WHITEPAPER

Cyberbedrohungen mit künstlicher Intelligenz bekämpfen

Stärken Sie Ihre Verteidigung und wehren Sie Angriffe ab

Kurzfassung

Noch vor einigen Jahren wurden in Gesprächen zu künstlicher Intelligenz (KI) überwiegend hochtrabende Versprechen gemacht. Doch nun werden KI-Innovationen immer schneller vorangetrieben – mit positiven, aber auch negativen Auswirkungen auf Unternehmen. Aufgrund des zunehmenden Missbrauchs von effektiven und disruptiven KI-Tools durch Cyberkriminelle stehen Security-Teams vor der schwierigen Aufgabe, ihre Unternehmen und digitalen Infrastrukturen möglichst schnell vor neuen KI-basierten Bedrohungen schützen zu müssen. Positiv wiederum ist, dass Cybersecurity-Anbieter KI-Technologien schon seit vielen Jahren erfolgreich nutzen. Doch da in Zukunft immer mehr Angreifer KI-basierte Taktiken einsetzen werden, müssen Führungskräfte und Teams im Security- und IT-Bereich ihre Sicherheitsstrategien ausbauen, um auch diese komplexen neuen KI-gestützten Bedrohungen abwehren zu können.

Innovationen für eine effektivere Verteidigung

Mit der fortschreitenden Digitalisierung wachsen auch die Angriffsflächen von Unternehmen. Initiativen zur Cloud-Nutzung, Verknüpfung von IT- und OT-Umgebungen, Einbindung von IoT-Geräten in Netzwerke und Unterstützung hybrider Arbeitsmodelle haben eines gemeinsam: Sie sind eine zusätzliche Belastung für Sicherheits- und IT-Teams und deren ohnehin knappe Ressourcen. Die Nutzung von KI-Tools durch Cyberkriminelle verschärft damit eine ohnehin schon angespannte und instabile Situation.

Vor Kurzem brachten Cyberkriminelle mithilfe von Deepfakes des CFO und anderer Angestellter in einer Videokonferenz einen Mitarbeitenden dazu, eine Überweisung in Höhe von 25,6 Millionen USD zu tätigen.[1]

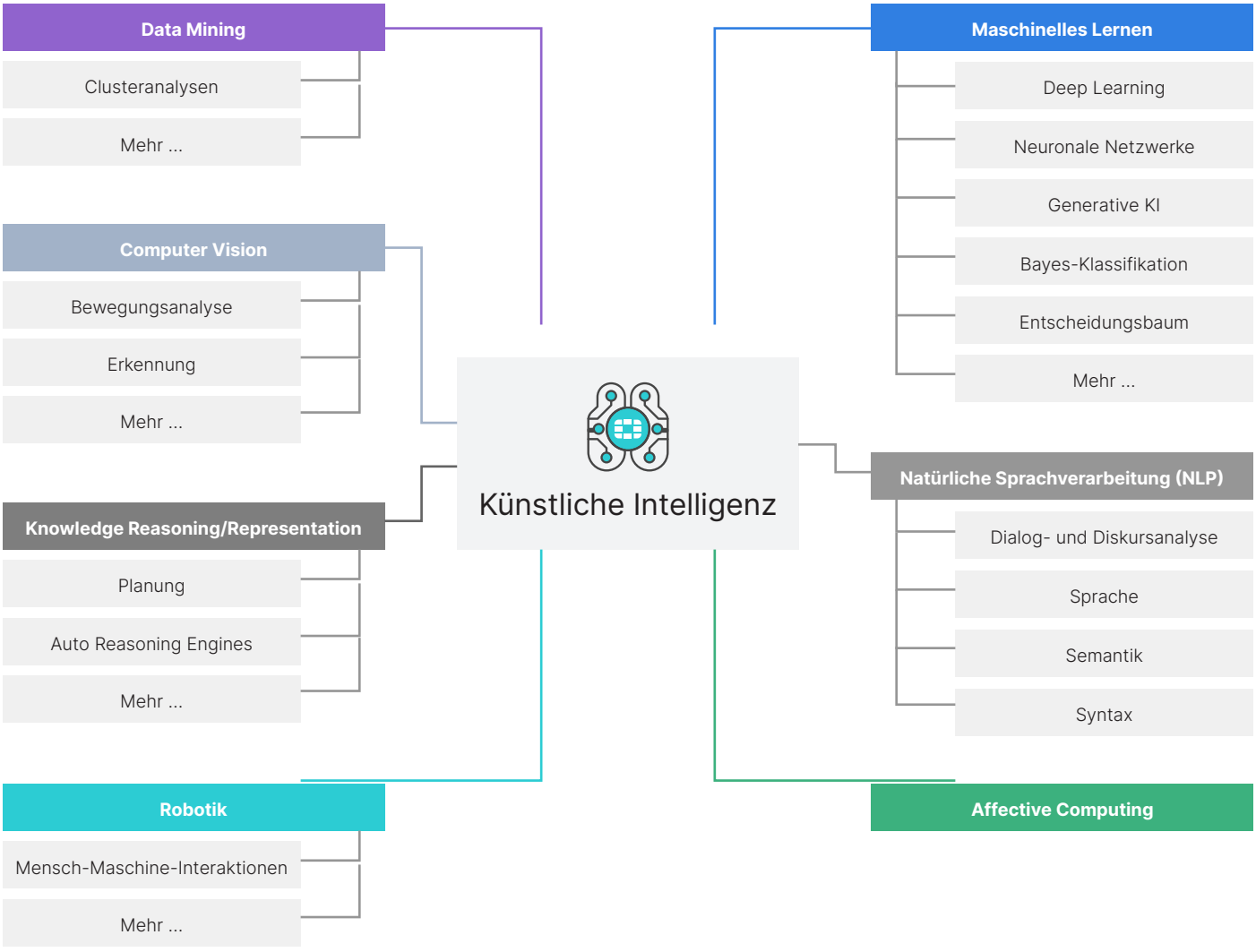


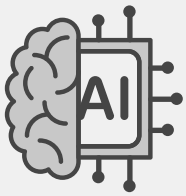
Abbildung 1: Unterkategorien oder Anwendungsbereiche der künstlichen Intelligenz

So nutzen Cyberkriminelle KI

Cyberkriminelle nutzen das Potenzial von KI, um überzeugendere und daher effektivere Angriffe wie Zero-Day-Exploits und andere gefährliche Kampagnen zu entwickeln. Außerdem können Angriffe mit KI schneller als je zuvor durchgeführt werden. In den Händen böswilliger Akteure hat die KI vielfältige Auswirkungen:

- KI-Technologien wie GPT (Generative Pretrained Transformers) oder generative KI (GenAI) senken die Einstiegshürden für neue „Mitspieler", denn damit können Angreifer weltweit auch ohne Englischkenntnisse überzeugende Phishing-E-Mails und Social-Engineering-Kampagnen mit korrekter Syntax erstellen.
- KI kann zur Programmierung von Schadcode verwendet werden und die Entwicklung neuer Malware erheblich vereinfachen.
- Die Nutzung von Deepfake-Technologie durch Cyberkriminelle hat unter Politikern und Wählern bereits für Aufregung gesorgt und ermöglicht auch groß angelegte Cyberkampagnen.
- Mithilfe von KI lassen sich Schwachstellen schneller aufdecken und ausnutzen. Dadurch wächst die Gefahr für Lieferketten von Unternehmen weltweit.
- KI kann auch genutzt werden, um an verschiedene Situationen angepasste Malware-Varianten zu entwickeln und koordinierte Massen- und Multi-Vektor-Angriffe zu starten.

Inzwischen gibt es schädliche KI-Taktiken für alle Schritte im Angriffszyklus des MITRE ATT&CK-Frameworks. MITRE hat die Wissensdatenbank ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) aufgebaut, in der KI-basierte Taktiken und Techniken von Angreifern aufgelistet und erläutert werden.[2]



Informatiker an der University of Illinois Urbana-Champaign haben in einem Versuch ChatGPT-4 von OpenAI in Kombination mit LangChain und dem Playwright-Webbrowser als Agent eingesetzt, um Websites nach Schwachstellen zu durchsuchen und diese dann ohne menschliches Eingreifen auszunutzen. Erstaunlicherweise konnte das Tool den Berichten zufolge einen Prozess aus 38 Schritten für einen SQL-Union-Angriff ausführen.[3]

Zunehmende Herausforderungen

Die Herausforderungen der heutigen dynamischen Bedrohungslandschaft werden durch den Einsatz von KI verschärft und verstärken den Druck auf die ohnehin schon strapazierten IT- und Security-Teams. Der Schutz der wachsenden Netzwerkumgebungen und Angriffsflächen vor diesen neuen Bedrohungen wird durch folgende Probleme zusätzlich erschwert:

- Unzureichender Überblick über die Umgebungen
- Keine zentrale und koordinierte Anwendung und Durchsetzung von Richtlinien
- Nutzung zu vieler separater Security-Tools und -Konsolen, sodass die Bedrohungsüberwachung, Ersteinschätzung von Warnmeldungen, Untersuchung von Sicherheitsvorfällen und Ergreifung von Maßnahmen zu lange dauern
- Andauernder Fachkräftemangel im Security-Bereich

Ein effektiver Schutz vor KI-basierten Bedrohungen ist nur möglich, wenn Unternehmen die Komplexität reduzieren, Konflikte minimieren und ihre Prozesse optimieren.

So nutzen Cybersecurity-Anbieter KI

Die Verschmelzung von KI und Cybersecurity ist nicht nur ein technologischer Fortschritt, sondern vielmehr eine dringend notwendige Entwicklung, um Unternehmen zu helfen, ihre Angriffsflächen besser vor neuen Bedrohungen zu schützen. Viele Cybersecurity-Anbieter nutzen KI-Technologien schon seit Jahren. So erforscht und nutzt Fortinet beispielsweise verschiedene KI-Technologien bereits seit mehr als zehn Jahren und passt sie fortlaufend an, um neue Herausforderungen bei der Bedrohungsabwehr stets meistern zu können.

KI-gestützte Threat Intelligence

Der wichtigste Anwendungsbereich von KI in der Cybersecurity ist die Erkennung und Abwehr von Bedrohungen. Besonders nützlich ist sie bei der Aufbereitung und kontinuierlichen Anreicherung von Threat Intelligence. KI-Technologien werden zur besseren Erfassung, Analyse und Korrelation von Daten genutzt, aus denen sich dann praxistaugliche Informationen und Maßnahmen ableiten lassen. Diese KI-gestützte Threat Intelligence wird dann in Tools zum Schutz vor diversen (KI-basierten und herkömmlichen) Bedrohungsvektoren und -arten integriert. Der Erfolg hängt maßgeblich davon ab, wie ein Anbieter KI-Technologien einsetzt und wie vielfältig die Datenquellen und Daten sind. Je größer die Transparenz, desto mehr können KI-Modelle aus den Daten lernen.

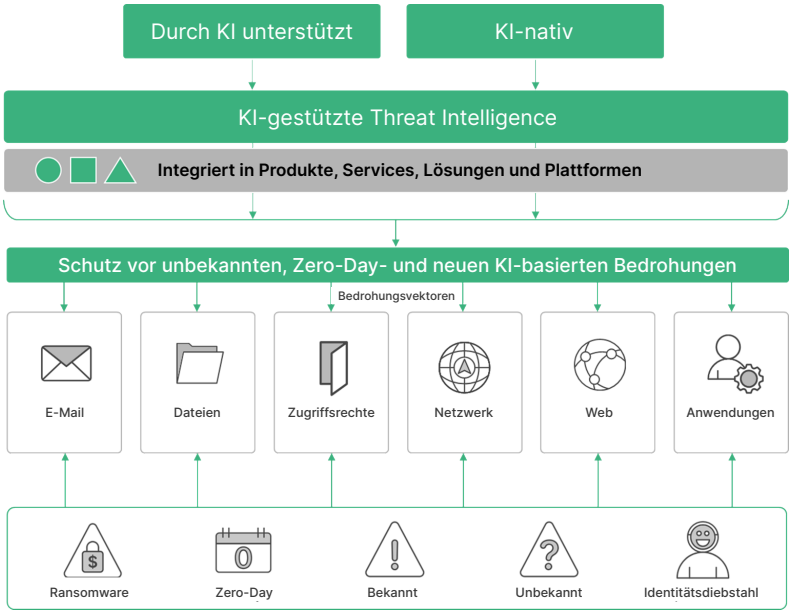


Abbildung 2: KI-gestützte und KI-native Fähigkeiten als Teil der Formulierung von Bedrohungsdaten

Wenn Sie mehr darüber erfahren möchten, wie Ihre Anbieter KI-Technologie nutzen, erkundigen Sie sich am besten zuerst nach der Art der Threat Intelligence, mit der die grundlegende Sicherheitsinfrastruktur Ihres Unternehmens geschützt wird. Ein wichtiger Bereich ist beispielsweise die Firewall-Infrastruktur, die zentrale Abwehrmaßnahme in Unternehmen.

Moderne Next-Generation Firewalls (NGFWs) umfassen mehr Funktionen als herkömmliche Firewalls. Dazu gehören unter anderem integrierte Funktionen für Intrusion Prevention, Malwareschutz – einschließlich Antivirus und Sandboxing –, aber auch Web-Security-Funktionen wie DNS- und URL-Filterung. Da die Anwendungsfälle so vielfältig und relevant sind, besprechen Sie mit Ihrem Anbieter, wie er KI zur Optimierung dieser Firewall-Funktionen nutzt.

Falls er dazu keine Auskunft geben kann, sollten Sie darüber nachdenken, zu einem anderen Anbieter zu wechseln, der transparenter arbeitet und die neuesten Technologien zur Optimierung seiner Lösungen einsetzt.

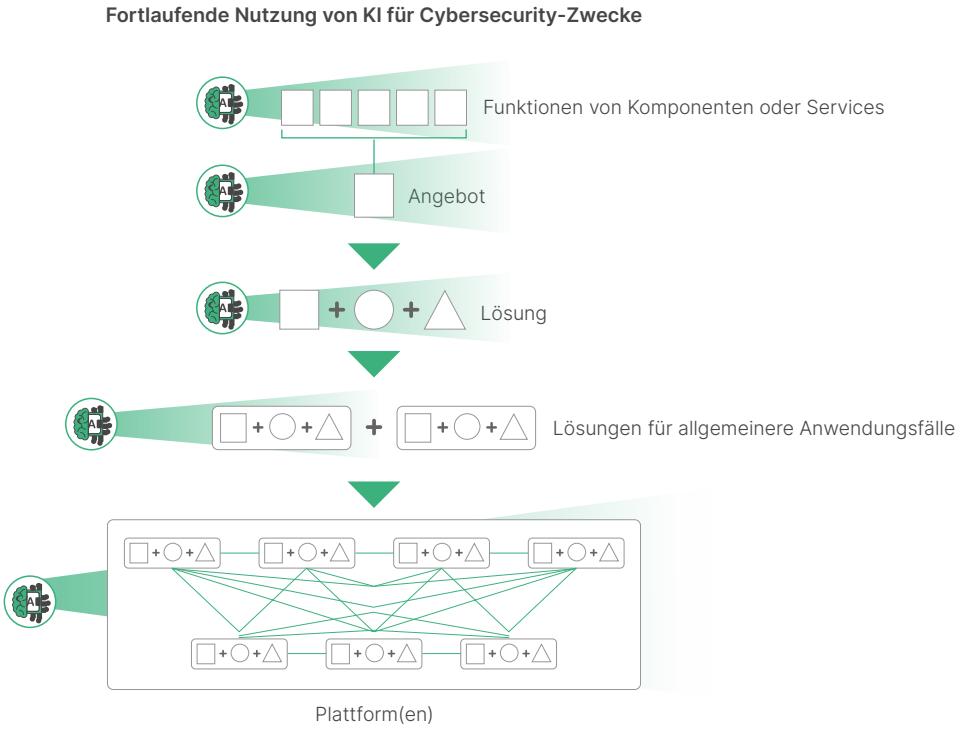


Abbildung 3: Die Anwendung von KI und Threat Intelligence von den Komponenten bis zur Plattform

Moderne durch KI unterstützte Lösungen bieten Vorteile für Anbieter und Kunden:

- **Firewalls:** NGFWs umfassen Security-Funktionen, die oft im Hintergrund von diversen KI-Modellen unterstützt werden. So werden unter Umständen in die Firewall integrierte Intrusion-Prevention-, Antivirus-, Web-Security- und Inline-Sandboxing-Funktionen durch KI-Technologien optimiert. Wenn Hybrid Mesh Firewalls mit NGFWs kombiniert werden, profitieren Unternehmen in mehrfacher Hinsicht: von dem KI-gestützten Bedrohungsschutz, einer besseren Firewall-Transparenz sowie dem zentralen Richtlinien- und Firewall-Management.
- **Application Scanning:** Obwohl Angreifer KI nutzen können, um bösartige Agenten zu erstellen, können Anwendungsscanner und Penetrationstester dieselbe Fähigkeit nutzen, um Schwachstellen sowohl in der Entwicklungs- als auch in der Produktionsphase schneller zu finden und zu beheben.
- **EDR (Endpoint Detection and Response):** EDR-Lösungen nutzen neuronale Netzwerke zur Erkennung von Mustern in den Ereignissen auf Endpunkten. Dazu gehören unter anderem Aktivitäten, Prozesse, Änderungen an Registry-Einträgen und Speicherzugriffe.
- **SIEM (Security Information and Event Management):** SIEM-Lösungen nutzen Modelle für überwachtes und nicht überwachtes maschinelles Lernen (ML), um komplexe lineare Regressionsanalysen durchzuführen. Dazu gehören Support-Vector-Regression, Gauß-Prozess-Regression und Regressionsbäume. ML wird auch für verschiedene Clusteranalysen verwendet. Mithilfe dieser Analysen können SIEM-Lösungen Bedrohungen und Schwachstellen korrekt identifizieren und False Positives minimieren. SIEM-Lösungen nutzen auch GPT-Technologie und natürliche Sprachverarbeitung (NLP), um SOC-Mitarbeitenden Informationen und Empfehlungen bereitzustellen. Analysten können direkte Anfragen an die KI-Engine senden, um Informationen zu Bedrohungen sowie Empfehlungen für angemessene Incident-Response-Maßnahmen zu erhalten.
- **Bildanalyse:** Für die Bildanalyse werden Computer Vision, Bilderkennung und neuronale Netzwerktechnologien kombiniert. Eventuell werden auch Nearest-Neighbor-Algorithmen verwendet. Das Ziel ist, Bilder in eingehenden E-Mails oder Downloads aus dem Internet auf Risiken oder Bedrohungen zu überprüfen. Dazu können QR-Codes, pornografische Bilder, Darstellungen von Gewalt und extremistischen Inhalten oder Bilder gehören, auf denen Waffen, Alkohol oder Drogen zu sehen sind.
- **Penetrationstests:** ChatGPT-4 von OpenAI kann zur Verbesserung von Penetrationstests eingesetzt werden. In Online-Videos wird erklärt, wie sich mit dem Large Language Model (LLM) von ChatGPT-4 innerhalb weniger Minuten entsprechende Python- und Bash-Skripte erstellen lassen.

Das Potenzial von KI ist jedoch nicht auf die Entwicklung und Anwendung KI-gestützter Threat Intelligence beschränkt. Fortinet nutzt KI-Technologien beispielsweise, um die Fortinet Security Fabric-Plattform zu ergänzen und eine proaktive, einheitliche und intelligente Lösung anzubieten.

KI-native Cybersecurity

Neue Cybersecurity-Lösungen, die auf KI-Funktionen aufsetzen, werden häufig als KI-native Cybersecurity bezeichnet. Es gibt zwar keine branchenweite Definition, aber KI-native Cybersecurity-Tools arbeiten mit der Geschwindigkeit eines Computers. So sind beispielsweise die Analyse potenzieller Bedrohungen, die Erstellung einer Einschätzung und die Ergreifung empfohlener Maßnahmen im Handumdrehen möglich. Die schnelle Durchführung von Aktionen hat viele Vorteile – sowohl für die Cybersecurity als auch für den Geschäftsbetrieb. KI-native Cybersecurity-Tools weisen in der Regel folgende Merkmale auf:

- Sie nutzen speziell entwickelte KI-Modelle.
- KI ist von Beginn an eingebettet.
- Sie lernen kontinuierlich dazu und passen sich an neue Bedrohungen an.
- Aktionen werden mit der Geschwindigkeit eines Computers durchgeführt.
- Sie liefern Ergebnisse in Echtzeit.

Anwendungsfälle und Empfehlungen

Security- und IT-Teams außerhalb der Cybersecurity-Branche müssen sich bewusst sein, dass Cybersecurity-Anbieter KI nutzen, und sie müssen sich darüber informieren, welche Art von KI verwendet wird, wie sie eingesetzt wird und vor allem wie das Unternehmen davon profitiert.

In Abbildung 4 sind Beispiele dafür aufgeführt, wie Cybersecurity-Anbieter KI-Technologien in ihren Lösungen nutzen können und welche Vorteile sich daraus ergeben. Sie können diese Liste als Ausgangspunkt nutzen, um Anbieter zu fragen, inwiefern die KI-Funktionen in ihren Lösungen das Sicherheitsniveau von Kundenunternehmen verbessern, insbesondere in Bezug auf KI-basierte Bedrohungen.

Wenn Sie KI in Ihre Sicherheitsstrategien einbinden möchten, empfehlen wir, sich an den folgenden Tipps zu orientieren:

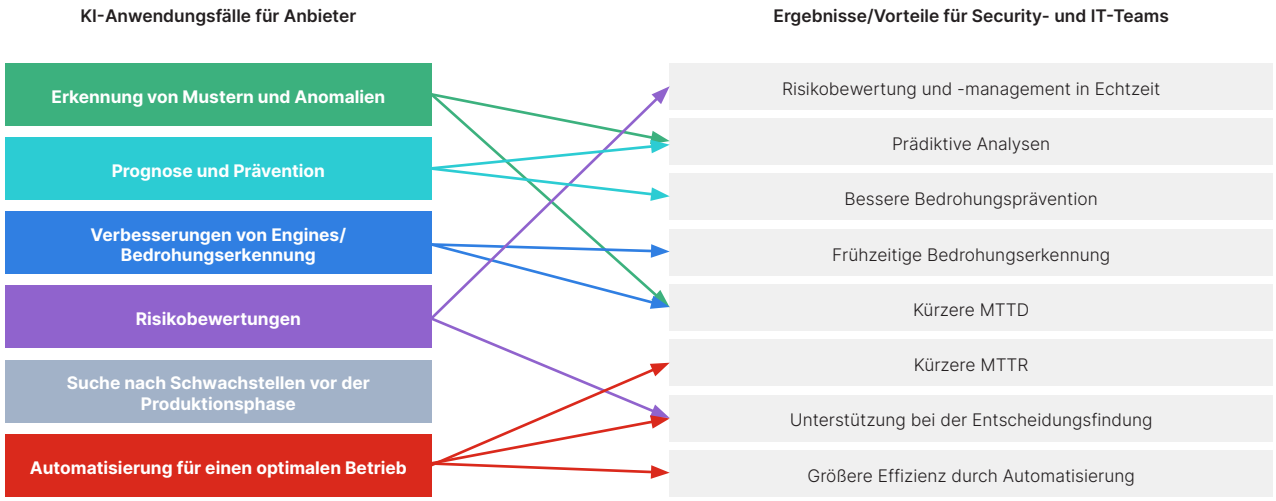


Abbildung 4: Anreize für die KI-Nutzung durch den Anbieter und die sich daraus ergebenden Vorteile für Kunden

Machen Sie KI zur Priorität

Besprechen Sie das Potenzial von KI mit Ihrem Team. Stellen Sie fest, wie gut sich die Teammitglieder bereits mit KI-Technologien und -Prinzipien auskennen. Legen Sie die Einführung von KI als strategisches Ziel in allen wichtigen Security- und IT-Infrastrukturbereichen fest und prüfen Sie diese Bereiche zuerst. Da Anbieter eventuell bereits KI-Technologien in ihren Lösungen nutzen, sollten Sie einen Fragenkatalog und einen Prozess zur Evaluierung der Anbieter in Bezug auf ihre KI-Kenntnisse und -Integration erstellen.

Informieren Sie sich über KI-Technologien

Führungskräfte im IT- und Security-Bereich sollten sicherstellen, dass sie und ihre Teams über KI im Allgemeinen, die Einsatzmöglichkeiten in ihrem Unternehmen und die erworbenen Lösungen informiert sind. Dadurch sind Sie besser vorbereitet, wenn Ihr Unternehmen KI-Technologien testet oder implementiert, und die Teams können dann die richtigen Fragen zu den einzelnen Anwendungsfällen stellen. Es gibt viele kostenlose Online-Ressourcen mit unterschiedlichen Informationen zu KI. Wenn die Führungskräfte und Teams die Grundlagen beherrschen, lohnt es sich eventuell, diese Kenntnisse mit kostenpflichtigen Inhalten oder sogar einem Kurs bei einer angesehenen Einrichtung im Bereich wie beispielsweise SANS weiter auszubauen.

Bleiben Sie auf dem Laufenden

Informieren Sie sich regelmäßig über die neuen KI-Entwicklungen in der Cybersecurity. Das Innovationstempo ist hoch – achten Sie daher darauf, dass Sie nicht den Anschluss verlieren.

Prüfen Sie Ihre Sicherheitsinfrastruktur

Stellen Sie fest, wie Sie KI-Technologie in Ihrer Sicherheitsinfrastruktur einsetzen können. Analysieren Sie zuerst, wie die wichtigsten Abwehrmaßnahmen Ihres Unternehmens von KI-Technologien profitieren könnten, und beziehen Sie dann weitere Kontrollfunktionen in die Überlegungen mit ein. Sie können sich bei dieser Prüfung in vielen Punkten auf Ihren vorhandenen Ansatz für die allgemeine Risikopriorisierung stützen (bei dem die Bereiche mit dem größten Risiko priorisiert werden).

Stellen Sie den Anbietern Fragen

Stellen Sie den Cybersecurity-Anbietern, mit denen Sie zusammenarbeiten, Fragen zur KI-Nutzung. Es ist wichtig, dass Sie verstehen, welche Technologien genutzt werden, wie diese eingesetzt werden und vor allem welche Vorteile die KI für Kunden bietet. Hier sind einige Beispiele für Einstiegsfragen:

- Wie genau nutzen Sie Ihre Einblicke in Bedrohungen und die relevanten Datenquellen für die Entwicklung von Threat Intelligence in Ihrem Produkt/Ihrem Service/Ihren Lösungen?
- Wie wird KI bei der Entwicklung von Threat Intelligence eingesetzt?
- Wie viel Erfahrung hat Ihr Unternehmen bei der Nutzung von KI-Technologien in Produkten/Services/Lösungen?

- Welche KI-Technologien kommen bei diesem Produkt/diesem Service/dieser Lösung zum Einsatz und wie werden sie genutzt?
- Können Sie mir sagen, welche Datenquellen das Produkt, der Dienst oder die Lösung nutzt, um die KI-Technologien zu speisen?
- Wie trainieren und aktualisieren Sie die KI-Modelle?
- Können wir direkt mit der KI-Funktionalität interagieren?
- Wie schützen Sie Daten vor Data-Poisoning-Angriffen?
- Wie unterstützen Ihre KI-Funktionen die folgenden Bereiche?
  - Risikominimierung
  - Bessere Bedrohungsprävention
  - Reduzierung der durchschnittlichen Zeit bis zur Entdeckung (Mean Time To Detect, MTTD)
  - Reduzierung von False Positives
  - Ersteinschätzung von Warnmeldungen und Untersuchung von Vorfällen
  - Reduzierung der durchschnittlichen Zeit bis zur Behebung (Mean Time To Remediate, MTTR)
  - Unterstützung der SecOps-Analysten bei Routineaufgaben

Diese Liste ist nicht vollständig und ist nur als Leitfaden gedacht. Sie sollten die Fragen den Anforderungen Ihres Unternehmens entsprechend anpassen und ergänzen.

Legen Sie KI als entscheidendes Kriterium bei der Wahl eines Anbieters fest

Bitten Sie den Anbieter, bei der Angebotserstellung auch auf die KI-Nutzung einzugehen. Finden Sie mithilfe der oben aufgeführten und Ihrer eigenen Fragen heraus, wie verschiedene Cybersecurity-Anbieter KI nutzen. So erfahren Sie nicht nur, wie der jeweilige Anbieter KI-Technologien zum Schutz seiner Kunden einsetzt, sondern können auch die Antworten der verschiedenen Anbieter vergleichen und feststellen, welche KI-Lösung Ihrem Unternehmen tatsächlich die gewünschten Vorteile bietet.

Fazit

Führungskräfte und Teams im Security- und IT-Bereich müssen sich besser mit den verschiedenen Technologien vertraut machen, die unter das Schlagwort „KI“ fallen. Handeln Sie daher proaktiv: Informieren Sie sich über KI und nutzen Sie deren Potenzial für Ihre Cybersecurity. Viele Anbieter haben bereits KI in ihre Sicherheitslösungen integriert. Sie sollten sich deshalb unbedingt über die verschiedenen Nutzungsmöglichkeiten und Anwendungsfälle informieren, bevor Sie KI-fähige Tools in Ihrem gesamten Unternehmen implementieren. Stellen Sie den Anbietern gezielt Fragen zur Nutzung von KI in ihren Lösungen, bevor Sie eine Kaufentscheidung treffen. Wenn Sie verstehen, wie die Lösungen KI bei Sicherheits- und IT-Prozessen einsetzen, können Sie sich besser vor den komplexen, KI-basierten Bedrohungen von heute schützen.

[1] Heather Chen und Kathleen Magramo, Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’, CNN, 4. Februar 2024.

[2] MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems).

[3] Richard Fang et al., LLM Agents can Autonomously Hack Websites, 6. Februar 2024.

10. Dezember 2024 15:22 / 2604482-A-0-DE