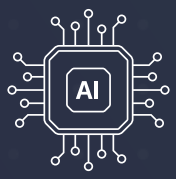
LINK11



WHITEPAPER

Algorithmen vs. Angreifer: wie KI die Cyber-Resilienz stärkt

www.link11.com

Liebe Leserinnen und Leser,

In einer Zeit, in der digitale Innovationen die Geschäftslandschaft transformieren, stehen wir vor einer unverkennbaren Realität: Die Sicherheit unserer IT-Systeme und Daten ist nicht nur eine Herausforderung, sondern eine strategische Notwendigkeit. Die Cyberangriffe werden komplexer, es kommen raffiniertere Methoden zum Einsatz und die Professionalisierung der Angreifer nimmt zu.

Es ist daher unerlässlich, proaktiv zu handeln und Cybersicherheit als einen Wettbewerbsvorteil zu betrachten. Dieses Whitepaper beleuchtet, wie künstliche Intelligenz nicht nur als Herausforderung, sondern als entscheidendes Werkzeug in der Cybersicherheitsstrategie fungieren kann. Es ist an der Zeit, dass wir gemeinsam die Zukunft der Cybersicherheit gestalten und mit den innovativsten Lösungen die Sicherheit der Unternehmen stärken.

Ich wünsche Ihnen eine spannende Lektüre!

Herzliche Grüße
Jens-Philipp Jung, CEO, Link11

Inhalt

Einleitung

Die Einführung von ChatGPT im November 2022 markierte einen bedeutenden Meilenstein in der Entwicklung der künstlichen Intelligenz (KI), indem sie der generativen KI (GenAI) einen enormen Schub verlieh. Diese fortschrittliche Technologie wird als zukunftsweisend angesehen und hat das Potenzial, die Produktivität weltweit erheblich zu steigern.

Die Auswirkungen dieser Technologie sind tiefgreifend. Bis 2030 könnten rund 30 % der aktuellen Arbeitsstunden durch Technologien wie generative KI automatisiert werden.[1] Ein schneller Einsatz dieser Technologien könnte das Produktivitätswachstum auf bis zu drei Prozent pro Jahr steigern. Kein Wunder also, dass die Nachfrage besonders nach GenAI, aber auch nach Machine Learning (ML) sowie anderen KI-Anwendungen exponentiell wächst.

Künstliche Intelligenz wie Machine Learning spielt eine entscheidende Rolle bei der frühzeitigen Erkennung von Cyberbedrohungen. Durch die Analyse großer Datenmengen können diese Technologien Anomalien und verdächtiges Verhalten in Netzwerken oder Systemen identifizieren, was schnelle Reaktionen und effektive Gegenmaßnahmen ermöglicht. IT-Sicherheitslösungen nutzen zunehmend Automatisierung durch KI, um potenzielle Sicherheitslücken zu erkennen und zu schließen. Dazu gehört etwa die automatische Priorisierung von Sicherheitsupdates sowie die kontinuierliche Überwachung und Anpassung der Sicherheitsmaßnahmen an neue Bedrohungen.

Die Mehrheit der IT-Führungskräfte ist der Meinung, dass Cyberangriffe ausgeklügelter und die Angreifer deutlich professioneller geworden sind. Viele von ihnen fühlen sich nicht ausreichend auf die neuen Bedrohungsvektoren vorbereitet, insbesondere auf KI-gestützte Angriffe. Die zunehmenden weltweiten Spannungen und Cyberangriffe bereiten auch den deutschen CEOs Sorgen. Laut der PwC Global CEO-Survey sehen 42 % der deutschen CEOs ihr Unternehmen in den nächsten zwölf Monaten stark durch Cyberrisiken gefährdet. Im globalen Vergleich sind es lediglich 21 %.[2]

Kriminelle nutzen KI etwa, um Phishing-Mails effektiver zu gestalten und geschäftskritische Informationen zu stehlen, während Sicherheitsanbieter KI einsetzen, um diese Bedrohungen zu erkennen und zu blockieren. Dieses ständige Wettrüsten erfordert einen proaktiven Sicherheitsansatz, der sowohl fortschrittliche Abwehrmechanismen als auch grundlegende Best Practices zur Risikoeindämmung umfasst.

Angesichts des globalen Mangels an über drei Millionen Cybersicherheitsfachkräften[3] wird die Automatisierung von Cybersicherheitsoperationen als entscheidend angesehen. Sie ermöglicht es, hochspezialisierte Fachkräfte im Bedrohungsfall schneller einzusetzen und damit auf Bedrohungen effektiver zu reagieren. Dem „Digital Trust Insights“[4] von PwC zufolge erkennen inzwischen Unternehmen weltweit, dass das Management von Cyberrisiken entscheidend für den Geschäftserfolg ist, was die geplanten Investitionen in Cybersicherheit zunehmen lässt.

Die rasante Entwicklung von KI hat weitreichende Auswirkungen auf die Cybersicherheitslandschaft. Angreifer nutzen KI, um die Komplexität und Effektivität ihrer Angriffe zu steigern, während Verteidiger KI zur Automatisierung und Verbesserung ihrer Sicherheitsmaßnahmen einsetzen. Das Whitepaper beleuchtet diese dynamische Beziehung und unterstreicht die Notwendigkeit, in fortschrittliche Technologien zu investieren. Gleichzeitig sollten Unternehmen einen robusten Rahmen für das Risikomanagement entwickeln, um die Vorteile der KI voll auszuschöpfen und dadurch die eigenen Sicherheitsstandards zu maximieren.

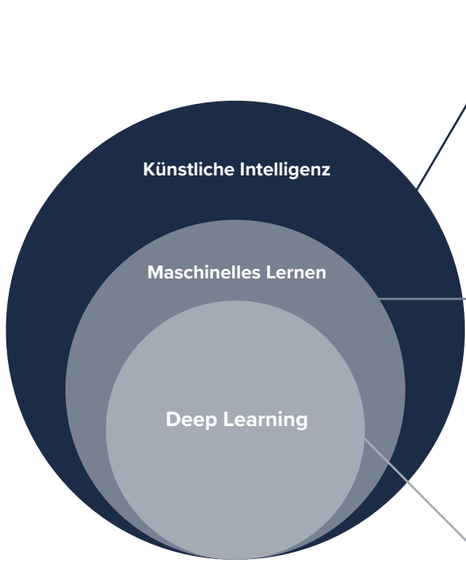
„Unternehmen, die in KI und moderne Cybersicherheitsmaßnahmen investieren, erhöhen ihre Widerstandskraft und können sich einen Wettbewerbsvorteil sichern.“

Jens-Philipp Jung, CEO, Link11

Was ist KI?

Im Bereich der künstlichen Intelligenz (KI) entwickeln und nutzen Wissenschaftler Methoden, um maschinelle Systeme zu schaffen, die eigenständig komplexe Probleme lösen. Diese Systeme übernehmen Entscheidungsprozesse, die traditionell menschliche Intelligenz erforderten. KI setzt Techniken wie Machine Learning (ML) und Deep Learning (DL) ein, um Muster in großen Datensätzen zu erkennen und basierend darauf Entscheidungen zu treffen.

Formen der künstlichen Intelligenz



Künstliche Intelligenz:

Künstliche Intelligenz (KI) beziehungsweise Artificial Intelligence (AI) simuliert menschliche Intelligenz mit Maschinen, insbesondere Computersystemen. Dies umfasst das Lernen (die Erfassung von Informationen und Regeln für die Verwendung der Informationen), die Schlussfolgerung (die Verwendung der Regeln, um ungefähre oder endgültige Schlussfolgerungen zu ziehen) und die Selbstkorrektur. Besondere Anwendungen der KI sind Expertensysteme, Spracherkennung und Machine Vision.

Maschinelles Lernen:

Machine Learning (ML), im Deutschen maschinelles Lernen, ist ein Teilgebiet der künstlichen Intelligenz. Durch das Erkennen von Mustern in vorliegenden Datenbeständen sind IT-Systeme in der Lage, eigenständig Lösungen für Probleme zu finden.

Deep Learning:

Deep Learning (DP) ist ein Teilbereich des Machine Learnings und nutzt neuronale Netze sowie große Datenmengen. Die Lernmethoden richten sich nach der Funktionsweise des menschlichen Gehirns und resultieren in der Fähigkeit eigener Prognosen oder Entscheidungen.

Der Begriff künstliche Intelligenz wurde 1956 im Rahmen einer Konferenz führender Wissenschaftler, wie etwa dem amerikanischen Informatiker und Gründungsvater der KI John McCarthy, am Dartmouth College geprägt. KI hat sich parallel zur Steigerung der Rechenleistung und der Datenbanktechnologien immer weiterentwickelt. Heutige Systeme können enorme Datenmengen in Echtzeit verarbeiten und sind besonders reaktionsschnell. Aktuell werden drei Arten von KI unterschieden:

- **Schwache künstliche Intelligenz (Weak/Narrow AI):** Spezialisiert auf singuläre und zielorientierte Aufgaben wie Zeichen-, Text- oder Gesichtserkennung, Internet-Suchmaschinen sowie Navigationssysteme.
- **Starke künstliche Intelligenz (Strong/General AI):** Theoretisch in der Lage, intellektuelle Aufgaben wie ein Mensch zu meistern. Eine KI, die ursprünglich für das Extrahieren von Text aus einem Bild entwickelt wurde, könnte beispielsweise ohne zusätzlichen Trainingsaufwand auch Text aus einem Video extrahieren. Solche Aufgaben erfordern jedoch fortgeschrittene Rechenkapazitäten und daher wurde dieses Level bisher noch nicht erreicht.
- **Künstliche Superintelligenz (Super AI):** Eine theoretische Zukunftsvision, in der die KI in der Lage wäre, sich selbst zu verbessern, eigene Werte und Ziele zu setzen und diese an verschiedene Situationen und Umgebungen anzupassen.

Vom Online-Handel bis zur IT-Sicherheit: Vielfältige Einsatzmöglichkeiten der KI

Anwendungen von KI im Alltag	Anwendungen von KI in der Geschäftswelt	Anwendungen von KI in der Cybersicherheit
Personalisierte Empfehlungen im Online-Handel	ML-Algorithmen analysieren Daten für Chatbots und Autonomie	Bedrohungserkennung und -abwehr in Echtzeit
Sprachassistenten wie Amazon Alexa und Siri	Nutzung von Deep Learning für Gesichts- und Stimmerkennung	Erkennung und Abwehr von Malware- und Phishing-Angriffen
Verbesserter Online-Übersetzer durch Neural Machine Translation	Virtuelle Support-Agenten bieten IT-Support und automatisieren Aufgaben	Virtuelle Support-Agenten bieten IT-Support und automatisieren Aufgaben
Gesichtserkennung bei Smartphones und Sicherheitsanwendungen (Face ID)	KI verbessert Planung, Wartung und Automatisierung in der Lieferkette	Identitäts- und Zugriffsmanagement
PayPal-Betrugserkennung	KI identifiziert neue Leads und optimiert Verkaufsprozesse	Transaktionsüberwachung und Betrugserkennung
Einsatz in Medizin und Pflege	Echtzeit-Personalisierung und Optimierung von Kampagnen	Schutz von Daten und persönlichen Informationen
Autonome Fahrzeuge und intelligente Fahrassistenzsysteme	Virtuelle Assistenten bieten proaktiven Kundenservice und Qualitätskontrolle	Sicherstellung der Integrität und Vertraulichkeit von Daten

Von Turing bis zu ChatGPT: Die wichtigsten Momente in der Geschichte der künstlichen Intelligenz

Einige Highlights in der Entwicklung der künstlichen Intelligenz sind:

1950er Jahre
Die Geburtsstunde der KI, als die ersten Algorithmen auf Basis elektrischer Schaltungen entwickelt wurden. Dies markiert den Beginn der Forschung und theoretischen Konzeption zur künstlichen Intelligenz.

1970er Jahre
Nach einem anfänglichen Hype um KI, der durch ehrgeizige Erwartungen geprägt war, begann der „KI Winter“, in dem Forschungsgelder gestrichen wurden und das Interesse stark nachließ. Dieser Zeitraum war geprägt von Enttäuschungen und einem Mangel an Fortschritten.

1997
Ein bedeutender Moment, als der Schachcomputer IBM Deep Blue den amtierenden Schachweltmeister besiegte. Hier zeigten sich erstmals die Fähigkeiten von KI in einem spezifischen Anwendungsbereich und das erhielt große Medienaufmerksamkeit.

2010er Jahre
Eine Renaissance für KI, unterstützt durch Fortschritte in der Hardware und der Verfügbarkeit großer Datenmengen. Dieser Zeitraum war geprägt von bedeutenden Durchbrüchen im Bereich des maschinellen Lernens und der tieferen Integration von KI in verschiedene Anwendungen.

2013
Das Startup DeepMind entwickelte eine KI, die selbstständig lernte, Atari-Software zu spielen. Dies war ein früher Hinweis auf die Fähigkeit von KI, komplexe Aufgaben durch selbstständiges Lernen zu bewältigen.

2015
Ein Deep Neural Network von Microsoft Research erreichte bei der Bilderkennung dieselben Fehlerraten wie ein Mensch. Das markierte einen bedeutenden Fortschritt in der visuellen Wahrnehmung durch KI.

2016
Google DeepMind entwickelte AlphaGo, eine KI, die den weltbesten Go-Spieler besiegte, was die Fähigkeit von KI unterstrich, strategische und komplexe Probleme in einem Spielkontext zu lösen.

2022
Open AI sorgte mit ChatGPT weltweit für Aufsehen - einem intelligenten Sprachmodell, das natürliche menschliche Unterhaltungen führen kann. Damit hat KI in Bezug auf Sprachverarbeitung und -verständnis ein neues Niveau erreicht.

Gefahren für künstliche Intelligenz

Die Integration von KI-Systemen verspricht effizientere Prozesse, bessere Entscheidungsfindungen und neue Möglichkeiten in der Automatisierung. Während die Vorteile und Potenziale von KI weitreichend sind, lauern beim Einsatz erhebliche Gefahren, insbesondere durch spezialisierte Angriffsvektoren, die gezielt Schwachstellen in KI-Systemen ausnutzen.

Adversarial Attacks haben sich als eine ernsthafte Bedrohung für KI-Systeme herausgestellt. Diese Angriffe zielen darauf ab, die Integrität und Funktionalität von KI-Modellen durch gezielte Manipulation von Eingabedaten zu untergraben. Angreifer können speziell gestaltete Eingaben nutzen, um das Modell zu falschen Vorhersagen zu bringen, wodurch die Wirksamkeit der KI erheblich beeinträchtigt wird.

Zu den Hauptarten von Adversarial Attacks gehören das Einbringen von fehlerhaften Daten während des Trainingsprozesses (**Data Poisoning**), das gezielte Verfälschen von Eingaben, um bestimmte Reaktionen des Modells hervorzurufen (**Model Evasion**), sowie das Auslesen sensibler Informationen über das Modell selbst oder seiner Trainingsdaten (**Model Extraction**).

Ein weiteres Sicherheitsrisiko sind etwa **Backdoor-Angriffe**. Diese beginnen mit der Manipulation von Trainingsdaten **(Poisoning)**, um später gezielte Fehlentscheidungen herbeizuführen, sobald ein bestimmter Auslöser **(engl. backdoor trigger)** in der Eingabe vorhanden ist. Ohne diesen Auslöser bleibt das Verhalten des Modells jedoch unverändert. Zum Schutz vor solchen Angriffen sollten vortrainierte Modelle nur aus vertrauenswürdigen Quellen bezogen, sicher übertragen und deren Integrität überprüft werden. Dokumentationen der Trainingsdaten und bestehende Schutzmaßnahmen gegen Datenmanipulation sind ebenfalls essenziell.

Darüber hinaus umgehen **Prompt Injection-Angriffe** Sicherheitsvorkehrungen, indem sie bösartige Befehle in Benutzereingaben einschleusen, um die Kontrolle über das System zu erlangen. Schließlich stellen **Inversion- und Model Stealing-Angriffe** eine Gefahr dar, indem sie durch Rückschlüsse auf Trainingsdaten oder durch gezieltes **Reverse Engineering** die sensiblen Daten und die Funktionsweise der KI offenlegen.

Diese vielfältigen Bedrohungen unterstreichen die Notwendigkeit robuster Sicherheitsstrategien, kontinuierlicher Überwachung und der Anwendung bewährter Schutzmaßnahmen, um die Integrität und Verlässlichkeit von KI-basierten Sicherheitslösungen zu gewährleisten.

Bedrohungsszenarien für KI: Risiken und Schwachstellen im Überblick

Gefahren	Beschreibung
Data Poisoning	Hierbei werden die Trainingsdaten des KI-Modells manipuliert, um die Genauigkeit und Verlässlichkeit des Modells zu untergraben. Angreifer könnten bösartige Daten in den Trainingsprozess einspeisen, um das Modell absichtlich zu schädigen oder zu korrumpieren.
Model Evasion	Bei diesen Angriffen wird das KI-Modell so umgangen, dass es Bedrohungen nicht erkennt. Angreifer nutzen hierfür Techniken, um Eingaben so zu gestalten, dass sie unauffällig bleiben, obwohl sie schädlich sind. Diese Angriffe sind oft darauf ausgelegt, bestehende Sicherheitssysteme zu umgehen, indem sie als legitim eingestuft werden.
Model Extraction	Bei diesen Angriffen versuchen Angreifer das KI-Modell zu kopieren oder zu stehlen, indem sie systematisch Eingaben und die entsprechenden Ausgaben des Modells analysieren. Dies kann zu einem Verlust von geistigem Eigentum und sensiblen Informationen führen und ermöglicht es Angreifern, die Funktionsweise des Modells zu verstehen und zu manipulieren.

IoT im Visier: Prof. Markus Miettinen über KI-gestützte Cybersicherheit und die Zukunft der Vernetzung

Prof. Dr.-Ing. Markus Miettinen, Frankfurt University of Applied Sciences, im Gespräch mit Lisa Fröhlich, Unternehmenssprecherin bei Link11

Prof. Miettinen, was sind Ihre Forschungsschwerpunkte?

Ich forsche an Systemen, die Angriffe gegen IoT-Geräte erkennen. IoT-Geräte durchdringen zunehmend unseren Alltag, von Smart Homes über industrielle Prozesse bis hin zu intelligenter Infrastruktur. Viele dieser Geräte weisen jedoch Sicherheitslücken auf, die sie anfällig für Angriffe machen. Wir nutzen KI-Modelle, um das normale Kommunikationsverhalten der Geräte festzustellen und abweichendes Verhalten als potenziellen Angriff zu identifizieren.

Wie hängt Ihre Forschung mit künstlicher Intelligenz (KI) zusammen?

Ein großes Problem bei KI-Modellen ist, dass sie nur richtig funktionieren, wenn sie mit korrekten Daten trainiert werden. Wenn ein Angreifer die Trainingsdaten oder den Trainingsprozess manipuliert, kann das KI-Modell falsche Ausgaben liefern. Deshalb forsche ich an Verfahren, um solche Manipulationen zu erkennen und zu eliminieren.

Wie hat sich die Landschaft der Cyberbedrohungen im Laufe der Zeit entwickelt und welche neuen Herausforderungen sind heute relevant?

Cyberangriffe sind professioneller geworden, mit Kriminellen, die auf Profit aus sind, und staatlichen Akteuren, die Cyberangriffe als Teil ihres Offensivpotenzials nutzen. Eine besondere Herausforderung heute ist die zunehmende Vernetzung im IoT. Viele dieser Geräte haben unzureichende Sicherheitsdesigns und sind anfällig für Angriffe, was die Bedrohungslage verschärft.

Warum ist die Bedeutung von Cybersicherheit in der heutigen digitalen Welt so entscheidend?

Die Cybersicherheit ist entscheidend, da fast alle gesellschaftlichen Prozesse digitalisiert sind – von Verwaltung und Geschäftstransaktionen bis hin zu kulturellen Angeboten und Kommunikation. Die Rolle der Cybersicherheit ist, unsere digitalisierten Prozesse und Systeme gegen Angriffe abzusichern und die Resilienz KI-gestützter Systeme gegen Manipulationen zu gewährleisten.

Wie setzen Cyberkriminelle KI-Technologien ein, um ihre Angriffe effektiver zu gestalten?

Cyberkriminelle nutzen KI, um ihre Angriffe zu optimieren. Beispielsweise können KI-Modelle Teile von Schadsoftware generieren und Spam-E-Mails verfassen, die durch ihre hohe Qualität Nutzer leichter täuschen. Sogar bei kleineren Sprachen wie Finnisch – meiner Muttersprache – kann man nicht mehr leicht erkennen, ob eine Mail echt ist oder ein Betrugsversuch.

Welche Rolle spielt KI in der Prävention von Cyberangriffen?

Wir können mithilfe von KI lernen, wie sich IoT-Geräte normalerweise verhalten und kommunizieren. Wenn ein Gerät angegriffen wird, erkennen wir das anhand seines abweichenden Kommunikationsverhaltens. Das System lernt eigenständig, was normal und was nicht normal ist, und arbeitet autonom.

Wird es eine stärkere Regulierung geben?

Es wird sicherlich Bestrebungen geben, den Einsatz von KI zu reglementieren, um unlautere Praktiken zu unterbinden und ethische Fragen zu berücksichtigen. Die Sicherheitsforschung ist den Angreifern dicht auf den Fersen und betreibt auch eigenständige Forschung, um ihnen im besten Fall einen Schritt voraus zu sein.

Vielen Dank für die spannenden Einblicke.

So setzen Kriminelle KI heute schon ein

Wenn die IT Ihres Unternehmens bisher noch nicht Ziel einer groß angelegten Attacke durch Kriminelle geworden ist, haben Sie schlichtweg Glück gehabt. Ein geflügeltes Wort unter Experten besagt, dass es nur zwei Arten von Unternehmen gibt: Es gibt solche, die einen großen Hackerangriff bereits hinter sich haben, und diejenigen, die nicht wissen, dass sie bereits angegriffen wurden.

Kriminelle und Hacker verfolgen die Entwicklung von KI genauso aufmerksam wie Unternehmen. Und genau wie diese machen sie sich diese Technologie zunutze. Firmen dürfen sich hier nicht von der trügerischen Idee leiten lassen, dass KI zu komplex oder zu teuer für Kriminelle ist. Denn inzwischen bieten Cloud-Anbieter wie Google, Amazon oder Microsoft bereits Schnittstellen zu Rechensystemen für das maschinelle Lernen an. Außerdem darf nicht vergessen werden, dass hinter Angriffen aus dem Internet auch Konkurrenten, Nachrichtendienste und Staaten stehen können. In einem solchen Fall spielt Geld eine untergeordnete Rolle.

Es gibt eine ganze Reihe von Szenarien für den Einsatz von KI durch Kriminelle, z. B.:

- **Biometrie:** Eine Vielzahl beeindruckender Beispiele zeigt, dass mittels KI täuschend echt wirkende Personen und Gesichter virtuell erzeugt werden können. Als Grundlage für solche „Deep Fakes" können die Systeme auch Alltagsaufnahmen der Betroffenen nutzen. Auf diese Weise lassen sich biometrische Sicherheitssysteme überwinden, die auf Gesichtserkennung basieren.

- **Spracherkennung und Sprachsynthese:** Ähnlich ausgeklügelt sind Anwendungen mit der Fähigkeit, Sprache künstlich zu generieren. Google beispielsweise hat einen Sprachcomputer entwickelt, der auf Wunsch telefonisch Termine abwickelt. Die Anrufer bemerken dabei nicht, dass sie mit einem Computersystem telefonieren. Mittels „Natural Language Generation" sind Angreifer in der Lage, Stimme und Tonfall einer vertrauenswürdigen Person zu imitieren und so an womöglich heikle Informationen zu gelangen. Umgekehrt können mittels Spracherkennung und Sprachanalyse Daten aus Telefonmitschnitten oder anderen Informationsquellen gewonnen werden, die Details über Sicherheitssysteme verraten oder Hinweise auf anstehende Transaktionen liefern, die dann abgefangen werden.

- **Maschinelles Lernen:** Maschinelles Lernen wird von Angreifern dazu genutzt, aus großen Datenmengen eines Unternehmens das Verhalten der Opfer besser zu analysieren. Das Ziel ist es, erfolgversprechende Phishing-Attacken zu entwickeln. Machine Learning lässt sich aber auch zur Analyse von Schwachstellen der eingesetzten Sicherheitssysteme nutzen. Maschinelles Lernen erlaubt die Programmierung von Malware, die kaum oder nur sehr bedingt zurückverfolgt werden kann. Ein Angriffsszenario wäre etwa „selbstlernende" Trojaner.

- **(Predictive) Analytics:** KI-Systeme werden vielfach dazu genutzt, Vorhersagen zu treffen. Auf Basis bereits gewonnener Daten aus erfolgreichen und abgewehrten Attacken können intelligente Systeme den Angreifer dabei unterstützen, eine Strategie für eine erfolgversprechende Attacke zu entwickeln. Auch kann ein KI-System automatisiert Schwachstellen in IT-Systemen identifizieren.

- **Generative KI:** Kriminelle könnten Generative KI wie ChatGPT und andere Large Language Models (LLM) nutzen, um sehr überzeugende Phishing-E-Mails zu erstellen. Zusätzlich können die Modelle bei der Entwicklung und Anpassung von Schadsoftware unterstützen.

Folgende Bedrohungen gehören aktuell zu den gravierendsten

Automatisierte Phishing-Angriffe:

Mithilfe von KI können Angreifer hochpersonalisierte Phishing-Nachrichten erstellen, die auf soziale Medien und Kommunikationsmuster der Zielpersonen zugeschnitten sind.

KI-generierte Malware:

KI verändert die Landschaft der Malware-Entwicklung. KI-generierte Malware kann sich an die Umgebung anpassen und ihr Verhalten ändern, wodurch traditionelle Erkennungsmethoden ausgehebelt werden.

Deepfake-Technologie:

KI erstellt täuschend echt gefälschte Bilder, Videos und Audioaufnahmen, die für Social Engineering und die Manipulation von Informationen verwendet werden. Ein gefälschter Videoanruf eines CEOs könnte beispielsweise einen Mitarbeitenden veranlassen, Geld zu überweisen oder sensible Informationen preiszugeben.

KI-gesteuerte Aufklärung:

Angreifer können KI nutzen, um Schwachstellen und potenzielle Ziele innerhalb eines Netzwerks schneller und genauer zu identifizieren. Diese automatisierte Aufklärung ermöglicht gezielte Angriffe auf spezifische Systeme oder Personen, die wertvolle Informationen oder Zugang bieten.

Autonome Waffen und DDoS-Angriffe:

KI-gesteuerte autonome Systeme können verwendet werden, um Botnetze zu erstellen, die DDoS-Angriffe durchführen können. Diese Systeme identifizieren selbstständig verwundbare Geräte und nutzen sie, um Netzwerke zu überlasten und Dienste unzugänglich zu machen.

KI-generierter Code als Sicherheitsrisiko:

KI kann verwendet werden, um automatisch Code zu erstellen oder zu optimieren. Dies birgt die Gefahr, dass fehlerhafter oder bösartiger Code erstellt wird, der Sicherheitslücken oder Schwachstellen in Softwareanwendungen oder Systemen einführt.

Datenleck durch kompromittierte KI-Modelle:

Kompromittierte KI-Modelle können sensible Daten abfangen oder falsche Ergebnisse liefern, was Datenschutzverletzungen zur Folge haben kann.

Vor diesen überwältigenden technischen Möglichkeiten und der daraus entstehenden konkreten Bedrohung durch Cyberkrimielle für die digitalen Geschäftsprozesse sollten Unternehmen nicht zögern, ebenfalls auf KI zur Abwehr von Gefahren zu setzen.

Angreifer oder Verteidiger? Prof. Stjepan Picek über die Zukunft der KI in der IT-Sicherheit

Dr. Stjepan Picek, Associate Professor, Radboud University,
im Gespräch mit Lisa Fröhlich, Unternehmenssprecherin bei Link11

Könnten Sie bitte kurz über Ihre Forschung im Bereich der Cybersicherheit und der künstlichen Intelligenz (KI) erzählen?

Meine Forschung befasst sich sowohl mit KI für Sicherheit als auch mit der Sicherheit von KI. Als Leiter der AISyLab-Gruppe erforschen wir Ansätze wie Deep-Learning-basierte Side-Channel-Analyse, KI-gestützte Fehlerinjektion und Backdoor-Angriffe auf neuronale Netze. Unsere Arbeit umfasst zentrale und dezentrale Lernparadigmen wie Federated Learning und Split Learning.

Warum gibt es in der Öffentlichkeit so wenig Differenzierung, wenn es um KI geht?

KI ist ein riesiges Gebiet. Es gibt ein großes Interesse am Deep Learning, einem Teilbereich des maschinellen Lernens. Die meisten Nachrichten, die ein allgemeines Publikum erreichen, machen es schwierig, den gesamten Bereich der KI zu erfassen.

Wie beurteilen Sie die aktuellen Entwicklungen im Bereich der KI und ihre Rolle in der Cybersicherheit?

KI wird zunehmend sowohl für Angriffe als auch zur Verteidigung eingesetzt. Entwicklungen im Deep Learning ermöglichen die Verarbeitung riesiger Datenmengen und genauere Vorhersagen. Ich glaube, dass wir in den nächsten Jahren die meisten Entwicklungen hier sehen werden: mehr Daten nutzen und genauere Ergebnisse erzielen.

Welche Herausforderungen sehen Sie?

Da wir ständig neue KI-Technologien entwickeln, ist es natürlich auch realistisch, dass es auch Angriffe auf diese neuen KI-Techniken geben wird.

Welchen IT-Sicherheitsbedrohungen ist KI ausgesetzt?

KI ist wie andere Systeme auch verschiedenen IT-Sicherheitsbedrohungen ausgesetzt und lässt sich anhand der CIA-Trias (Vertraulichkeit, Integrität, Verfügbarkeit) klassifizieren. Ein wesentlicher Unterschied besteht darin, dass KI aufgrund ihres aktuellen Hypes verstärkt in den Fokus der Öffentlichkeit gerückt ist, während andere Bedrohungen oft nur Spezialisten betrachten. Dennoch ist KI nicht immun gegen Angriffe und muss entsprechend abgesichert werden.

Wie sehen Sie die Entwicklung der KI im Bereich der Cybersicherheit in der Zukunft?

Es ist schwer vorherzusagen, da sich die KI so schnell entwickelt. Wir werden mehr Angriffe auf neue KI-Systeme sehen und mehr Ansätze für eine vollautomatische Verteidigung. Generative KI und große Sprachmodelle werden die Forschungsgemeinschaft in den nächsten Jahren beschäftigen.

Wer hat im Wettlauf zwischen Angreifern und Verteidigern die Nase vorn und warum?

Ich würde sagen, die Angreifer. Viele KI-Systeme sind leicht anzugreifen, während Verteidigung schwierig und teuer ist. Für jede gemeldete böswillige Nutzung von KI gibt es vermutlich viele unbekannte, was eine angemessene Bewertung erschwert. Außerdem sagt eine Verteidigung gegen einen Angriff nichts über die Sicherheit von KI-Systemen gegen verschiedene Angriffe aus.

Welche Unterstützung kann KI gegen Cyberangriffe bieten?

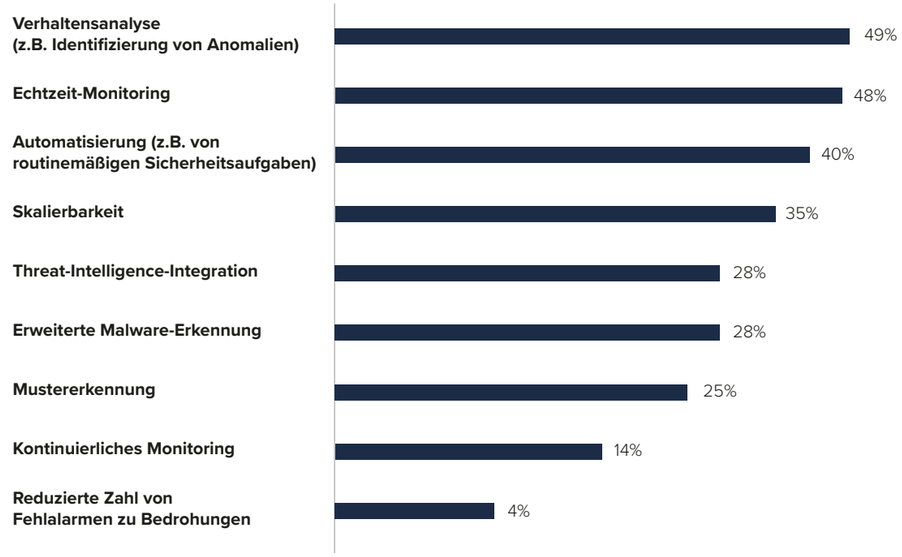
KI ist bereits weit verbreitet und wird entweder in Verteidigungsmechanismen wie etwa zur Erkennung von Malware und Spam oder als Intrusion Detection eingesetzt. Darüber hinaus können Sicherheitsexperten mithilfe von KI die Rolle des Angreifers übernehmen, um die Sicherheit von Systemen zu testen.

Vielen Dank für das spannende Gespräch.

Möglich ist auch, dass leistungsfähigere KI-Modelle bei der Abwehr von Angriffen helfen, indem sie eine schnellere Erkennung sowie Verhinderung von Angriffen ermöglichen und dadurch den Bedarf an menschlichen Experten zumindest verringern.

Wo genau KI-Modelle bei der Abwehr von Angriffen helfen können, zeigen die Ergebnisse des aktuellen Capterra Sicherheitsreports[5]:

Wie KI die Bedrohungserkennung und -reaktion im Vergleich zu herkömmlichen Cybersicherheitsmethoden verbessert



Quelle: Capterra Sicherheitsreport
Frage: Wie verbessert KI die Bedrohungserkennung und -reaktion im Vergleich zu herkömmlichen Cybersicherheitsmethoden?
Wählen Sie alles Zutreffende aus. n: 670
Hinweis: Da es mehrere Antwortmöglichkeiten gab, kann die Gesamtsumme 100% übersteigen

„Die Zukunft der Cybersicherheit liegt in der intelligenten Automatisierung. KI-gestützte Systeme bieten nicht nur rund um die Uhr Schutz, sondern lernen auch eigenständig, Bedrohungen in Echtzeit zu erkennen und abzuwehren.“

Karsten Desler, CTO, Link11

15

Cyber-Resilienz gewinnt an Bedeutung

In einer zunehmend digitalisierten Geschäftswelt führen Cyber-Attacken häufig unmittelbar zu Betriebsunterbrechungen. Der deutschen Wirtschaft entsteht dadurch ein Schaden von rund 150 Milliarden Euro pro Jahr, stellt der Branchenverband Bitkom fest.[6] Der Stärkung der Widerstandskraft der IT-Infrastrukturen kommt daher eine immer größere Priorität zu.

Zu diesem Zweck werden Konzepte erstellt und Maßnahmen definiert, die die Weiterführung und Wiederaufnahme der Geschäftstätigkeiten während bzw. nach einer Cyber-Attacke gewährleisten. Ziel der Cyber-Resilienz ist es, gut vorbereitet und schnell auf Sicherheitsverletzungen zu reagieren sowie Sicherheitsvorfällen entgegenzuwirken und gleichzeitig die Steuerbarkeit des Geschäftes zu erhalten.

Die Widerstandsfähigkeit gegen Angriffe von außen steht und fällt dabei mit der gelebten Sicherheitskultur im Unternehmen sowie mit den eingesetzten Schutzlösungen. Beides erfordert permanente Anpassungen der Sicherheitskonzepte und der Steuerungslösungen. Ein statischer Ansatz, bei dem Prozesse und Schutzlösungen einmalig definiert werden, reicht angesichts der hochdynamischen Sicherheitsrisiken nicht mehr aus.

Wer clever in neue Technologien investiert, kann den Grad der Widerstandskraft überproportional steigern. Nach Ergebnissen des State of Cybersecurity Resilience 2023 von Accenture konnten diejenigen Unternehmen, die Cybersicherheitsmaßnahmen einbetten, eine fast sechsmal effektivere digitale Transformation erleben, als diejenigen, die es nicht tun. Damit stärken sie nicht nur ihre Cyber-Resilienz, sondern haben auch eine 18 % höhere Wahrscheinlichkeit ihr Umsatzwachstum zu steigern.[7] Als Zukunftstechnologie gilt dabei KI und maschinelles Lernen.

KI ist bei der Angriffsabwehr überlegen

KI ist eine neutrale Technologie, die in ihrem Kern weder gut noch böse ist. In den Händen von Kriminellen stellt sie eine ernstzunehmende Bedrohung dar, doch im Umkehrschluss kann sie auch zur Abwehr von Gefahren eingesetzt werden. Der Versuch, bedrohliche KI mit menschlichem Einsatz zu bekämpfen ist aufgrund der technischen Größenunterschiede zum Scheitern verurteilt. In der IT-Sicherheit profitieren Security-Lösungen von KI-Komponenten deutlich, da zahlreiche Schwachstellen traditioneller Lösungen überwunden werden.

1. KI ist schneller

Durch die voranschreitende Digitalisierung stehen Unternehmen heute vor der Herausforderung, eine wachsende Anzahl von Anwendungen, externen Cloud-Anbietern und Geräten zu überwachen und abzusichern. In den kommenden Jahren wird die Zahl der zu überwachenden Systeme durch das Internet-of-Things (IoT) stetig steigen. Intelligente Sensoren übernehmen die Steuerung in der Haustechnik, dienen der Übermittlung von Informationen in der Supply Chain oder erlauben neue Geschäftsmodelle. Ein Abrechnungsmodell, das sich beispielsweise an der konkreten Nutzung von Geräten (Pay-per-Use) orientiert, ist ohne Sensoren nicht denkbar.

Im Umkehrschluss bedeutet dies, dass die von einer Organisation verarbeiteten Datenmengen weiter anwachsen. Gleichzeitig wird die Zahl der Schnittstellen und Kommunikationskanäle innerhalb des Unternehmens steigen. Bekanntlich ist aber jeder zusätzlich in die IT-Landschaft eingebettete Kanal potenziell auch ein Einfallstor für politisch motivierte Angreifer. Automatisierte KI-Systeme, die etwa den Datenverkehr von IoT-Sensoren überwachen, sind sehr viel schneller in der Lage, Anomalien in deren Verhalten zu entdecken. Sie schlagen schneller Alarm oder leiten Gegenmaßnahmen ein, als es der Mensch je könnte.

In großen und möglicherweise weltweit tätigen Unternehmen loggen sich rund um die Uhr Mitarbeiter auf interne Systeme ein. Augenscheinlich zu viele, um diese manuell zu überprüfen. KI kann in diesem Zusammenhang etwa Besonderheiten erkennen, um auf Basis von „Predictive Analytics" und „Mustererkennung" angemessen zu reagieren. Loggt sich ein Mitarbeiter üblicherweise zu festen Arbeitszeiten aus einer definierten Region auf einem System der Firma ein, so ist eine erfolgreiche Anmeldung mitten in der Nacht, aus einer anderen Zeitzone oder einer völlig anderen Region zumindest verdächtig. Ein solches Vorkommnis manuell zu entdecken, gleicht der sprichwörtlichen Suche nach der Stecknadel in einem Heuhaufen.

2. KI übersieht nichts

Groß angelegte Attacken erfordern Vorbereitung und zeitlichen Vorlauf. Während dieser Zeit versuchen die Angreifer, möglichst viele Systeme bzw. Angriffsvektoren in Stellung zu bringen. Dabei hinterlassen sie durchaus Spuren auf gekaperten Systemen. Durch Mustererkennung und Analysen können KI-basierte Verteidigungssysteme bereits kleinere Abweichungen erkennen. Administratoren und Sicherheitsverantwortliche erhalten rechtzeitig einen Alarm, wenn das System ein Vorkommnis als potenzielle Vorbereitung eines Angriffs einstuft.

Bei einer drohenden DDoS-Attacke ist schnelles Handeln notwendig. Aber wann handelt es sich noch um ein organisches Wachstum des Netzwerkverkehrs? Wann zeichnet sich eine Attacke ab? Auch in diesem Zusammenhang spielt KI ihre Geschwindigkeit aus. Binnen Sekunden werden regelmäßige Analysen über Wachstum, Datenquellen und Charakteristika einer DDoS-Attacke angestellt. Die Software ist hier selbst erfahrenen Mitarbeitern überlegen, da sie schneller in der Verarbeitung mehrerer Datenquellen, der Analyse und der Ergreifung von Gegenmaßnahmen ist.

Konventionelle Erkennungssysteme[8]
Software (SW) arbeitet mit starren Modellen
SW erzeugt Entscheidungen basieren auf einem transparenten Regelsystem
SW ist nicht lernfähig
SW setzt Signaturen und Korrelationen gegen verschiedene Arten von Daten ein

Erkennungssysteme mit lernender / KI-Komponente
SW arbeitet mit adaptiven Modellen
SW erzeugt Entscheidungen auf Basis einer graduellen Bewertung
SW lernt laufend hinzu
SW lernt komplexe Muster aus einer großen Mengen an Daten

3. KI ist besser als jeder Patch

Die Abwehr krimineller Attacken erinnert häufig an ein Katz-und-Maus-Spiel. Typischerweise unterscheiden Sicherheitslösungen zwischen „guten" und „bösen" Anfragen oder Programmcode. Werden neue Sicherheitslücken entdeckt, besteht die Reaktion in der Regel in manuellen Anpassungen. Es wird ein Patch eingespielt, die Regeln in einer Firewall geändert und Signaturen von Schadprogrammen aktualisiert.

Die Sicherheitssysteme werden so auf den aktuellsten Stand gebracht. Die Entwicklung von Patches, Updates und Regeln benötigt aber Zeit und bezieht sich dabei auf bereits aufgetretene Vorfälle oder entdeckte Sicherheitslücken. In der Zwischenzeit haben die Kriminellen bereits weitergearbeitet. Sie verwenden andere Netzwerke für Attacken, die noch nicht in der Firewall erfasst sind, nutzen neue Sicherheitslücken aus oder setzen sogenannte „polymorphe" Schädlinge ein. Deren Code verändert sich ständig, um Erkennungsprogrammen die Aufgabe zu erschweren und die Tarnung des Schadprogramms zu verbessern.

Analysesysteme auf Basis von KI sorgen hier für Chancengleichheit gegenüber den Angreifern. Selbstlernende KI-Systeme, die sich während des Einsatzes immer weiter verbessern und somit automatisiert eigene Entscheidungen treffen, stellen ein mächtiges Werkzeug dar. Bei einer Strategie des „Whitelistings" wird jeder Netzwerkverkehr zunächst als schädlich klassifiziert, bis das Gegenteil bewiesen ist, also beispielsweise Paketinhalte analysiert wurden. KI beschleunigt die Analysen und trifft in einem lernenden System die Entscheidung, welche Datenströme passieren dürfen.

4. KI überwindet Personalmangel

In allen Branchen zeigen sich in den vergangenen Jahren drei parallele Entwicklungen in der IT-Sicherheit, deren Kombination Anlass zur Besorgnis bietet. Die Zahl der Attacken gegen Unternehmen ist gewachsen. Phishing, erfolgreiche Angriffe mit Ransomware, DDoS-Angriffe: Die Bedrohungslage hat sich verschärft. Wie bereits dargestellt, hat dies auch damit zu tun, dass die Zahl potenzieller Einfallstore und Plattformen wächst.

Gleichzeitig wurden von der Politik neue Regularien verabschiedet, die unmittelbaren Einfluss auf die IT-Sicherheit haben. Die DSGVO oder die NIS2 beschreiben im Kern sehr genau, was

Unternehmen und Behörden im Rahmen „technisch-organisatorischer" Maßnahmen tun müssen, um Daten vor unbefugten Zugriffen, Manipulation und Diebstahl zu schützen. Somit wachsen die Anforderungen an die IT-Sicherheit auch hier.

Umsetzung der Compliance und Reaktion auf die gestiegene Bedrohung erfordern somit mehr Fachpersonal. Der Bedarf an IT-Sicherheitsexperten ist sehr groß. Jedoch gelingt es vielen Unternehmen, insbesondere kleineren und mittelgroßen, gar nicht, diese Fachkräfte zu gewinnen. Es herrscht ein ausgesprochener Mangel an Fachkräften in diesem Segment.[9]

Das hat erwartungsgemäß Konsequenzen: Das vorhandene Personal ist überlastet und kann sich somit wichtigen Themen nur begrenzt widmen. So verwundert es kaum, dass es nach wie vor Organisationen gibt, in denen veraltete Software und Betriebssysteme im Einsatz sind. Doch genau damit machen sich die Firmen wiederum leichter angreifbar.

Der Einsatz von KI in IT-Sicherheitslösungen spart personelle Ressourcen, weil die Maschinen viele Entscheidungen selbstständig (auf Basis von Regeln) treffen, bei der Analyse schneller als der Mensch agieren und deutlich mehr Daten verarbeiten. In der Analyse von Protokolldateien übersehen Algorithmen keine Anomalien, während der Mensch möglicherweise schon müde geworden ist oder nicht mehr so genau hinsieht, weil er beispielsweise in den Feierabend möchte. KI eliminiert also die Fehlerquelle Mensch.

Warum KI-basierte Lösungen unverzichtbar sind

Aufgrund des hohen Risikopotenzials ist ein umfassender Schutz für alle Komponenten der IT-Infrastruktur essenziell. Dieser Schutz erfordert eine lückenlose Überwachung rund um die Uhr, die jedoch kaum allein durch menschliche Mitarbeiter realisierbar ist. Die größten Herausforderungen sind begrenzte Personalkapazitäten und der Mangel an Zeit, um die zunehmend dynamischen und komplexen Angriffsstrukturen zu erkennen. Zudem hat das Datenvolumen, mit dem Angriffe durchgeführt werden, ein Ausmaß erreicht, das menschliche Kontrolle überfordert. Um diesem Problem zu begegnen, müssen Unternehmen auf intelligente IT-Sicherheitslösungen setzen.

Genau hier zeigen KI-basierte IT-Sicherheitslösungen ihre Stärken. Sie sind nicht nur rund um die Uhr einsatzbereit, sondern können auch Auffälligkeiten in großen Datenmengen nahezu in Echtzeit identifizieren. Cyberangriffe sind letztlich Normabweichungen in IT-Netzwerken, die mithilfe künstlicher Intelligenz erkannt werden können. Im Gegensatz zu klassischen Ansätzen benötigen einige Tools für maschinelles Lernen und Deep Learning keine vordefinierten Regeln oder Informationen aus früheren Angriffen. Sie lernen eigenständig, kritische Situationen zu erkennen. Als Datenbasis dienen je nach Lösung beispielsweise Log-Dateien oder Echtzeitanalysen des Netzwerkverkehrs.

Trotz der Herausforderungen durch Personalmangel, eingeschränkte Budgets und Zeitdruck ermöglichen Fortschritte beim Einsatz von KI in der Cybersicherheit und in Automatisierungstechnologien den Unternehmen und Regierungsorganisationen transformative operative Verbesserungen. Diese Technologien beschleunigen die Erkennung und Reaktion auf Cybervorfälle erheblich, reduzieren deren Kosten und Auswirkungen und steigern die Cyber-Resilienz.

> *„Dank der autonomen Lernfähigkeit unserer KI-Modelle können wir kontinuierlich auf neue Bedrohungen reagieren und unsere Sicherheitsmaßnahmen ständig verbessern."*
>
> **Ziv Grinberg, Vice President Product, Link11**

Laut dem IBM Institute for Business Value sparen Organisationen, die auf diese Technologien setzen, im Durchschnitt 3 Millionen Dollar bei Datenverletzungen und verkürzen die Zeit zur Bewältigung von Cybervorfällen um bis zu 99 Tage. Mit einer 40 % höheren Rendite auf Sicherheitsinvestitionen und einem signifikanten Geschäftswachstum erhöhen KI und Automatisierung nicht nur die Cyber-Resilienz, sondern auch den Unternehmenswert.[10]

Unternehmen werden in der Zukunft nicht umhinkommen, in der IT-Sicherheit auf KI zu setzen, wenn sie den Fachkräftemangel überwinden und sich gegen hochgradig spezialisierte Kriminelle wehren wollen.

Investitionen in Cybersicherheit sind dabei von entscheidender Bedeutung, da integrierte Cyber-Technologie-Plattformen und generative künstliche Intelligenz (GenAI) zunehmend an Bedeutung gewinnen. Laut dem Digital Trust Inisghts 2024 von PwC wollen in Zukunft 84 % der deutschen Unternehmen ihr Budget für Cybersecurity erhöhen. Um Risiken zu mindern und finanzielle Schäden zu begrenzen, setzen immer mehr Unternehmen auf fortschrittliche Technologien. In Deutschland nutzen bereits 49 % der Unternehmen integrierte Cyber-Technologie-Plattformen (global 44 %) und weitere 43 % (global 39 %) planen den Umstieg in den nächsten zwei Jahren. Die Nutzung von KI unterstützt die Sicherheitsexperten in ihrem Alltag und hilft ihnen dabei, sich auf besonders dringende und zeitkritische Aufgaben zu fokussieren, ohne Abstriche bei der Sicherheit insgesamt machen zu müssen. In Deutschland planen in den nächsten zwölf Monaten 75 % der Befragten, GenAI-Tools für die Cyberabwehr einzusetzen (global 69 %).[11] Diese Zahlen verdeutlichen die Notwendigkeit, in moderne Cybersicherheitslösungen zu investieren, um den wachsenden Bedrohungen effektiv begegnen zu können.

Wie Link11 Sie dank KI besser schützt

Link11 hat sich bereits früh mit der Frage auseinandergesetzt, wie KI Security-Lösungen noch besser und Unternehmen damit noch resilienter gegen Cyberattacke machen kann. So werden maschinelles Lernen, Mustererkennung und Predictive Analytics in immer mehr Services zu einem integralen Bestandteil.

Bot-Management: Wie KI sind Bots an sich nicht gut oder böse. Die von diesen automatisierten Programmen verursachten Anfragen machen in vielen Unternehmen inzwischen einen Großteil des Traffics aus. Suchmaschinen indizieren mit Bots die Inhalte der Seiten. Vergleichsportale verwenden Bots dazu, aktuelle Preisinformationen zu gewinnen. Bots können aber auch betrügerisch und kriminell eingesetzt werden. Beispielsweise wenn sie Werbeformate in betrügerischer Absicht abrufen oder die Bedienbarkeit von Systemen einschränken.

Mit unserem Bot-Management-Service bieten wir die Möglichkeit, den von Bots verursachten Traffic auf Ihren Systemen zu klassifizieren und zu steuern. KI hilft dem System dabei, bisher unbekannte Bots zu erkennen und zu beurteilen. So hilft die künstliche Intelligenz Ihnen beim Einsatz des Service dabei, echten Nutzern ein besseres Erlebnis beim Besuch ihrer Seiten zu verschaffen, weil auf den Traffic durch unerwünschte Bots reagiert wird.

DDoS-Schutz: Nicht nur die Link11 Cyber-Resilienz-Netzwerkanalysen zeigen, dass DDoS-Attacken immer mehr zunehmen

> *„Unsere Lösungen vereinen technische Raffinesse mit künstlicher Intelligenz, um maßgeschneiderte Antworten auf die Sicherheitsanforderungen unserer Kunden zu liefern."*
>
> **Karsten Desler, CTO, Link11**

und komplexer werden. Die Schutzlösung von Link11 kombiniert den Einsatz der Cloud mit der Nutzung von künstlicher Intelligenz. Dank der Cloud ist der Schutz gut skalierbar und schnell einsatzbereit. Und mit „Always On" handelt das System bei einem Angriff rund um die Uhr. Im Falle eines Angriffs spielt Zeit eine wichtige Rolle. Die KI-Lösung lernt in Echtzeit aus allen von Link11 abgewehrten Attacken. Das System analysiert jeden Angriff und überträgt die Ergebnisse auf andere Gefährdungsmuster. Anders als bei jedem manuellen Ansatz ist das System somit auf neue Angriffsvektoren vorbereitet. Davon profitieren alle Kunden und Unternehmen, da der Abwehrschild permanent besser wird. Er sieht ähnliche Vorfälle voraus und kann somit immer schneller im Gefährdungsfall reagieren. Diese automatisierte Sicherheit spart nicht nur Zeit und Geld, sondern macht es noch einfacher für Sie, sich auf das Wesentliche zu konzentrieren.

KI-Systeme entbinden nicht von Verantwortung

Bei allem Potenzial: Ein Allheilmittel in Sachen IT-Sicherheit und Cyber-Resilienz stellt künstliche Intelligenz – zumindest bis auf Weiteres – nicht dar. Zwar ist KI nach einem intensiven Training stark in der Erkennung von Gefahren wie Malware oder DDoS-Attacken und zudem in einem direkten Vergleich genauer als die menschliche Angriffserkennung. Da die Bedrohungslage in der digitalen Welt aber hochdynamisch ist, wird es weiterhin dem Menschen obliegen, die Angriffe einzuordnen und Maßnahmen daraus abzuleiten. Das wichtigste Assistenzmittel dafür wird künstliche Intelligenz sein. Sie wird den Menschen immer stärker in der Entscheidungsfindung entlasten, ihn jedoch nicht gänzlich ersetzen.

Wollen Sie mehr darüber erfahren, wie der Einsatz von künstlicher Intelligenz Ihre IT besser schützt und Ihnen dabei hilft, Sicherheitsstrategie umzusetzen? Dann kontaktieren Sie noch heute einen unserer Spezialisten.

Michael Scheffler
Vice President Sales

+49 69 58004926-306
m.scheffler@link11.com

Nachweise

1 https://www.mckinsey.de/news/presse/genai-ist-ein-hilfsmittel-um-die-produktivitaet-zu-steigern-und-das-globale-wirtschaftswachstum-anzukurbeln
2 https://www.pwc.de/de/cyber-security/ceosurvey.html
3 https://www.ibm.com/thought-leadership/institute-business-value/report/ai-security-automation
4 https://www.pwc.de/de/cyber-security/digital-trust-insights.html
5 https://www.capterra.com.de/blog/4532/ki-cybersecurity-studie
6 https://www.bitkom.org/Presse/Presseinformation/Organisierte-Kriminalitaet-greift-verstaerkt-deutsche-Wirtschaft-an
7 https://www.accenture.com/us-en/insights/security/state-cybersecurity
8 J. Müller-Quade: Künstliche Intelligenz und IT-Sicherheit. Bestandsaufnahme und Lösungsansätze, April 2019
9 https://www.bitkom.org/Presse/Presseinformation/Rekord-Fachkraeftemangel-Deutschland-IT-Jobs-unbesetzt
10 https://www.ibm.com/thought-leadership/institute-business-value/report/ai-security-automation
11 https://www.pwc.de/de/cyber-security/digital-trust-insights.html

Hauptsitz

Link11
Lindleystr. 12
60314 Frankfurt