KÜNSTLICHE INTELLIGENZ

Die wesentliche Sicherheitsschicht

Was ist künstliche Intelligenz?

Künstliche Intelligenz (KI) wird allgemein als Prozess der Entwicklung von Computersystemen zur Anpassung an sich ändernde Bedingungen und zur Durchführung von Aufgaben definiert, für die normalerweise menschliche Intelligenz erforderlich wäre. Häufig wird KI als einfaches Modewort abgetan, obwohl es das Konzept der künstlichen Intelligenz (KI) schon mindestens seit den 1950er-Jahren gibt. Avantgardistische Computerwissenschaftler wie Alan Turing stellten die These auf, dass Computer in der Zukunft in der Lage sein könnten, die Arbeit von Menschen auszuführen und intelligente Aufgaben (z. B. Schachspielen) durchzuführen. Der Hype und die Hoffnung im Zusammenhang mit KI kamen in den letzten 60 Jahren in Schüben. Durch Fortschritte im Bereich Computertechnologie konnten plötzlich große Datensätze analysiert werden und die Entwicklung ganz neuer Anwendungen wurde möglich.

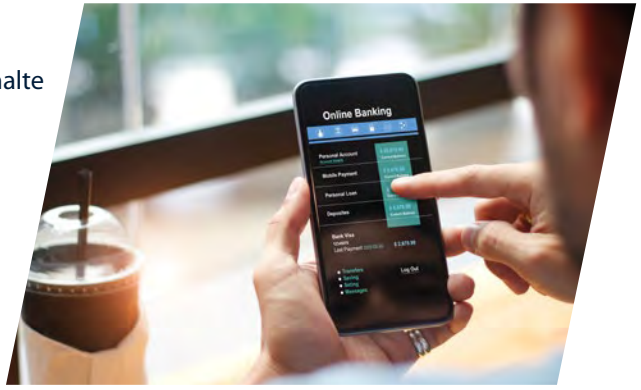
Künstliche Intelligenz im Verlauf der Zeit

KI wird vom Hype zu gefeierter Technologie

In den letzten zwei Jahrzehnten haben sich die Fähigkeiten von künstlicher Intelligenz maßgeblich weiterentwickelt. Nehmen wir nur den knappen Sieg von IBM Deep Blue gegen den Schachweltmeister Gary Kasparov im Jahr 1997 und den Triumph von Watson AI gegen die Jeopardy-Champions Brad Rutter und Ken Jennings im Jahr 2011 – beide Ereignisse zeigen, dass künstliche Intelligenz auf dem Vormarsch ist.

Heutzutage verlassen wir uns in vielen Bereichen des täglichen Lebens auf künstliche Intelligenz.

- **Apps für Mitfahrgelegenheiten** wie Uber und Lyft verwenden KI und maschinelles Lernen zur Bestimmung von Preisen, Vorhersagen der Nachfrage an Fahrern und Schätzung der Ankunftszeit. Teilweise werden Fahrern sogar Empfehlungen zur Änderung des Standorts für die Abholung gegeben, die auf Mustern aus Millionen von erfolgreichen und schwierigen Abholungen basieren.
- **Für das Einlösen von Checks** über Smartphones ist ein komplexes System aus KI und maschinellem Lernen erforderlich, damit Handschrift auf Checks präzise erkannt und zur Verarbeitung in Text umgewandelt werden kann.
- **Bei Videospielen** werden KI-Elemente schon lange eingesetzt, um die Herausforderung für den Gamer zu verbessern. So können Gegner nun mit ihrer Umgebung interagieren und aus früheren Begegnungen mit dem Gamer lernen, sodass sich ihre Erfolgschancen erhöhen.
- **Musik- und Filmempfehlungen** von Spotify, Netflix und Pandora wenden ein einfaches KI-System an, um neue Inhalte anzuzeigen, die individuellen Interessen und Präferenzen entsprechen.
- **Das Investmentmanagement** wird ebenfalls immer intelligenter: Mithilfe von KI werden Finanzportfolios in Übereinstimmung mit Investmentzielen und Risikotoleranzen des Kunden entwickelt und entsprechend den Marktveränderungen in Echtzeit verwaltet.
- **Chatbots und virtuelle Assistenten** werden nun bei vielen Marken an vorderster Front im Kundenservice eingesetzt und sind für zahlreiche Aufgaben vom Recruiting bis zum technischen Support zuständig.



Künstliche Intelligenz wird immer mehr zum wesentlichen Bestandteil unseres Lebens und die Nutzung der Technologie wird in den nächsten Jahren voraussichtlich stark zunehmen. Laut eines Berichts von PWC wird die gesamtwirtschaftliche Bedeutung bis zum Jahr 2030 15,7 Billionen USD erreichen.

Vielen bereitet die Einführung und das Wachstum von KI aber auch große Sorgen. Skeptiker befürchten nicht nur den potenziellen Verlust von Arbeitsplätzen durch Automatisierung, sondern haben auch Bedenken, dass Computer komplexe Aufgaben (z. B. das autonome Fahren) ausführen können.

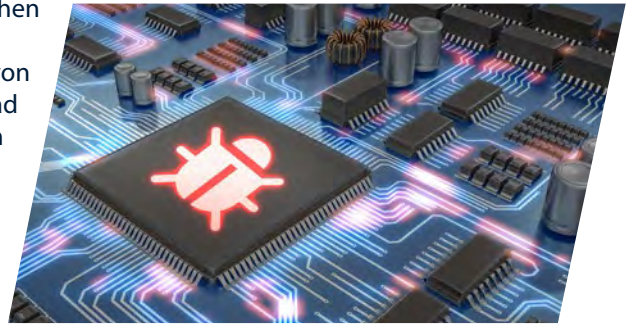
Cyberkriminelle mit KI noch intelligenter

Einer der größten Vorteile von künstlicher Intelligenz ist ihr Einsatz als eine Art Leistungsverstärker. So lassen sich große Mengen von komplexen Daten ganz einfach verarbeiten und stark repetitive Aufgaben ohne menschliches Eingreifen durchführen. Durch die Automatisierung von normalerweise manuellen Prozessen können Kriminelle – vor allen Dingen Cyberkriminelle – ihre Ziele besser anvisieren, den Umfang von Angriffen vergrößern und die Entwicklung von neuer Malware drastisch beschleunigen. Bis zum heutigen Zeitpunkt konnten nur wenige Angriffe beobachtet werden, bei denen KI zum Einsatz kam, doch Sicherheitsforscher arbeiten mit Hochdruck daran, herauszufinden, was alles möglich ist.

Im Folgenden finden Sie einige Beispiele aus der Forschung dazu, wie Angreifer KI verwenden könnten:

- **Umgehen von CAPTCHA-Systemen:** CAPTCHA ist mittlerweile ein wichtiges Tool im Internet, mit dem sich feststellen lässt, ob es sich bei einem Websitebesucher um einen Menschen oder einen Bot handelt. Besuchern wird ein Bild, ein Kontrollkästchen oder ein verzerrter Text angezeigt und sie werden dazu aufgefordert, eine Aktion durchzuführen, die in der Regel nur von einem Menschen bewerkstelligt werden kann (zum Beispiel das Identifizieren von ähnlichen Bildern). Mithilfe von KI-Techniken gelang es Forschern an der Columbia University reCAPTCHA von Google in 98 % der Fälle zu umgehen.

- **Verbessern der Genauigkeit und des Umfangs von Phishing:** 76 % der Organisationen wurden laut Berichten im Jahr 2017 Opfer eines Phishing-Angriffs. Als Reaktion darauf haben viele Organisationen strenge Programme zur Schulung ihrer Mitarbeiter ins Leben gerufen, damit diese Phishing-Versuche erkennen und die Angriffe somit vermieden werden können. Mit KI verfügen Cyberkriminelle über ein Tool, mit dem sie große Mengen von Daten zu ihren Zielen analysieren und Nachrichten erstellen können, die zu einer höheren Erfolgsquote führen. Sicherheitsforscher bei ZeroFox haben einen solchen Ansatz für den Angriff von Twitter-Benutzern mithilfe von SNAP_R (Social Network Automated Phishing with Reconnaissance) demonstriert. SNAP_R nutzt KI zum Identifizieren lohnenswerter Ziele und zur schnellen Entwicklung eines Profils dieses Ziels basierend auf den in der Vergangenheit vom Ziel abgesetzten Tweets. Mithilfe dieses Ansatzes brachten die Forscher Ziele in 30 % der Fälle dazu, auf bösartige Links zu klicken (verglichen mit der 5- bis 15-prozentigen Erfolgsrate anderer automatisierter Ansätze).



- **Entwickeln von extrem gut versteckter Malware:** Hacker haben bei der Entwicklung und Verteilung von Malware lange auf Skripte und Toolkits zurückgegriffen, doch da die Cyberabwehrmaßnahmen immer intelligenter und ausgereifter werden, haben sich Angreifer simplen KI-Techniken zugewandt, um die Tarnung von Malware zu verbessern. Malware-Autoren verwenden nun KI, um Hardwarekonfigurationen und die Umgebungen zu identifizieren, in denen sie sich befinden (z. B. eine Sandbox im Vergleich zu einem physischen Rechner), und um zu bestimmen, ob der Rechner aktuell von einem Menschen bedient wird. DeepLocker (entwickelt von Forschern bei IBM Research) zeigt die Gefahren von künstlicher Intelligenz, die im Rahmen von Malware als Waffe eingesetzt wird. Die KI von DeepLocker ist darauf trainiert, sicherzustellen, dass die Payload nur ausgeführt wird, wenn sie ein bestimmtes Ziel erreicht. Dabei kommen drei Verschleierungsebenen zum Einsatz, die verhindern, dass Sicherheits-Tools die Bedrohung erkennen.

Das Wettrüsten im Bereich Cybersicherheit nimmt immer mehr zu und es lässt sich mit Verlaub sagen, dass wir uns einer neuen Phase nähern, in der KI und maschinelles Lernen eine immer wichtigere Rolle spielen – sowohl beim Angriff als auch bei der Abwehr.

Eine grundlegende Sicherheitsebene für Unternehmen jeder Größe

Cyberangriffe passieren im Bruchteil einer Sekunde. Eine einzelne Infektion kann sich wie ein Lauffeuer von Endpunkt zu Endpunkt, Standort zu Standort und Unternehmen zu Unternehmen ausbreiten. Herkömmliche Ansätze zum Schutz sind in großem Maß von manuellen Prozessen und vorab festgelegten Richtlinien abhängig, um Angriffe abzuwehren. Sie können nicht mit der stetigen Weiterentwicklung von Bedrohungen Schritt halten.

Das Analysieren großer Mengen von Bedrohungsindikatoren ist selbst für die qualifiziertesten Teams ein intensiver, zeitaufwendiger Prozess. Es ist gut möglich, dass Ihre IT-Teams bereits vollständig durch Warn- und Falschmeldungen ausgelastet sind, sodass Angriffe unter Umständen monatelang nicht entdeckt werden. An dieser Stelle bietet KI einen großen Mehrwert. Mit einem soliden KI-Fundament können Sie Zeit sparen, mehr Daten korrelieren, schnellere Entscheidungen treffen, menschliche Fehler minimieren, zukünftige Bedrohungstrends vorhersagen und gleichzeitig Ihren Sicherheitsstatus verbessern.

Welche Probleme können Sie mit KI lösen?

Mangel an Sicherheits-Know-how

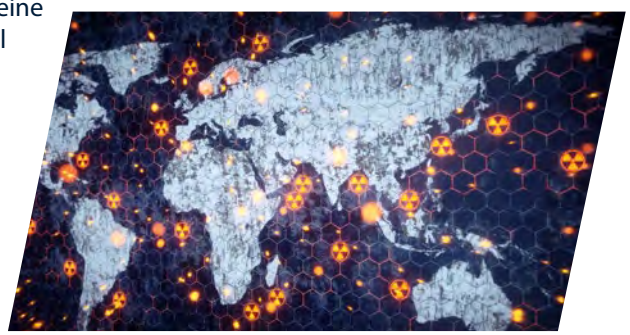
- Viele Organisationen, vor allen Dingen kleine Unternehmen, verfügen nicht über ausreichend Personal und Know-how im Bereich Sicherheit. IT-Teams haben in Unternehmen häufig mehrere Rollen und Verantwortungsbereiche. KI ermöglicht die Automatisierung von Sicherheitsprozessen – eine Zeitersparnis, durch die IT-Mitarbeiter sich stärker auf geschäftskritische Aufgaben konzentrieren können. Tatsächlich können Aufgaben, für die normalerweise ein fachkundiger Sicherheitsanalyst erforderlich wäre, so mithilfe von KI durchgeführt werden, zum Beispiel die Durchsicht großer Mengen von Sicherheitsdaten und automatische Maßnahmen zur Verbesserung des Sicherheitsstatus.

Ressourcenbeschränkungen

- SIEM- und Sicherheits-Management-Tools sind für kleinere Organisationen mit engen Budgets unerschwinglich. Obwohl die Daten vorhanden sind, kann ein Großteil von ihnen aufgrund von zeitlichen Beschränkungen nicht rechtzeitig analysiert und verarbeitet werden, um eine effektive Nutzung sicherzustellen. Bei entsprechender Implementierung kann KI die Korrelation, Analyse und Bewertung für Sie übernehmen und gleichzeitig aus verschiedenen Threat-Intelligence-Quellen lernen, um Wachsamkeit im Hinblick auf Cyberangriffe zu gewährleisten. Zum können Sie mithilfe von KI auch die Behebung automatisieren – mit minimalen Unterbrechungen für Ihren Geschäftsbetrieb.

Bedrohung durch Zero-Day- und versteckte Malware

- Richtlinien und Signaturen sind schnell veraltet, sodass sie eine große Sicherheitslücke hinterlassen, wenn keine anderen Maßnahmen verwendet werden. KI stellt intelligente Abwehrebenen bereit, sodass Sie Malware viel schneller erkennen und abwehren können als mit herkömmlichen Ansätzen. Bei entsprechendem Training bietet KI prädiktive Schutzmechanismen, die zukünftige Bedrohungen antizipieren, ohne dass Signaturen, Cloud-Konnektivität usw. erforderlich sind. KI kann Hunderttausende Merkmale einer bestimmten Datei untersuchen und den Bedrohungsgrad der Datei schnell bestimmen.



Team

Das Ziel eines jeden Sicherheitsanalysten ist es, Angriffe so effektiv wie möglich zu vermeiden und Bedrohungen so früh wie möglich zu erkennen und abzuwehren. Dank Automatisierung übernimmt KI die Rolle eines fachkundigen Sicherheitsanalysten, der rund um die Uhr daran arbeitet, Sie zu schützen. KI ermöglicht die Automatisierung von:

PRÄVENTION
Ohne die Notwendigkeit von Signaturen oder Cloud-Konnektivität

ERKENNUNG
Mithilfe von selbstlernenden Tools für statische und dynamische Analysen

RESPONSE
Über korrelierte Bedrohungsbewertung

KI im Sicherheitdienstportfolio

Im Rahmen des WatchGuard-Sicherheitsserviceportfolios fungiert künstliche Intelligenz als eine Art Leistungsverstärker, der die Automatisierung von Prozessen ermöglicht und den Schutz gegen aufkommende Bedrohungen umfassend verbessert. Während sich die Sicherheitsimplementierungen von KI immer weiterentwickeln, sorgt die Technologie für eine Verknüpfung all unserer Portfolioplattformen und bietet so auf dem einfachsten und praktischsten Wege die tiefsten Einblicke sowie den modernsten Schutz gegen zukünftige Angriffe.

Was können Sie von KI in unserer Lösung erwarten?

Prädiktiver Schutz: Die Verzögerung zwischen der Erkennung einer Malware-Bedrohung und der Möglichkeit zur Anwendung von Signaturen, Heuristik und Verhaltensmustern stellt eine große Herausforderung dar. Antivirus mit KI bietet prädiktiven Schutz gegen Malware-Bedrohungen – und das 25 Monate bevor diese in der Praxis auftreten.

Schnellere Erkennung: Um gut versteckte Malware-Bedrohungen rechtzeitig erkennen und abwehren zu können, benötigen Sie das Know-how und die Möglichkeit, nach Tausenden Indikatoren für böswillige Angriffe zu suchen. Unsere Engine zur Korrelation und Bewertung erkennt verdächtige Dateien und verschiebt diese zur tiefergehenden Analyse in eine Sandbox der nächsten Generation. Während dieser gründlichen Prüfung nutzt diese Sandbox KI, um Dateien umfassend zu analysieren.

Automatisierte Bedrohungsabwehr: Mithilfe von künstlicher Intelligenz lassen sich große Mengen von Daten aus praktisch jeder erdenklichen Quelle erfassen und diese Daten können für Trainingszwecke verwendet werden, um höhere Sicherheit zu gewährleisten. Unsere Sicherheitsdienste werden durch einen konstanten Fluss neuer Daten, Feedback und Training stetig weiterentwickelt, sodass Ihr Sicherheitsstatus verbessert wird.

In Anbetracht der Raffinesse aufkommender Bedrohungen und der Geschwindigkeit ihrer Weiterentwicklung bietet künstliche Intelligenz ein wichtiges Tool beim Wettrüsten im Bereich Cybersicherheit in Organisationen jeder Größe. Als Branchenführer beim Thema Sicherheit suchen wir nach neuen Möglichkeiten zur Weiterentwicklung der Produkte und Services mit KI-Technologien.

Unsere Produkte nutzen WatchGuard-Technologie

WatchGuard® gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Es bietet die zentralen Technologien, um sich gegen die heutigen aggressiven Bedrohungen zu wehren.