeln

Auch im Zeitalter der KI benötigt die Cyberabwehr daher – über eine Mustererkennung hinausgehend – weiterführende Ansätze der Verhaltensanalyse, um verwertbare Sicherheitsregeln dynamisch auf der Grundlage von Rolle, Verhalten und unternehmensspezifischem Kontext zu definieren. Spezifische Merkmale einer Nutzerkategorie ergeben sich dabei aus der Funktion und Tätigkeit einer Person oder Personengruppe im Unternehmen, aus ihrer regionalen Herkunft und aus ihrer Branchenzugehörigkeit.

Das Festlegen charakteristischer Nutzergruppen anhand ihres individuellen Verhaltens, das sich aus ihren



Wer Living-off-the-Land-Angriffe überwachen und abwehren will, benötigt Regeln zum Nutzen von Tools in Korrelation mit angelegten Nutzerprofilen. (Bild: Bitdefender)

Aufgaben ergibt, hilft dabei, unnötiges und damit oft verdächtiges Nutzen von Tools zu blockieren und so die Angriffsfläche für LOTL effizient zu reduzieren.

Für PowerShell heißt dies zum Beispiel: LOTL-Angriffe mit PowerShell lassen sich problemlos für die meisten Nutzer blocken, weil Vertrieb, Marketing, Produktionsmanager, Management, Controlling oder HR für ihre Arbeit keinen PowerShell-Einsatz auf ihrem Endpunkt benötigen. Das betrifft also die allermeisten Anwender im Unternehmen. Ganz so einfach ist das aber nicht, weil auch Drittanbieter-Applikationen auf einem Endgerät PowerShell am Arbeitsplatz etwa der HR-Abteilung nutzen können – ohne Mitwissen des Mitarbeiters. Dieses applikationsbedingte Nutzen des Tools lässt sich durch KI erkennen und durch eine Regel erlauben. Nicht erklärbare PowerShell-Aktivitäten konsequent zu blockieren, reduziert hingegen potenzielle Angriffsflächen erheblich.

Aus der Verhaltensanalyse ergeben sich folgende segmentierte Nutzertypen:

_____ **Task-User:** Diese Mitarbeiter nutzen für LOTL-Angriffe beliebte Tools aufgrund vordefinierter Arbeitsabläufe nur eingeschränkt oder kaum. Notwendig und hilfreich sind hier strenge Ausführungsregeln und eine auf das Notwendigste beschränkte Vergabe von Privilegien.
_____ **Knowledge-User:** Fachleute wie Ingenieure, Analysten und Berater benötigen eine gewisse Flexibilität, Tools zu nutzen, folgen aber gegebenen Mustern.
_____ **C-Level:** Sie verwenden nur eine begrenzte Zahl von Tools, haben aber umfassenden Zugriff. Sie brauchen deswegen präzise Verhaltensvorgaben. Hier kommt es primär darauf an, dass privilegierte Aktionen mit dem erwarteten Verhalten übereinstimmen.

Sind die Benutzer in Gruppen segmentiert, können IT-Sicherheitsverantwortliche Richtlinien individuell und bedarfsgerecht definieren und dynamisch – auf Wunsch automatisiert – anpassen, anstatt pauschale Blockaden durchzusetzen. In der Praxis hat sich das manuelle Segmentieren als zu umständlich erwiesen und oft zu zusätzlichen Reibungsverlusten innerhalb des Unternehmens geführt. Durch den Einsatz eines adaptiven Sicherheitsmodells, das das Verhalten jedes Einzelnen versteht und Benutzer automatisch auf der Grundlage ihres Verhaltens gruppiert, können Firmen potenzielle Gefahren frühzeitig verhindern, ohne die Produktivität zu beeinträchtigen.

KI benötigt Kontext

Eine klassische Verhaltensanalyse, die allein auf KI basiert, aber ohne das Clustern von Nutzertypen arbeitet, bleibt oft zu allgemein. Das führt zu Fehlalarmen oder blinden Flecken in der Abwehr. Denn wenn Modelle keine individuellen Nutzungsmuster und keinen konkreten Kontext einbeziehen, lassen sie sich von Angreifern leicht aushebeln. Jedoch kann ein neuer Ansatz, der Nutzergruppen segmentiert sowie Kontext und individuelle Benutzerverhaltensmuster granular und dynamisch in die Sicherheitsmaßnahmen mit einbezieht, eine präzisere Erkennung bieten. Mit den sich daraus ergebenden individuellen Nutzerregeln lassen sich legitime Aktivitäten klar vom Missbrauch trennen – und Risiken schon im Vorfeld eindämmen, bevor sie zu Vorfällen werden.

KI ist dabei ein mächtiges Werkzeug – aber erst in Kombination mit intelligenter Nutzungsanalyse, die automatisiert, individuell und adaptiv arbeitet, entfaltet sie ihr volles Potenzial. Denn jede technologische Revolution ist erst dann von Nutzen, wenn sie handhabbare Ergebnisse liefert. ■

noris network

itsa

7.-9.10.2025
Messe Nürnberg
Halle 7 / 7-212

Ihr Premium-IT-Dienstleister für **maximale Sicherheit & Verfügbarkeit**

- Moderne, hochsichere Rechenzentren in Deutschland – zertifiziert bis **TÜViT-TSI-Level-4**
- **Georedundanz** zwischen Nürnberg und München mit Latenzen **< 2 Millisekunden**
- Umfassendes Portfolio von **Colocation bis Cloud-Services**
- Kompetente Unterstützung durch unsere IT-Security-Experten bei der Umsetzung Ihrer Sicherheitsauflagen: **MaRisk, DORA (BAIT, VAIT, ZAIT), IT-SiG 2.0, KRITIS, NIS2, FISG und ISAE 3402**
- Ausgefeilte **SIEM-Systeme** und **eigenes SOC** für die Bearbeitung und Dokumentation Ihrer Security-Events

Jetzt informieren

Threat Intelligence trifft KI

Automatisierte Prozesse sorgen für mehr Tempo und Präzision in der IT-Sicherheit

Sicherheitsverantwortliche stehen unter erheblichem Druck: Die Bedrohungslage wird immer komplexer, während gleichzeitig die Reaktionszeiten aufgrund rechtlicher Vorgaben zunehmend kürzer werden müssen. Wer Threat Intelligence effektiv nutzt, verschafft seinem Security Operations Center (SOC) nicht nur einen entscheidenden Wissensvorsprung, sondern gewinnt auch an Handlungsschnelligkeit und Flexibilität.

Von Michael Klatte, ESET Deutschland GmbH

Neue Angriffsmethoden, polymorphe Malware und dynamisch agierende Akteure stellen IT-Abteilungen vor enorme Herausforderungen. In dieser Umgebung reicht es längst nicht mehr aus, auf reaktive Sicherheitsmechanismen zu setzen. Unternehmen benötigen Threat Intelligence (TI), um Bedrohungen frühzeitig zu erkennen, zu analysieren und automatisiert Gegenmaßnahmen einzuleiten – ganz im Sinne des „Prevention First"-Ansatzes von ESET.

Mehr als nur eine (Reputations-)Datenbank

Threat Intelligence bezeichnet die strukturierte Erhebung, Korrelation und Kontextualisierung sicherheitsrelevanter Informationen aus verschiedenen Quellen. Dazu zählen etwa Malware-Analysen, globale TI-Feeds, Indicators of Compromise (IoCs), Datenbanken für bekannte Schwachstellen, Deep-Web-Quellen und forensische Artefakte. Entscheidend ist dabei nicht die Quantität der Daten, sondern ihre qualitative Verwertbarkeit im Sicherheitskontext: Welche Schwachstellen betreffen meine Systeme konkret? Welche Advanced-Persistent-Threat-(APT)-Kampagnen zielen auf meine Branche? Ist eine verdächtige IP-Adresse in Verbindung mit bekannten Command-and-Control-Infrastrukturen bei mir aufgetaucht?

ESET Threat Intelligence adressiert genau diese Fragen, indem es die gesammelten Informationen mithilfe KI-gestützter Analysemethoden bewertet, kontextualisiert und priorisiert. Damit entwickelt sich diese TI-Lösung vom reinen Datenlieferanten zu einem integralen Bestandteil der Sicherheitsarchitektur.

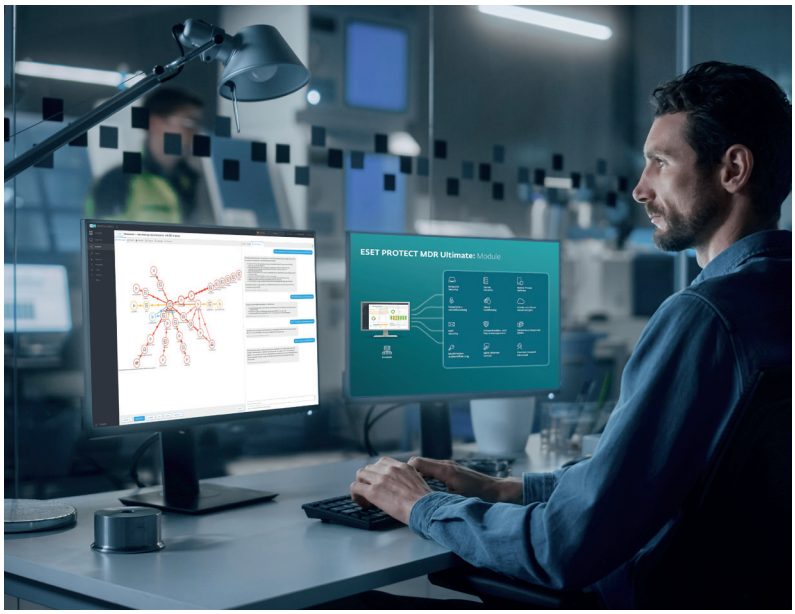
Drei Ebenen und ihre technische Relevanz

Threat Intelligence lässt sich in drei Anwendungsebenen gliedern, die unterschiedliche technische und operative Aufgaben erfüllen:

- **Strategische TI:** Sie liefert übergeordnete Analysen zu Bedrohungsakteuren, geopolitischen Entwicklungen und sektorspezifischen Angriffstrends. Diese Erkenntnisse dienen der strategischen Risikobewertung, der Priorisierung von Investitionen in Sicherheitstechnologien und der Governance-Planung auf Management- und CISO-Ebene. Quellen sind unter anderem CERTs, OSINT-Plattformen und branchenspezifische Allianzen.
- **Taktische TI:** Hier geht es um verwertbare technische Indikatoren wie IP-Adressen, Hashes, Signaturen oder Exploit-Ketten. Diese Daten lassen sich über standardisierte Schnittstellen wie STIX/TAXII in Security-Information-and-Event-Management-(SIEM)-, Endpoint-Detection-and-Response-(EDR)- oder Extended-Detection-and-Response-(XDR)-Systeme integrieren. Tools wie YARA, Suricata-Regeln oder benutzerdefinierte APT IoC-Feeds ermöglichen es, Bedrohungsindikatoren automatisiert zu erkennen und Maßnahmen wie Quarantäne oder Blockierung auszulösen.
- **Operative TI:** Diese Ebene umfasst die kurzfristige Reaktion auf Bedrohungen und ihre Erkennung im aktiven Netzwerkverkehr. Sie liefert Kontext zu laufenden Angriffen und unterstützt Incident-Response-Prozesse – etwa durch automatisierte Analysen verdächtiger DNS-Anfragen, Auffälligkeiten bei Benutzerverhalten oder anomaler Skriptausführung auf Endpunkten. Ziel ist es, Bedrohungen in Echtzeit zu identifizieren, zu stoppen und forensisch auszuwerten.

Die Plattform von ESET konsolidiert diese drei Ebenen auf einer einheitlichen Datenbasis und sorgt mittels KI-gestützter Verfahren für eine priorisierte Aufbereitung relevanter Informationen. Die Integration in vorhandene Systeme erfolgt über Application-Programming-Interfaces (APIs), sodass sich die TI-Feeds automatisiert in bestehende Workflows einbetten lassen. ESET nutzt dabei eigene Sensorik aus dem globalen Netzwerk, zum Beispiel Telemetriedaten aus etwa 110 Millionen

Endpoints, Sandbox-Analysen aus dem ESET LiveGrid-System sowie Erkenntnisse der ESET Research Teams mit Standorten in Bratislava, Montreal, Buenos Aires und Singapur. Zusätzlich unterstützt ESET auch den Zugriff auf community-basierte Plattformen wie die Malware Information Sharing Platform (MISP). Dadurch lassen sich IoCs und Tactics, Techniques and Procedures (TTPs) aus vertrauenswürdigen Quellen organisationsübergreifend integrieren und automatisiert weiterverarbeiten. Dies ist ein wichtiger Beitrag zur kollektiven Bedrohungserkennung.



Ein Experte überwacht Cyberangriffe mithilfe der ESET-Plattform, die detaillierte Angriffspfade und Sicherheitslösungen visualisiert. (Bild: ESET)

ESET AI Advisor: Kontext verstehen, bevor es kritisch wird

Mit der zunehmenden Datenmenge steigt die Gefahr der Überforderung in SOCs. Der ESET AI Advisor dient hier als System zur Entscheidungsunterstützung, das durch maschinelles Lernen und semantische Analysen Bedrohungen automatisch klassifiziert und kontextualisiert. Anhand bestehender Klassifizierungswerte – wie dem Severity Score aus ESET Inspect – leitet es Handlungsempfehlungen ab. Eine Priorisierung im eigentlichen Sinne erfolgt nicht direkt durch den AI Advisor, sondern basiert auf der Auswertung vorhandener Risikowerte, die durch die Sicherheitsplattform bereitgestellt werden. Die zugrundeliegende Architektur kombiniert Natural Language Processing (NLP), Entity Recognition und modellgestützte Bedrohungsbewertung.

Der AI Advisor verarbeitet unter anderem:

- Echtzeitdaten aus internen Logfiles, globalen TI-Feeds und Malware-Samples,
- Kontextinformationen wie Asset-Kritikalität und Schwachstellen-Exposition,
- bekannte TTPs nach MITRE ATT&CK.

Ein zentrales Element dabei ist die Fähigkeit, große Mengen an Threat-Intelligence-Daten mit kontextsensitiven Metainformationen anzureichern, beispielsweise zur geografischen Verteilung, Branchenrelevanz oder Angriffshistorie. Darüber hinaus lassen sich auch individuelle TI-Fragestellungen adressieren, etwa durch natürliche Fragen wie „Welche bekannten APTs haben in den letzten 7 Tagen Schwachstellen in VPN-Gateways ausgenutzt?“

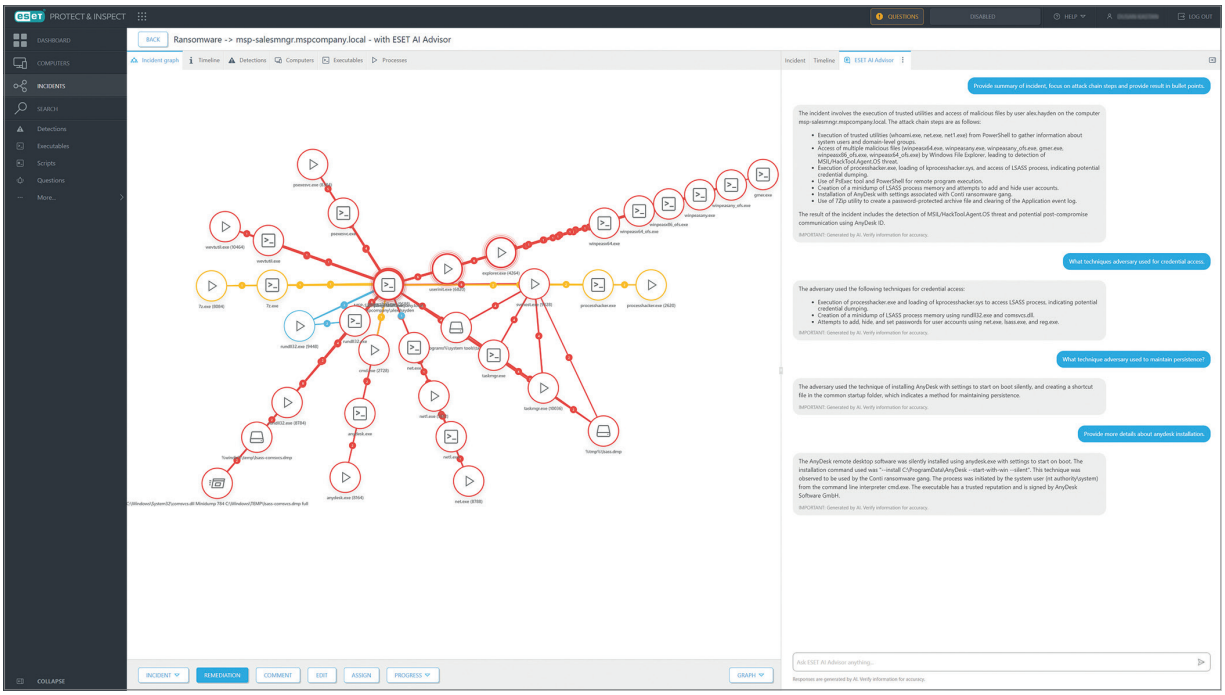
Datensicherheit „Made in EU“

Die Verarbeitung aller Daten erfolgt vollständig in europäischen Rechenzentren – zum Beispiel im von ESET betriebenen Datacenter in Frankfurt – und erfüllt damit höchste Datenschutzanforderungen gemäß Datenschutz-Grundverordnung (DSGVO) und der Netz- und Informationssicherheits-Richtlinie (NIS-2). ESET entwickelt seine Sicherheitslösungen ausschließlich innerhalb der EU und speichert keine sicherheitsrelevanten Kundendaten außerhalb europäischer Hoheitsbereiche. Damit unterstreicht das Unternehmen mit „Made in EU“ seinen Anspruch auf digitale Souveränität und bietet eine echte Alternative zu außereuropäischen Anbietern, bei denen Fragen zur Transparenz und Zugriffssicherheit oft offenbleiben.

Automatisierung als Schlüssel zur Skalierbarkeit

Ein zentrales Ziel moderner TI-Plattformen ist die Automatisierung der Reaktion auf erkannte Bedrohungen. In Verbindung mit Security-Orchestration-Automation-and-Response-(SOAR)-Systemen lassen sich zahlreiche Prozesse automatisieren:

- **IoC-Verarbeitung:** Neue Indikatoren können automatisch zur Blockierung in Firewalls oder Web-Proxies eingesetzt werden.
- **Asset-Matching:** Bei Erkennung einer kritischen Schwachstelle wird automatisch geprüft, welche Assets betroffen sind. Ist das der Fall, wird ein Ticket erstellt oder eine Eskalation ausgelöst.
- **Netzwerksegmentierung:** Erkennt das System *Lateral Movement* oder eine potenzielle Kompromittierung, kann es automatisch



Die Prozessstruktur eines Ransomware-Angriffs, analysiert durch die ESET-Plattform, mit detaillierten Angriffspfaden und Sicherheitsinformationen. (Bild: ESET)

VLAN-Grenzen ziehen oder Quarantäne-Regeln aktivieren.

ESET bietet hier mit ESET PROTECT MDR eine erweiterbare Plattform. Die Kombination aus ESET Inspect (XDR) und MDR-Diensten erlaubt es, Bedrohungsinformationen automatisch in Reaktionspläne zu überführen, beispielsweise durch Isolierung betroffener Hosts, Auslösung forensischer Analysen oder automatischer Eskalation an das Expertenteam. Diese Form der Automatisierung entlastet nicht nur SOC-Mitarbeiter, sondern reduziert Reaktionszeiten drastisch und verringert das Risiko menschlicher Fehlinterpretation.

Praxisbeispiel

Im Jahr 2023 registrierte ESET eine Serie gezielter Ransomware-Angriffe auf mittelständische Unternehmen in Europa. Ausgangspunkt war jeweils ein kompromittierter Remote-Zugriffspunkt über VPN-Dienste mit dokumentierten Schwachstellen. Die Threat-Intelligence-Plattform identifizierte entsprechende IOC-Korrelationen in frühen Phasen der Attacke, etwa durch die Wiederverwendung bekannter Infrastruktur (C2-Domains, Shell-Skripte). Noch bevor ein Payload ausgeführt wurde, konnten betroffene Unternehmen dank automatischer TI-Integration in ihre SIEMs Gegenmaßnahmen einleiten.

ESETs globale Analyseinfrastruktur ermöglichte es, diese Kampagne mit vorhergehenden Angriffen derselben Bedrohungsakteure in Verbindung zu bringen und Kunden mit Frühwarnungen zu versorgen. Dazu zählen kontextualisierte Handlungsempfehlungen, die auf ihre jeweilige Branchenlage zugeschnitten sind.

Damit Unternehmen von Threat-Intelligence profitieren, sollten sie folgende Best Practices berücksichtigen:

_____ **Integration in den SOC-Alltag:** TI sollte nicht als Zusatzfunktion, sondern als Grundpfeiler in SIEM-, EDR- und SOAR-Prozesse eingebunden sein.

_____ **Kontextualisierung vor Aktionismus:** Nur wer IoCs im Kontext der eigenen IT-Landschaft versteht, kann effizient reagieren. Automatische Priorisierung nach Asset-Kritikalität und Angriffswahrscheinlichkeit ist entscheidend.

_____ **Schulungen für Analysten:** Ein effektiver Einsatz erfordert Kenntnisse zu TI-Taxonomien, Feed-Standards, Machine Learning-Grundlagen und Limits KI-gestützter Bewertung.

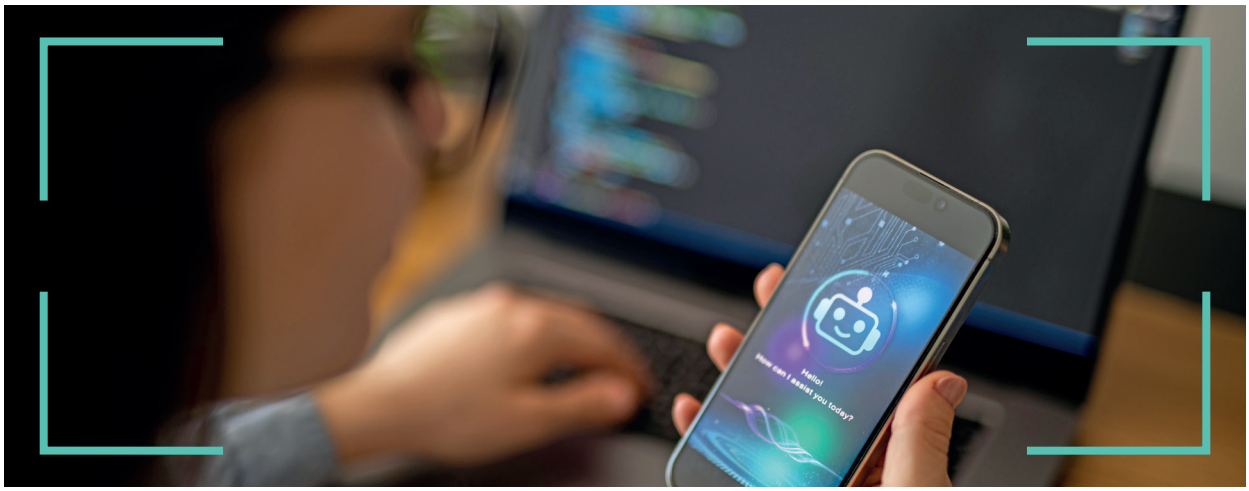
Fazit

Die Digitalisierung des Angriffsraums erfordert eine gleichwertige Digitalisierung der Verteidigung. Threat-Intelligence entfaltet ihr volles Potenzial erst durch die Kombination mit KI-basierter Kontextanalyse und automatisierter Reaktion. ESET Threat Intelligence bietet hier eine skalierbare Lösung, die sich in bestehende Infrastrukturen integrieren lässt und sowohl menschliche Analysten als auch automatische Schutzsysteme mit handlungsrelevanten Erkenntnissen versorgt. Die Zukunft gehört nicht jenen mit den meisten Daten, sondern jenen mit der treffsichersten Interpretation und Umsetzung. Am besten gelingt dies in einem europäischen Sicherheitsökosystem ohne versteckte Hintertüren und mit einem klaren „Prevention First“-Selbstverständnis. ■

TÜVNORD

Zukunftssicher mit KI: Chancen und Risiken verstehen und effektiv managen

Best Practice für ein sicheres KI-Management



Künstliche Intelligenz (KI) ist mehr als nur ein technologischer Fortschritt; sie ist ein entscheidender Faktor für die Zukunftssicherung von Unternehmen. Doch mit den Chancen kommen auch Herausforderungen, die es zu bewältigen gilt. Führungskräfte und IT-Verantwortliche müssen die Gefahren der KI verstehen und effektiv managen, um die Potenziale voll auszuschöpfen.

Gefahren der KI: Eine Bitkom-Umfrage zeigt, dass viele Unternehmen KI als Chance begreifen, aber auch ihre Risiken ernst nehmen. Zu den Hauptgefahren gehören Datenmissbrauch, unvorhersehbare Entscheidungen von KI-Systemen und die Abhängigkeit von automatisierten Prozessen. Diese Risiken können durch die Anwendung regulatorischer und technischer Anforderungen eingedämmt werden.

Chancen der KI: Trotz der Risiken bietet KI enorme Chancen zur Effizienzsteigerung und für Innovationen. Unternehmen können durch den Einsatz von KI ihre Leistung steigern, neue Märkte erschließen, die Kundenzufriedenheit erhöhen und nachhaltige Wettbewerbsvorteile erlangen.

Es gilt eine strukturierte Herangehensweise zu entwickeln.

Best Practices für ein zukunftssicheres KI-Management:

1. Risikobewertung:
Regelmäßige Überprüfung der KI-Systeme und ihrer Auswirkungen auf die Geschäftsprozesse.

2. Rechtskonformität:
Die umfangreiche IT-Compliance-Landschaft mit den regulatorischen und technischen Anforderungen können als Belastung im Mittelstand wahrgenommen werden. Gleichzeitig können diese jedoch dabei helfen, Risiken einzudämmen.

3. Weiterbildung:
Investition in Seminare und Trainings, zur Vorbereitung aller Anwender:innen auf die Herausforderungen, die KI mit sich bringt.

Nutzen Sie unsere breite Auswahl an KI- und IT-Seminaren, um die Herausforderungen in Ihrem Unternehmen effektiv anzugehen.

Zum Beispiel:
- KI und Cybersecurity
- Intensivseminar KI-Management
- KI-Spezialist (TÜV®)

Lesen Sie unseren umfassenden Blog-Beitrag zur „Zukunftssicherheit mit KI“
tuev-nord.de/wissen/ki-gefahren

Ein Schutzschild für Ihr Business!

Entdecken Sie unsere Seminarübersicht für Weiterbildungen zu KI-Themen und finden Sie das passende Angebot für Ihre Bedürfnisse.

Stellen Sie die Weichen für sichere KI-Anwendungen in Ihrem Unternehmen!

Alle Details zu den **TÜV NORD Akademie KI-Seminaren**

Bitdefender®

Global Leader
In Cybersecurity

GravityZone PHASR schützt Ihre systemeigenen Tools vor gezielten Angriffen

Reduzieren Sie Ihre Angriffsfläche durch intelligente Härtung kritischer Betriebssystem-Komponenten – automatisiert, dynamisch, effektiv.

bitdefender.de/phasr

Trusted.
Always.

Modulare Rechenzentren und KI-Sicherheit:

IT-Infrastruktur im Wandel der Bedrohungslagen

Mit dem Aufstieg künstlicher Intelligenz (KI) verschieben sich nicht nur technologische, sondern auch sicherheitspolitische Koordinaten in der digitalen Infrastruktur. Was früher vor allem Rechenleistung bedeutete, wird heute zum strategischen Baustein in der Auseinandersetzung mit immer komplexeren Cyberrisiken. Modulare Rechenzentren gewinnen vor diesem Hintergrund an Bedeutung – als flexible Reaktion auf technische Anforderungen und als Antwort auf volatile Bedrohungsszenarien, in denen Rechenkapazitäten, Energieverfügbarkeit und Sicherheit neu gedacht werden müssen.

Von Michael Lang, noris network AG

Angreifer nutzen zunehmend KI, um Schwachstellen in der IT-Infrastruktur von Unternehmen gezielt auszunutzen. So lassen sich beispielsweise Phishing-Mails mittels generativer Modelle überzeugender gestalten oder Identitätsfälschungen durch synthetische Stimmen sowie Deepfakes perfektionieren. Automatisierte Schwachstellen-Scans oder adaptiver Schadcode, der sich durch maschinelles Lernen laufend der Erkennung entzieht, verschärfen die Lage für Organisationen zusätzlich.

Darüber hinaus ermöglicht es die KI, großangelegte Desinformationskampagnen in sozialen Netzwerken zu koordinieren und zu automatisieren – mit potenziell gravierenden Folgen für politische und wirtschaftliche Stabilität. Sogar das gezielte Training von KI-Modellen auf gestohlenen Daten zur Rekonstruktion sensibler Informationen ist kein theoretisches mehr, sondern ein real gewordenes Szenario.

Verteidigung mit KI: Mustererkennung in Echtzeit

Doch KI ist nicht nur zum probaten Werkzeug von Angreifern geworden. Sie hat sich ebenso zum entscheidenden Mittel zur Verteidigung entwickelt: Lernende Algorithmen ermöglichen es, Anomalien in Netzwerkverkehr, Nutzerverhalten oder Systemprozessen schneller und präziser zu erkennen als klassische, signaturbasierte Systeme. Integriert in Security Operations Center (SOC) und kombiniert mit Security-Information-and-Event-Management-(SIEM)-Lösungen, wird KI zu einem Schlüsselbaustein proaktiver Cybersicherheit. Besonders vielversprechend sind selbstlernende Systeme, die aus vergangenen Angriffen lernen und ihre Erkennungsalgorithmen kontinuierlich und idealerweise in Echtzeit verbessern. Solche Lösungen stellen jedoch hohe Anforderungen an Infrastruktur, Datenqualität und fachliche Expertise, sowohl bei der Implementierung als auch im laufenden Betrieb.

Modularisierung: Strategischer Infrastrukturansatz

Vor diesem Hintergrund gewinnen modulare Rechenzentren an Bedeutung. Sie brechen mit dem klassischen Modell monolithischer Großanlagen, das oft von langen Planungszyklen, hohen Vorabinvestitionen und begrenzter Anpassungsfähigkeit geprägt war. Stattdessen ermöglichen sie eine bedarfsgerechte Skalierung, eine rasche Implementierung von KI-Modulen in rund sechs Monaten, schnelle Inbetriebnahmen und präzise Anpassungen an sich wandelnde technologische Anforderungen oder Sicherheitslagen. Hinzu kommt: Autarke Module lassen sich flexibel kombinieren, ersetzen oder erweitern. Das reduziert nicht nur Kosten, sondern erhöht auch die Reaktionsgeschwindigkeit im Fall neuer Bedrohungen oder technologischer Entwicklungen.

Energie, Kühlung, Standardisierung

Mit steigender Rechenleistung wachsen gleichzeitig die Anforderungen an Energieversorgung und Kühlung. KI-Racks mit hoher Leistung benötigen innovative

Die Abbildung zeigt ein modulares Rechenzentrum von noris. (Bild: @noris network AG)

Versorgungskonzepte, etwa Hochvolt-Gleichstromnetze (HVDC), die Energie effizienter und mit weniger Umwandlungsverlusten direkt ins Rack transportieren. Die Abwärme solcher Systeme kann heute nicht mehr allein mit Luft abgeführt werden. Flüssigkühlung – besonders Direct-to-Chip-Konzepte – hat sich in diesem Zusammenhang als technischer Standard für Hochleistungsrechner etabliert. Der Vorteil: thermische Effizienz, Geräuschreduktion und das Potenzial zur Abwärmenutzung, etwa zur Einspeisung in Fernwärmenetze oder für industrielle Prozesse.

Ein Beispiel für die Umsetzung dieser Anforderungen ist das UHD-KI-Rack von noris network. Die Plattform wurde speziell für den Betrieb von Hochleistungs-KI-Systemen entwickelt und vereint mehrere zentrale Infrastrukturmerkmale: eine elektrische Leistungsaufnahme von mehr als 150 kW pro Rack, eine direkte Flüssigkühlung (Direct-to-Chip) zur effizienten Wärmeabfuhr und eine HVDC-Stromversorgung zur Reduktion von Umwandlungsverlusten. Das System ist modular aufgebaut und lässt sich flexibel in bestehende IT-Umgebungen integrieren. Damit bietet es nicht nur eine technische Antwort auf zunehmende Leistungsdichten, sondern schafft auch eine infrastrukturelle Grundlage für den sicheren und energieeffizienten Betrieb KI-gestützter Anwendungen – vom Training großer Sprachmodelle bis zu sicherheitskritischen Inferenzsystemen im operativen Betrieb.

Hybride Modelle als Infrastruktur der Zukunft

Trotz aller technologischen Fortschritte ist eine wesentliche Herausforderung noch zu meistern: die Standardisierung. Der Markt ist fragmentiert, Schnittstellen sind uneinheitlich, proprietäre Systeme dominieren. Erst durch einheitliche Standards – etwa in Stromversorgung, Wasserkupplungen oder Steuerungssystemen – ließen sich Modularität und Interoperabilität wirklich konsequent umsetzen. Eine moderne Sicherheitsstrategie kombiniert deshalb häufig zentrale und dezentrale Strukturen. Zentrale „KI-Fabriken“ übernehmen rechenintensive Trainingsaufgaben, während Edge-Rechenzentren in Nutzer- oder Standortnähe für die Inferenz und unmittelbare Sicherheitsanwendungen zuständig sind. Dieses „Hub-and-Spoke“-Modell verbindet Effizienz mit Resilienz und adressiert zugleich geopolitische Anforderungen an Datenhaltung und digitale Souveränität. In sicherheitskritischen Bereichen – von der Finanzwirtschaft über das Gesundheitswesen bis zur öffentlichen Verwaltung – eröffnet dieses Modell die Möglichkeit, sowohl Rechenleistung als auch Datenschutz unter operativen Bedingungen zu vereinen. Lokale Verarbeitung sensibler Daten, kombiniert mit zentraler Intelligenz, ergibt eine robuste und flexible Architektur.

Organisationale Voraussetzungen und strategische Planung

Und: Die Einführung modularer KI-Infrastrukturen bedeutet nicht nur technologische, sondern auch organisatorische Veränderungen. Es entstehen neue Rollenprofile: Experten für KI-Infrastruktur, Cybersicherheit und regulatorische Anforderungen müssen eng zusammenarbeiten. Interdisziplinäre Teams, die technisches, operatives und sicherheitspolitisches Know-how bündeln, werden zur Norm. Ferner stehen Organisationen mehr denn je vor der strategischen Entscheidung, ob und in welchem Maße Infrastruktur selbst betrieben oder ausgelagert wird. Gerade modulare Architekturen ermöglichen es, komfortabel hybride Modelle zu fahren: Ein Teil der Ressourcen wird vorgehalten, ein anderer bedarfsgerecht über Partner bezogen – flexibel, kontrollierbar und anpassbar. Unbestritten ist: KI verändert nicht nur die Art von Bedrohungen, sondern auch die Mittel zu ihrer Abwehr. Die daraus resultierenden Anforderungen an Rechenleistung, Skalierbarkeit und Integration machen modulare Rechenzentren zur logischen Antwort auf eine sich wandelnde Sicherheitslandschaft. ■

IT-Sicherheit ist Vertrauenssache

Machen Sie Ihr Unternehmen NIS2-Ready mit ESET Technologien aus der Europäischen Union

eset® Digital Security
Progress. Protected.

eset.de/nis2

Gefragt: Neue Qualifikationen für KI-gestützte IT-Sicherheit

Der deutsche ITK-Markt wächst 2025 um 4,4 Prozent auf 235,8 Milliarden Euro. Besonders dynamisch zeigt sich der Software-Bereich mit einem Plus von 9,5 Prozent auf 52,7 Milliarden Euro, angetrieben durch Cloud-Technologien und Künstliche Intelligenz (KI). Das Geschäft mit KI-Plattformen legt sogar um 50 Prozent auf 2,3 Milliarden Euro zu. Parallel entstehen rund 9.000 neue Arbeitsplätze in der Digitalwirtschaft – so das Ergebnis einer aktuellen Bitkom-Studie.

KI als Chance und Risiko zugleich

KI eröffnet der IT-Sicherheit neue Möglichkeiten: Sie kann Muster in Datenmengen in Echtzeit analysieren, potenzielle Angriffe frühzeitig erkennen und Abwehrmaßnahmen automatisiert einleiten. Gleichzeitig vergrößert sie aber auch die Angriffsfläche. Selbstlernende Systeme können fehlerhafte Entscheidungen treffen oder von außen manipuliert werden, neue Angriffstechniken entstehen, die klassische Schutzmechanismen an ihre Grenzen bringen.

Technologisches Verständnis allein reicht nicht mehr aus

Die zunehmende Komplexität macht deutlich: Technisches Grundwissen allein ist nicht mehr ausreichend. Gefragt ist die Fähigkeit, **KI-Modelle ganzheitlich zu verstehen, zu bewerten und kontinuierlich zu überwachen**. Beschäftigte müssen algorithmische Risiken einschätzen können und wissen, wie sich Datenflüsse, Modellentscheidungen und Sicherheitsarchitekturen gegenseitig beeinflussen.

Neben tiefem technologischen Know-how werden **analytische Fähigkeiten** immer wichtiger. Sicherheitsverantwortliche müssen in der Lage sein, große Datenmengen effizient zu bewerten, ungewöhnliche Muster zu erkennen und daraus Handlungsempfehlungen abzuleiten.

Regulatorische Anforderungen und ethisches Bewusstsein rücken in den Fokus

Mit Vorgaben wie dem AI Act und der DSGVO gewinnen rechtliche und ethische Aspekte stark an Bedeutung. Sicherheitsverantwortliche sollten nicht nur über technisches Fachwissen verfügen, sondern auch regulatorische Anforderungen sicher anwenden können. Ebenso wichtig ist es, Sicherheitsstrategien klar zu vermitteln und Vertrauen bei Mitarbeitenden, Kunden und Partnern zu stärken.

Darüber hinaus ist **Kommunikationsfähigkeit** entscheidend: Sicherheitsstrategien und Maßnahmen müssen transparent vermittelt werden, um Vertrauen bei Mitarbeitenden, Kunden und Partnern aufzubauen.

Spezielle Weiterbildungsmaßnahmen

Unternehmen, die diese vielseitigen Fähigkeiten in ihren Teams systematisch aufbauen, können neue Bedrohungen frühzeitig erkennen, regulatorische Risiken reduzieren und gleichzeitig die Innovationskraft ihrer KI-Anwendungen stärken.

Seminare der Bitkom Akademie wie „KI-Compliance-Beauftragter“, „Cybersecurity 2.0: KI in der IT-Sicherheit“ oder „Cybersecurity Awareness Expert“ helfen dabei, technisches Wissen mit regulatorischem und ethischem Verständnis zu verknüpfen — und so die Grundlage für eine zukunftsfähige Sicherheitsstrategie zu legen.

Haben Sie Fragen zu unseren Seminaren und Inhouse-Angeboten im Bereich KI und IT-Sicherheit? Dann kontaktieren Sie Nicole Stoitschew. ■

n.stoitschew@bitkom-service.de

bitkom akademie

KI zwischen Cybercrime und Cyberdefense

Generative Modelle als Assistenzsysteme der Verteidigung

Generative KI schafft neue Möglichkeiten – für Angreifer ebenso wie für Verteidiger. Während Cyberkriminelle ihre Werkzeuge professionalisieren, hoffen Security-Teams auf intelligente Assistenten, die schneller warnen, analysieren und reagieren.

Von Frank Schwaak, Rubrik

Cyberangriffe werden zunehmend durch den Einsatz von generativer künstlicher Intelligenz (GenAI) professionalisiert. Angreifer nutzen Modelle wie WormGPT oder FraudGPT, um täuschend echte Phishing-Mails zu generieren, Malware-Varianten zu entwickeln oder Inhalte für Deepfake-basierte Kampagnen zu erzeugen. Gleichzeitig steigt die Frequenz erfolgreicher Ransomware-Angriffe rapide – Cybersecurity Ventures zufolge könnte die Zahl bis 2031 auf einen Vorfall alle zwei Sekunden ansteigen.

Darüber hinaus spitzt sich der Mangel an Fachpersonal in der IT-Sicherheit in Deutschland weiter zu. Laut Bitkom werden bis 2040 mehr als 660.000 IT-Stellen unbesetzt bleiben, sofern politische Gegenmaßnahmen nicht greifen. In diesem Spannungsfeld – zunehmende Bedrohung bei abnehmender personeller Abwehrfähigkeit – wird der Einsatz von künstlicher Intelligenz (KI) in der Defensive zu einer strategischen Notwendigkeit.

Schließlich verspricht KI erhebliche Effizienzgewinne, Einblicke und Skalierbarkeit, doch ihr Potenzial ist noch lange nicht ausgeschöpft. Die Überführung von KI-Pilotprojekten in die Produktion und Mehrwert in großem Umfang zu generieren, bleibt eine große Herausforderung für Unternehmen.

Doch wie werden KI-Systeme sinnvoll und verantwortungsvoll in Cybersecurity-Angebote integriert, um dieser sich entwickelnden Bedrohungslandschaft nicht nur zu begegnen, sondern sich proaktiv dagegen zu verteidigen?

Wo KI unterstützen kann – und wo nicht

Während klassische Machine-Learning-Verfahren bereits seit Jahren zur Anomalie-Erkennung im Einsatz sind, zielt der Einsatz generativer KI-Modelle darauf ab, die menschliche Entscheidungsfindung zu unterstützen. Dabei geht es nicht um die vollständige Automatisierung sicherheitsrelevanter Prozesse – vielmehr übernehmen KI-Systeme eine beratende Rolle, etwa bei der Analyse von Vorfällen, der Priorisierung von Maßnahmen oder der strukturierten Wiederherstellung betroffener Systeme.

In sicherheitskritischen Bereichen wie Recovery-Prozessen gilt: Fehlentscheidungen, etwa ausgelöst durch falsch-positive Erkennungen, können operative Systeme gefährden oder zu Datenverlust führen. Daher sehen viele Experten den Einsatz generativer KI in der Cyberabwehr vor allem als Assistenzsystem – mit klaren Leitplanken und menschlicher Kontrolle.

Generative KI als interaktiver Sicherheitsassistent

Ein konkreter Anwendungsfall für GenAI ist die assistierte Reaktion auf Sicherheitsvorfälle mit KI-basierten Chat-Begleitern. Diese intelligenten Begleiter greifen in Echtzeit auf riesige Bestände an technischer Dokumentation, forensischen Daten und komplexen Systemabläufen zu. Dadurch können sie sofort kritische Fragen beantworten wie: „Wie erkenne ich den vollen Umfang dieses Ransomware-Angriffs?“ oder „Wo finde ich das letzte unversehrte Backup?“ – und leiten so Sicherheitsteams mit Präzision und Schnelligkeit an, wenn die Zeit drängt.

Ein Beispiel ist Rubrik Ruby (www.rubrik.com/de), ein GenAI-Begleiter, der in der Rubrik Security Cloud integriert ist. Er wurde entwickelt, um Cyber-Erkennung, -Wiederherstellung und -Widerstandsfähigkeit zu vereinfachen, zu beschleunigen oder zu automatisieren.

Sobald Ruby eine Bedrohung identifiziert, werden die Benutzer sofort benachrichtigt und erhalten über eine


Bild: Radalalstock.adobe.com

interaktive Chat-Schnittstelle eine schrittweise Anleitung. Dies erlaubt eine tiefere Untersuchung der Bedrohung, den Start von Aktionen wie die Suche nach verwandten Indikatoren oder betroffenen sensiblen Daten. Ruby bietet außerdem Empfehlungen für die Quarantäne und Wiederherstellung infizierter Daten sowie herunterladbare Berichte.

Sichere Datenbereitstellung für generative Modelle

Wenn Unternehmen versuchen, GenAI einzuführen, stehen sie vor mehreren Hürden, darunter die Modellgenauigkeit, die Leistung im großen Maßstab und das Kostenmanagement. Darüber hinaus sind Allzweck-LLMs oft langsam sowie kostspielig und Daten in KI-Projekten oft schlecht verwaltet. In Anbetracht dieser Herausforderungen berichtet Gartner, dass voraussichtlich mehr als die Hälfte der KI-Projekte nie in großem Maßstab umgesetzt werden.

Um dieses Dilemma zu lösen und die Einführung von KI zu beschleunigen, hat Rubrik kürzlich seine Absicht bekanntgegeben, Predibase zu übernehmen, eine Plattform für das Training, die Feinabstimmung und den Einsatz von KI-Modellen. Mit dieser Lösung können Kunden die Einführung von agentenbasierter KI beschleunigen und ihre Fähigkeit verbessern, GenAI rasch, kosteneffizient und sicher von der Pilotphase bis zur Produktion zu beschleunigen.

Unterschätzte Identitätsangriffe

Parallel zur Absicherung von Daten rückt der Schutz digitaler Identitäten zunehmend in den Fokus. Die Nutzer-Authentifizierung (Identity) ist ein zentraler Bestandteil der IT-Infrastruktur einer großen Mehrheit der Unternehmen – und bleibt ein konstant attraktives Ziel für Angreifer. Angriffe auf Authentifizierungssysteme zählen laut der US-amerikanischen Cybersecurity and Infrastructure Security Agency (CISA) zu den häufigsten Einstiegsvektoren für erfolgreiche Cyberangriffe. Einmal kompromittiert, ermöglichen gestohlene Identitäten oft eine sich immer weiter ausdehnende Bewegung durch das Netzwerk, bis hin zum Zugriff auf kritische Systeme und Daten wie Anmeldeinformationen. Eine solche Störung kann sogar eine Wiederherstellung nach einem Cyberangriff verhindern.

Insbesondere nicht-menschliche Identitäten (Servicekonten, Zugriffstoken, Automatisierungsschnittstellen) stellen ein wachsendes Risiko dar, da sie oft unzureichend überwacht und schwer zu verwalten sind. Eine wirksame Verteidigung erfordert daher nicht nur Schutzmaßnahmen für Benutzerkonten, sondern ein umfassendes Risikomanagement für alle Arten von Identitäten. Zentrale Elemente dabei sind:

- **Umfassende Risikoanalyse für menschliche und nicht-menschliche Identitäten** mit einer einheitlichen Sicht auf alle Identitätsanbieter
- **Transparenz über Rechteveränderungen** und verdächtige Zugriffsmuster
- **Automatisierte Wiederherstellung** kompromittierter Identitätsinfrastrukturen (zum Beispiel Active Directory, Entra ID)
- **Verknüpfung von Identitätsinformationen mit sensiblen Datenkontexten** zur fundierten Bewertung von Bedrohungen

KI-gestützte Verteidigung mit menschlichem Entscheidungsrahmen

Der Einsatz generativer KI in der Cybersecurity bietet großes Potenzial – vorausgesetzt, er erfolgt geregelt, kontextbezogen und eingebettet in bestehende Sicherheitsprozesse. Generative Modelle können nicht entscheiden, ob ein Recovery-Prozess eingeleitet werden soll oder ob ein Datenabfluss gemeldet werden muss. Sie können aber unterstützen: bei der Informationsbeschaffung, Analyse, Priorisierung und strukturierten Aufbereitung komplexer Zusammenhänge.

Gerade in Zeiten knapper Ressourcen und wachsender Bedrohungslagen eröffnet diese Form der intelligenten Assistenz neue Handlungsspielräume – ohne dabei die Verantwortung zu verschieben. ■

TREND MICRO™ | Global Leader in Cybersecurity

Proaktive Sicherheit beginnt hier.

Ihr Weg zu Innovationen beginnt mit einer Cybersecurity-Plattform, die Risikomanagement, Security Operations und mehrschichtigen Schutz in sich vereint.

Machen Sie Security zum Innovationstreiber mit Trend Vision One™.

Erfahren Sie mehr unter **trendmicro.com/visionone**

Doxing – Bloßstellung mit System

Wenn persönliche Daten zur Waffe werden – Doxing-Risiken und Schutzmaßnahmen für Organisationen

Wenn persönliche Informationen in bösartiger Absicht im Internet veröffentlicht werden, schadet das zwar vordringlich den Betroffenen – doch auch Arbeitgeber oder Organisationen, die mit den „Doxees" im Zusammenhang stehen, können in Mitleidenschaft gezogen werden. Dieser Artikel skizziert typische Abläufe von Doxing-Vorfällen, analysiert die daraus entstehenden Risiken für Unternehmen und Organisationen und gibt praxisnahe Empfehlungen, um solche Angriffe zu verhindern oder ihnen zumindest vorbereitet begegnen zu können.

Von Anjuli Franz, Darmstadt

Doxing bezeichnet die Veröffentlichung persönlicher Informationen über eine Person mit dem Ziel, ihr zu schaden. Der Begriff stammt aus dem Hacker-Slang („dropping Docs") und reicht vom Teilen einzelner Informationen wie Name oder Kontaktdaten bis zum systematischen Aggregieren umfangreicher Datensätze – aus öffentlichen Quellen wie Behördenregistern oder Social-Media-Posts ebenso wie durch Hacking oder Social-Engineering.

Die Motive sind vielfältig: Mal geht es um Deanonymisierung, mal um die Preisgabe des Aufenthaltsorts – häufig ein Einfallstor für physische Gewalt –, oft aber schlicht darum, Betroffene zu delegitimieren, ihre Glaubwürdigkeit zu untergraben und sie als „unseriös" darzustellen. Doxing ist eng mit anderen Formen digitaler Gewalt wie Hatespeech und Stalking verflochten. Die sogenannten Doxer* nutzen es, um Opfer (Doxees) gezielt einzuschüchtern, aus dem öffentlichen Diskurs zu verdrängen, Rache zu üben oder schlicht die eigenen Fähigkeiten im Bereich Open-Source-Intelligence (OSINT) zu demonstrieren [1].

Obwohl Angriffe primär Einzelpersonen treffen, müssen auch Unternehmen und Organisationen diese Gefahr ernst nehmen: Werden Mitarbeiter oder Führungskräfte gedoxt, kann dies als Hebel dienen, um den Betriebsablauf zu blockieren oder strategische Entscheidungen zu beeinflussen. Ein eindrückliches Beispiel sind die Proteste in Hongkong 2019: In einem Telegram-Kanal mit über 50 000 Mitgliedern veröffentlichten Doxer Fotos und Informationen von Polizeibediensteten und deren Familien. Mehr als 800 Betroffene wurden daraufhin belästigt oder sogar gewalttätig angegriffen – mit dem klaren Ziel der Einschüchterung und politischen Einflussnahme [2]. In Deutschland wurden 2019 die Daten von fast 1000 Politikern und Prominenten im Internet veröffentlicht – darunter private Handynummern, Chatprotokolle, Dokumente und Bilder, abgegriffen von öffentlich zugänglichen Quellen sowie durch unsichere Passwörter oder Schwachstellen bei der Passwortwiederherstellung zusammengetragen [3,4].

Neben politisch motivierten Angriffen wird Doxing eingesetzt, um Karrieren zu belasten: Nach Ankündigungen von Massenentlassungen oder bei (vermeintlich) korrupten Praktiken geraten CEOs und andere Führungskräfte ins Visier von Doxern, die das Veröffentlichen persönlicher Informationen als Hebel nutzen, um sie zum Richtungswechsel oder Rücktritt zu drängen.

Typischer Ablauf von Doxing

Doxing-Attacken folgen in der Regel einem typischen Ablauf – das trifft allem voran auf groß angelegte, strategisch orchestrierte Kampagnen zu: In der ersten Phase, dem eigentlichen Doxing per Definition, sammeln Angreifer systematisch Informationen über ihre Ziele. OSINT-Techniken spielen dabei eine Schüsselrolle – soziale Netzwerke, behördliche Register, Medienbe-

richte oder durch Datenlecks veröffentlichte Datensätze dienen als durchsuchbare Archive. Doxing wird deshalb auch als „Low-Key-Hacking" bezeichnet – denn die nötigen Fähigkeiten besitzt prinzipiell jeder durchschnittliche Internetnutzer. Unterstützt wird das Vorgehen von Tools wie KI-gestützter Gesichtserkennung (z. B. PimEyes) oder Google Street View, die das Zusammenfügen digitaler Spuren über verschiedene Plattformen hinweg erleichtern. Häufig entsteht so in Online-Threads ein umfassendes Dossier aus Name, Adresse, beruflichen Hintergründen, Kontaktdaten, privaten Bildern und Korrespondenz – inklusive Details zu Familienangehörigen.

Entscheidend ist hierbei, dass die einzelnen Informationen häufig frei verfügbar und für sich genommen harmlos sind – erst ihre gezielte Zusammenführung und böswillige Rekontextualisierung machen sie gefährlich.

Nach der Veröffentlichung streuen Doxer und andere Personen aus dem Online-Publikum die Daten über soziale Netzwerke, Foren oder Chat-Gruppen. Sie mobilisieren gezielt dem Doxee potenziell feindlich gesinnte Online-Communities, um Momentum zu erzeugen und den Einsatz der veröffentlichten Informationen gegen das Opfer zu fördern. Plattformalgorithmen, die Engagement mit Reichweite belohnen, wirken dabei als Brandbeschleuniger.

Die Folgen für Doxees reichen von Belästigungen über Identitätsdiebstahl bis hin zu physischer Gewalt und wirken oft in alle Lebensbereiche hinein (vgl. [5,6]). Manche Betroffene fühlen sich nach der Veröffentlichung ihrer Adresse so unsicher, dass sie sich für einen Umzug entscheiden. Weil die aggregierten Informationen auf zahlreichen Plattformen vervielfältigt und archiviert werden, stellen sie oft eine langfristige Bedrohung dar.

Für Betroffene beginnt dann ein langwieriger Kampf um rechtliche und technische Gegenmaßnahmen – von Löschanträgen bei Plattformen bis hin zu zivil- oder strafrechtlichen Schritten (etwa nach § 126a StGB). Laut Berichten von Betroffenen und Experten sind diese Prozesse zäh und können mit der Schnelligkeit und Interaktivität digitaler Räume nicht Schritt halten [7,8].

Risiken für Unternehmen und Organisationen

Parallel zu den unmittelbaren Schäden für Einzelpersonen setzt Doxing auch Unternehmen und Organisationen, deren Mitarbeiter zum Ziel solcher Angriffe wurden, erheblichen Risiken aus.

Business-Continuity und Produktivität: Doxing gefährdet direkt die Sicherheit von Mitarbeitern und kann Betriebsabläufe massiv stören – etwa wenn Polizisten oder Ärzte aus Angst vor Übergriffen nicht mehr öffentlich tätig sein wollen oder wenn CEOs oder Politiker durch Bedrohungen vom Tagesgeschäft abgehalten werden. Im Extremfall droht die Einschränkung oder sogar Einstellung kritischer Infrastrukturen.

Reputationsverlust: Koordinierte Doxing-Kampagnen mischen oft wahre Informationen mit Desinformation und schädigen so den Ruf der involvierten Personen und Organisationen nachhaltig. Parallel fluten Angreifer Portale wie Google Reviews oder kununu mit Negativbewertungen, was das Vertrauen von Kunden und Geschäftspartnern untergräbt.

Bindung von Mitarbeitern: Doxing-Vorfälle können schwerwiegende psychosoziale Folgen für Doxees haben [5], was die betroffene Organisation zum Beispiel mit erhöhtem Krankenstand, Kündigungen und Fluktuationen belastet. Wenn die Attraktivität der Organisation im Speziellen oder des Berufsfelds im Allgemeinen aufgrund der Exponiertheit in kontroversen Tätigkeitsfeldern leidet, kann dies ganze Branchen negativ beeinflussen.

Rechts- und Compliance-Risiken: Entstammen veröffentlichte Informationen über Mitarbeiter internen Datenlecks, drohen unter Umständen Bußgelder und Schadensersatzforderungen wegen Verstößen gegen die EU Datenschutzgrundverordnung (DSGVO).

Abbildung 1: Schematische Darstellung eines Doxing-Angriffs und der damit verbundenen Risiken für Organisationen

Abbildung 2: Checkliste für Doxingschutzmaßnahmen

Diese Risikofelder belegen: Doxing ist nicht nur ein individuelles, sondern ein unternehmenskritisches Problem, das proaktive Sicherheits- und Krisenstrategien erfordert.

Präventions- und Schutzmaßnahmen

In der schnelllebigen Welt sozialer Medien, in der sich Kontroversen binnen Stunden zu feindlichen Kampagnen auswachsen können, sollten alle Unternehmen und Organisationen grundlegende Präventivmaßnahmen gegen Doxing treffen. Besonders exponierte Branchen – etwa Politik, Gesundheitswesen, Investigativjournalismus oder zivilgesellschaftlich-aktivistische Organisationen – benötigen zusätzlich klar definierte Reaktionsroutinen.

Als Ausgangsbasis zur Implementierung von Doxing-Schutzmaßnahmen kann die nachfolgende Checkliste dienen, die Maßnahmen zur Prävention, Detektion sowie Reaktion und Schadenswirkung umfasst.

Prävention

_____ *Datensparsamkeit:* Prinzipiell sollten nur wirklich notwendige Angaben zu Mitarbeitern veröffentlicht werden. Obwohl zum Beispiel persönliche Interviews in Werbematerial oder der „Über uns"-Rubrik einer Firmenwebsite ansprechend und nahbar wirken, lassen sich darin befindliche Informationen wie Wohnort oder Familienverhältnisse von Doxern missbrauchen.

_____ *Social-Media-Audits und Awareness-Trainings:* Führungskräfte und öffentlich sichtbare Teams sollten dafür sensibilisiert werden, welche Informationen sie in der eigenen Internetpräsenz veröffentlichen beziehungsweise welche Informationen durch Veröffentlichungen Dritter über sie zu finden sind.

_____ *Grundlegende Informationssicherheitsmaßnahmen:* Zugriffsbeschränkungen, starke Passwörter, Multi-Faktor-Authentifizierung (MFA) und Richtlinien für Mobilgeräte sind auch für die Doxing-Prävention essenziell.

Detektion

_____ *Monitoring öffentlicher Plattformen:* Regelmäßige Scans von Foren, sozialen Netzwerken und sogenannten „Pastebins" sollten für Organisationen mit hohem Doxingrisiko zum Alltag gehören.

_____ *Alerts zum gehäuften Auftreten von Schlüsselbegriffen:* Zur Früherkennung sollten Schlüsselbegriffe (Unternehmens- oder Projektnamen, Namen von Mitarbeitern usw.) in sozialen Medien und Foren automatisiert per API verfolgt und hierfür im Security-Information-and-Event-Management (SIEM) Schwellenwerte definiert werden. So entsteht ein Frühwarnsystem, das bei einer plötzlichen Häufung geteilter Informationen eine schnelle Incident-Response unterstützt.

Reaktion und Schadensminderung

_____ *Interdisziplinäres Krisenteam:* Verantwortliche aus IT, Kommunikation, Recht, Human Resources (HR) und anderen relevanten Funktionen sollten in einem abgestimmten Ablauf zusammenarbeiten.

_____ *Einbindung in bestehende Managementsysteme:* Es empfiehlt sich, Doxing als Bedrohung in bestehenden Business-Continuity-Management- (BCMS) und Information-Security-Management-Systemen (ISMS) abzubilden, Risiken zu bewerten und Notfallpläne regelmäßig zu üben.

_____ *Stärkung von Informationssicherheitsmaßnahmen:* Doxing-Kampagnen gehen häufig mit einem Anstieg an Phishing-Attacken oder illegitimen Zugriffsversuchen einher – entsprechend sollte man nach Doxing-Vorfällen das Security-Monitoring anpassen und die Belegschaft warnen.

_____ *Bereithalten von Vorlagen zur Ansprache von Host-Providern:* Die Kommunikation und Zusammenarbeit mit Host-Providern sind häufig zäh – Meldeprozesse sind versteckt, langsam oder funktionieren nicht, Anbieter fühlen sich für auf ihren Plattformen stattfindende Doxing-Aktivitäten nicht verantwortlich oder berufen sich auf die

Meinungsfreiheit (vgl. [7,8]). Daher sollten klare Zuständigkeiten, Rechtsberatung und vorformulierte Anfragen vorab geklärt sein.

Fazit

Doxing hat sich von einer Nischenpraxis der Hackerszene zu einer ernstzunehmenden Bedrohung für Einzelpersonen und Organisationen entwickelt. Durch das systematische Sammeln und böswillige Rekontextualisieren zuvor häufig öffentlich zugänglicher Daten gefährden Doxer die Sicherheit von Mitarbeitern, beschädigen die Reputation von Organisationen und können im Extremfall ganze Betriebsabläufe lahmlegen.

Besonders gefährdet sind Beschäftigte in öffentlich exponierten Funktionen oder soziopolitisch stark aufgeladenen Bereichen. Die Sicherheit, Handlungsfähigkeit und Glaubwürdigkeit solcher Personen kann durch Doxing massiv beeinträchtigt werden.

Unternehmen und Organisationen sollten Doxing deshalb in ihre Risiko-, Krisen- und Sicherheitsmanagementsysteme integrieren. Präventive Maßnahmen wie Datensparsamkeit, Awareness-Trainings und proaktives Monitoring sowie klar definierte Reaktionsprozesse in IT, Kommunikation, HR und Rechtsabteilung sind essenziell, um Schäden zu begrenzen.

Wer solche Schutzvorkehrungen nachweislich etabliert, stärkt nicht nur die eigene Resilienz, sondern gewinnt auch Vertrauen bei aktuellen und künftigen Mitarbeitern – denn viele Menschen, die beruflich in kontrovers umkämpften Feldern beheimatet und der Öffentlichkeit ausgesetzt sind, sind sich der Gefahren von Doxing und digitaler Gewalt mittlerweile durchaus bewusst. ■

Dr. Anjuli Franz ist Managerin bei PD – Berater der öffentlichen Hand GmbH. Zuvor forschte sie an der Technischen Universität Darmstadt zum Faktor Mensch in der Informationssicherheit.

Literatur

[1] David M. Douglas, Doxing: a conceptual analysis, September 2016, https://link.springer.com/article/10.1007/s10676-016-9406-0 (Open Access)

[2] Paul Mozur, In Hong Kong Protests, Faces Become Weapons, The New York Times, Juli 2019, www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html (Registrierung erforderlich)

[3] Eike Kühl, Eine Waffe namens Doxing, Die ZEIT, Januar 2019, www.zeit.de/digital/datenschutz/2019-01/privatsphaere-doxing-daten-sammeln-datensicherheit-politiker

[4] Siri Warrlich, Doxing-Angriff auf Politiker und Prominente, Diese Konsequenzen zieht das Justizministerium aus dem Datenleak, Stuttgarter Zeitung, Januar 2019, www.stuttgarter-zeitung.de/inhalt.doxing-angriff-auf-politiker-und-prominente-diese-konsequenzen-zieht-das-justizministerium-aus-dem-datenleak.5bbb7bea-478b-42dd-85f3-dd6ba8beecd9.html

[5] Anjuli Franz, Jason Bennett Thatcher, Doxing and Doxees: A Qualitative Analysis of Victim Experiences and Responses, in: European Conference on Information Systems (ECIS) 2023 Research Papers, Juni 2023., S. 397, https://aisel.aisnet.org/ecis2023_rp/397/ (kostenpflichtig)

[6] Daniel Stäcker, Anjuli Franz, Johannes Hett,, Opening Pandora's Dox: Investigating Dynamics Among Doxing Actors Within Online Environments, in: Social and Ethical Implications of Using Digital Tech (ECIS) 2025 Proceedings, Juni 2025, https://aisel.aisnet.org/ecis2025/ethical/ethical/6/ (Open Access)

[7] HateAid, TU München (Hrsg.), Luise Koch, Dr. Angelina Voggenreiter, Prof. Dr. Janina Steinert, Angegriffen & alleingelassen, Wie sich digitale Gewalt auf politisches Engagement auswirkt – ein Lagebild, Studie, Januar 2025, https://hateaid.org/wp-content/uploads/2025/01/hateaid-tum-studie-angegriffen-und-alleingelassen-2025.pdf

[8] Thomas Mrazek, Pressefreiheit – Wir müssen jetzt handeln!, Blogbeitrag, Bayerischer Journalisten-Verband (BJV) e. V., Mai 2025, www.bjv.de/blog/pressefreiheit-wir-muessen-jetzt-handeln/