Künstliche Intelligenz für Effektive Cybersicherheit

Whitepaper

Erleben, was verbindet.

in Kooperation mit

Akamai

INHALT

ZUSAMMENFASSUNG

Wie jede Technologie, kann auch Künstliche Intelligenz (KI) zum Guten wie zum Bösen verwendet werden. Während die Vorteile von KI für die Gesellschaft vielfältig und unumstritten sind, gibt es auch ernstzunehmende Risikofaktoren. So verwenden Cyberkriminelle jetzt schon KI-Tools, um Cyberangriffe zu entwickeln und auszuführen. Um dieser Bedrohung entgegenzusetzen, brauchen wir effektive Verteidigungsmechanismen und -dienste, die unsere Cybersicherheit gewährleisten.

Die Deutsche Telekom und unser Partner Akamai unterstützen unsere Kunden dabei, effektive KI-Modelle zu entwickeln und kriminellen Akteuren einen Schritt voraus zu sein. Unser Whitepaper zeigt, dass KI-gestützte Cybersicherheit mittlerweile unerlässlich ist, und beantwortet Fragen nach den wichtigsten Voraussetzungen, Herausforderungen und Faktoren erfolgreicher KI-Modelle. Wir geben Einblick in Akamais besondere Expertise, außerordentlich effektive KI-Modelle am Markt zu entwickeln, und stellen unser gemeinsames Angebot an KI-gestützten Lösungen zur Cybersicherheit vor. Unsere Kunden können damit sorgenfrei ihrem Tagesgeschäft nachgehen, ohne einem Cyberangriff zum Opfer zu fallen.

1. EINLEITUNG

Künstliche Intelligenz (KI) hat sich in den letzten Jahren zunehmend verbreitet und leistet mittlerweile einen wertvollen Beitrag zum Fortschritt der Gesellschaft. Menschliches Denken und Lernen auf den Computer zu übertragen und ihn damit zu befähigen, Probleme eigenständig zu lösen, bietet eine Vielzahl von Möglichkeiten, die immer breiter eingesetzt werden. Zum Beispiel erregen zurzeit die texterstellenden KIs ChatGPT, Bard und Pi viel Aufsehen. Diese Sprachsysteme produzieren automatisierte Texte mit bemerkenswerter Qualität, die sich von menschengeschriebenen Texten kaum unterscheidet. Weitere Einsatzbeispiele finden sich im Gesundheitswesen, beim autonomen Fahren oder beim Online-Shopping.

KI verändert die Art und Weise, wie wir mit Maschinen interagieren und wie wir Informationen sammeln und verarbeiten. Innovativste KI-Modelle können Prozesse und Aufgaben automatisieren, Produktivität und betriebliche Effizienz steigern und Geschäftsentscheidungen durch die fortlaufende Verarbeitung von Echtzeitdaten verbessern. KI kann uns dabei helfen, komplexe Probleme zu lösen, die menschliche Kapazität übersteigen, und neue Möglichkeiten für die Zusammenarbeit zwischen Mensch und Maschine schaffen.

Die Liste der Chancen, die sich durch den sinnstiftenden Einsatz von KI bietet ist lang und deren Vorteile unbestritten. Allerdings sind mit der Verbreitung von KI auch Risiken verbunden, welchen sich die Gesellschaft insgesamt und insbesondere auch Unternehmen stellen müssen. Neben potentiellen Jobverlusten und den Gefahren, die KI-basierende Fake News aufbringen können, ist der Einsatz von KI zur Durchführung von Cyberangriffen ein ernstzunehmendes Risiko.

Gefahr ruinöser Cyberangriffe

Cyberkriminelle nutzen zunehmend KI-Technologien, um ihre Angriffe effektiver zu gestalten und bei Unternehmen unsäglichen Schaden anzurichten. Hierbei werden beispielsweise Angriffe auf Schwachstellen durch maschinelles Lernen optimiert oder Social-Engineering-Angriffe automatisiert. Dies ist ein ernstzunehmendes Problem für die IT-Sicherheit, da KI-gestützte Angriffe schwer zu erkennen und zu bekämpfen sein können.

In der Schlacht um die Cybersicherheit haben Angreifer mit ihrer KI-gestützten Schadsoftware klare Vorteile, da diese ihr Verhalten automatisch und kontinuierlich anpassen kann. Die Malware kann die Schutzmaßnahmen eines Unternehmens zur Früherkennung von Angriffen umgehen, da sie mittels KI lernen kann, in einer Umgebung unauffällig zu bleiben. Sie imitiert menschliches Verhalten und kann sich somit immer besser in die bestehende Infrastruktur des unter Beschuss stehenden Unternehmens einfügen. Ein Beispiel dafür ist das "DeepLocker"-Projekt von IBM, das als eine Art "Tarnkappenbomber" beschrieben wurde, da es in der Lage ist, sein Ziel sehr präzise zu identifizieren und nur dann anzugreifen, wenn es das richtige Ziel ist. Außerdem wird KI-gestützte Malware zunehmend modularer und kann damit fallweise entscheiden, welche der vorhandenen Module für welchen Angriffszweck eingesetzt werden. Das macht es erheblich schwieriger für die Sicherheitslösungen der Verteidiger, sie zu erkennen und zu bekämpfen.

Herkömmliche Security-Ansätze können solche Cyberangriffe nicht mehr aufdecken, damit müssen sich Unternehmen fortan mit Hilfe von KI schützen. So wird IT-Sicherheit zu einem Wettrennen zwischen guten und bösen KI-Systemen.

Cybersicherheit durch effiziente KI-Technologien

Techniken des maschinellen Lernens spielen ihre Rolle auf beiden Seiten des Schlachtfeldes, sowohl auf der Seite des Angreifers als auch auf der Seite der Cybersicherheit. Die von den Cyberkriminellen verwendeten Machine Learning (ML) Techniken finden die Schwachstellen eines Systems sowie ausgeklügelte Angriffsmöglichkeiten immer schneller, und überwinden so die Verteidigungsmauer eines Unternehmens immer leichter.

Daher muss der Einsatz von KI-Technologien zur Cybersicherheit dazu beitragen, Bedrohungen schneller und effektiver zu erkennen und zu bekämpfen. Auf der Verteidigungsseite spielen Machine Learning Modelle eine wichtige Rolle, um robuste und intelligentere Techniken zur Verbesserung der Leistung und Früherkennung von Angriffen bereitzustellen. Nur so können die Auswirkungen und der aufgetretene Schaden verringert werden. Techniken des maschinellen Lernens werden hierbei kombiniert, um die Genauigkeit der korrekten und frühzeitigen Klassifizierung von Cyberangriffen zu verbessern. Mit fortschrittlichen Algorithmen und Modellen kann KI große Mengen von Daten in Echtzeit analysieren und Muster und Anomalien erkennen. Durch ML lernen KI-Systeme kontinuierlich und passen sich umgehend an neue Bedrohungen an.

Voraussetzungen für einen effektiven KI-Einsatz

ML-Techniken liefern bessere Ergebnisse, wenn sie auf diversen, massiven und Echtzeit-Datensätzen trainiert werden. Um bestmöglichste Resultate zu gewährleisten, müssen daher mehrere Vorrausetzungen erfüllt werden.

So ist eine umfangreiche und qualitativ hochwertige Datenbasis entscheidend für die Genauigkeit und Effektivität eines KI-Modells. Je mehr Daten zur Verfügung stehen und analysiert werden können, desto besser kann die KI lernen und Anomalien erkennen. Die Auswahl der richtigen Algorithmen und Modelle ist ebenfalls wichtig. Die KI muss in der Lage sein, Muster in den Daten zu erkennen und sie schnell und präzise zu analysieren, um Bedrohungen zu identifizieren und abzuwehren. Außerdem ist eine laufende Validierung und Überwachung des KI-Modells unerlässlich, um sicherzustellen, dass es auf dem neuesten Stand der Bedrohungen und Trends in der Cybersicherheit ist. Die Überprüfung und Aktualisierung müssen dabei kontinuierlich erfolgen, um ihre Effektivität und Genauigkeit zu gewährleisten.

Um die Daten effizient zu verarbeiten und die Modelle zu trainieren und auszuführen, ist natürlich auch eine leistungsfähige Infrastruktur notwendig. Dazu gehören Hardware- und Softwarekomponenten wie GPUs, Cloud-Plattformen oder Frameworks.

Sicher im Netz mit der Deutschen Telekom und Partner Akamai

Die Deutsche Telekom gehört mit rund:

245 MILLIONEN

Mobilfunk-Kundinnen und Kunden

25 MILLIONEN

Festnetz-Anschlüssen und

21 MILLIONEN

Breitband-Anschlüssen

zu den führenden integrierten Telekommunikations-Unternehmen weltweit.

Das Fokusthema Cybersicherheit hat bei der Deutschen Telekom in den letzten Jahren zunehmend an Relevanz gewonnen. Sicherheits- und Netzlösungen (Netzwerk, IT und Cloud) verschmelzen zu hochsicheren Ende-zu-Ende-Lösungen. Hier bietet die Deutsche Telekom passende Beratung und Sicherheitslösungen für ein breites Digitalisierungsspektrum in den Bereichen Managed Cyber Defense, Cloud & Datensicherheit, Netzwerksicherheit, Endpunktsicherheit, und Industrielle & IoT-Sicherheit.

Unser Engagement zeigt sich auch bei der Auswahl unserer Partner, mit denen wir zum Thema Cybersicherheit zusammenarbeiten. Diese Unternehmen sind allesamt führend in ihrem Expertenfeld. Akamai Technologies ist eine renommierte Firma, mit der wir seit langem im Onlinegeschäft kooperieren. Beidseitiger Fokus ist die Daten- und Cybersicherheit, auch im Bereich KI. Akamai ist ideal positioniert, um hocheffiziente KI-Modelle zu entwickeln. Das Unternehmen ist für alle voraussetzenden Aspekte marktführend: von der Datenbasis, die eine umfassendste Sicht auf alle globalen Internetverkehre hat, über die fortschrittlichsten Algorithmen und Modelle, hin zu einer hocheffizienten Validierung und Überwachung.

Sorgenfrei dem Tagesgeschäft nachgehen

Dieses Whitepaper zeigt, wie KI bei der Analyse und Abwehr von Cyberangriffen eingesetzt wird. Wir betrachten die verschiedenen Arten von KI-Modellen und die Vorteile und Herausforderungen bei der Implementierung einer wirkungsvollen KI in der Cybersicherheit. Wir stellen außerdem unseren Partner Akamai vor. Als Marktführer im Bereich Cybersicherheit besitzt Akamai besondere Expertise und spielt eine wichtige Rolle bei der Entwicklung von KI-Modellen. Gemeinsam mit Akamai stellen wir Web-Sicherheitsdienste bereit, die speziell auf die Bedürfnisse einzelner Firmen zugeschnitten sind. Kunden können somit ihrem Tagesgeschäft nachgehen, ohne sich Sorgen über einen potenziellen Cyberangriff machen zu müssen.

2. EINSATZ VON KÜNSTLICHER INTELLIGENZ BEI DER ANALYSE UND ABWEHR VON CYBERANGRIFFEN

In der heutigen digitalen Welt werden Cyberangriffe immer ausgefeilter und anspruchsvoller. Traditionelle Sicherheitsmaßnahmen sind oft nicht mehr ausreichend, um diese Angriffe zu erkennen und abzuwehren. Hier kommt Künstliche Intelligenz (KI) ins Spiel. Durch den Einsatz von KI können Abwehrmechanismen entwickelt werden, die Bedrohungen schneller und effektiver erkennen und bekämpfen.

KI-gestützte Datenwissenschaft ist die Grundlage für zeitgemäße Bedrohungsinformationen. Sie ist ein Bereich innerhalb von Big Data, der Algorithmen verwendet, die statistische Techniken und andere Berechnungen beinhalten, um Daten zu interpretieren und aussagekräftige Muster aufzudecken. In der Sicherheitswelt bedeutet Data Science die Verwendung von Algorithmen, um böswillige Aktivitäten nahezu in Echtzeit aufzudecken, indem riesige Datenmengen aus Netzwerken und anderen Quellen verarbeitet werden.

Um diese Datenmengen effektiver verarbeiten zu können, werden Automation und Machine Learning eingesetzt. Der Einsatz von Machine Learning in der IT-Sicherheit bietet mehrere Vorteile, darunter:

- **Schnellere Erkennung von Angriffen:** ML-Modelle können in Echtzeit Anomalien erkennen und Benutzer oder Sicherheitspersonal warnen, um schnellere Reaktionszeiten zu ermöglichen.
- **Höhere Genauigkeit:** ML-Algorithmen können große Datenmengen verarbeiten und komplexe Muster in den Daten erkennen, was zu einer höheren Genauigkeit bei der Erkennung von Angriffen führt.
- **Automatisierte Abwehrmaßnahmen:** ML-Algorithmen können automatisch Abwehrmaßnahmen ergreifen, wie z.B. das Blockieren von verdächtigem Netzwerkverkehr oder das Quarantänisieren von infizierten Endgeräten.

Machine Learning wird bei der Erkennung und Abwehr von Cyberangriffen auf verschiedene Weise eingesetzt. So können ML-Algorithmen daraufhin trainiert werden, um anomale Verhaltensmuster in Netzwerkverkehr zu erkennen, die auf eine mögliche Attacke hindeuten. Bei der sogenannten Malware-Erkennung werden ML-Modelle auf Malware-Samples trainiert und lernen, ähnliche Malware-Dateien in Echtzeit zu erkennen und zu blockieren. Ähnlich sieht es bei der Phishing-Erkennung aus. Hier werden ML-Algorithmen trainiert, um E-Mails zu identifizieren, die Phishing-Angriffe enthalten, indem sie auf verdächtige Inhalte, URLs oder Absenderadressen achten. Weiterhin können ML-Modelle zur Identifizierung von Angriffsvektoren genutzt werden, um Schwachstellen in IT-Systemen und Netzwerken zu erkennen, die von Angreifern ausgenutzt werden können, und diese dann zu schließen.

Die Entwicklung und der Einsatz von leistungsfähigen KI-Modellen in der Cyberabwehr ist unerlässlich, um sich gegen immer intelligentere und auch KI-basierte Cyberangriffe zu schützen.

3. FOKUS DATENSICHERHEIT: DEUTSCHE TELEKOM UND PARTNER AKAMAI

Als Managed Security Service Provider bietet die Deutsche Telekom passende Beratung und Sicherheitslösungen für ein breites Digitalisierungsspektrum an, einschließlich Managed Cyber Defense, Cloud & Datensicherheit, Netzwerksicherheit, Endpunktsicherheit, industrielle & IoT-Sicherheit und professionelle Services. Dazu geht sie Partnerschaften mit anderen führenden Unternehmen ein.

Datensicherheit bei der Deutschen Telekom

Die Deutsche Telekom gehört mit rund 245 Millionen Mobilfunk-Kundinnen und Kunden, 25 Millionen Festnetz- und 21 Millionen Breitband-Anschlüssen zu den führenden integrierten Telekommunikations-Unternehmen weltweit.

Auf Basis globaler, sicherer Konnektivität, flexibler softwarebasierter Netze und Ende-zu-Ende-Sicherheitslösungen treiben wir als vertrauenswürdiger Partner die Digitalisierung unserer Kund*innen voran.

Fokusthemen wie Cybersicherheit gewinnen zunehmend an Relevanz: Sicherheits- und Netzlösungen (Netzwerk, IT und Cloud) verschmelzen zu hochsicheren Ende-zu-Ende-Lösungen. Sicherheitsfunktionen, die bislang separat erworben wurden, werden zunehmend ein Teil des Konnektivität-Produkts bzw. von Sicherheitslösungen.

Akamai betreibt die weltweit größte Plattform für Internet-Traffic mit mehr als

4000 STANDORTEN.

Web Security Lösungen in Partnerschaft mit Akamai

Um alle Bereiche der Cybersicherheit abzudecken, geht die Deutsche Telekom neben der Bereitstellung ihrer eigenen Netze und Services auch Partnerschaften mit anderen führenden Unternehmen ein.

Ein Beispiel für eine erfolgreiche Partnerschaft im Bereich Cybersicherheit ist die Zusammenarbeit mit Akamai Technologies. Akamai bietet als führendes Unternehmen im Bereich Web-Security hocheffektive Sicherheitslösungen zum Schutz vor Cyberangriffen. Diese Position wurde erst 2022 bestätigt: Im Gartner®-Bericht für 2022 „Magic Quadrant™ for Cloud Web Application and API Protection“ wurde Akamai zum führenden Anbieter ernannt. Auch im Bericht „Forrester Wave™: Web Application Firewalls, Q3 2022“ ist Akamai als führender Anbieter im Bereich „Angriffserkennung“ klassifiziert.

Mit mehr als 4.000 Standorten betreibt Akamai die weltweit größte Plattform für Internet-Traffic und verfügt damit über eine einzigartige Datenbasis sowohl in Bezug auf das Datenvolumen als auch die Datenqualität. Sie stellt jeden Tag Einblicke aus mehr als 300TB Angriffsdaten auf Webanwendungen und APIs, sowie Milliarden von Bot-Anfragen bereit.

Im Folgenden zeigen wir, welche grundsätzlichen Aspekte für die Entwicklung einer effektiven KI maßgeblich sind. Außerdem erläutern wir, wie die nahezu einmalige Basis an Echtzeit-Daten von Akamai mit fortschrittlichsten KI-Methoden kombiniert werden kann. Die dadurch ermöglichten intensiveren Analysen erkennen neue Bedrohungen immer besser und bilden die Grundlage für die Entwicklung passender Sicherheitslösungen.

4. ENTWICKLUNG EINES EFFEKTIVEN KI-MODELLS ZUR CYBERSICHERHEIT

Um der Bedrohung von Cyberangriffen wirkungsvoll entgegenzusetzen, brauchen wir effektive Verteidigungsmechanismen und -dienste, die unsere Datensicherheit gewährleisten. Hierzu sind Sicherheitslösungen, die auf speziell entwickelte KI-Modelle basieren, mitlerweile unerlässlich.

Bei der Entwicklung einer Künstlichen Intelligenz (KI) gibt es mehrere wesentliche Aspekte zu berücksichtigen:

1. **Zielsetzung:** Im ersten Schritt muss das Ziel der KI-Entwicklung definiert werden. Es soll realistisch, spezifisch und messbar sein.

2. **Datenbasis:** Eine solide Datenbasis ist entscheidend für die Entwicklung einer erfolgreichen KI. Die Daten müssen qualitativ hochwertig, ausreichend und repräsentativ für das Problem sein, das die KI lösen soll.

3. **Algorithmen und Modelle:** Die Auswahl und Anpassung der richtigen Algorithmen und Modelle beeinflusst, wie erfolgreich eine KI trainiert und optimiert werden kann, um sie in die Lage zu versetzen, präzise Vorhersagen oder Entscheidungen zu treffen.

4. **Infrastruktur:** Eine leistungsfähige Infrastruktur ist notwendig, um die Daten effizient zu verarbeiten und das KI-Modell zu trainieren und auszuführen. Dazu gehören Hardware- und Softwarekomponenten wie Grafikprozessoren (GPUs), Cloud-Plattformen oder Frameworks.

5. **Validierung und Überwachung:** Es ist wichtig, die Leistung der KI laufend zu validieren und zu überwachen, um sicherzustellen, dass sie weiterhin präzise Vorhersagen und Entscheidungen trifft, die den Erwartungen entsprechen.

6. **Ethik und Datenschutz:** Die Einhaltung ethischer Standards und der Datenschutz sind bei der Entwicklung von KI-Systemen von größter Bedeutung, damit die KI-Systeme fair, transparent und sicher sind, und die Privatsphäre der Nutzer respektiert wird.

Im Hinblick auf den Einsatz von KI bei der Entwicklung effektiver Web-Sicherheitsdienste sind die drei Aspekte Datenbasis, Algorithmen und Modelle, sowie Validierung und Überwachung besonders bedeutend.

Qualität der Datenbasis: das Kernstück einer KI-gestützten Web-Sicherheitslösung

Eine gut konstruierte, vielseitige und qualitativ hochwertige Datenbasis ist unerlässlich, um eine leistungsfähige und zuverlässige KI zur Cybersicherheit zu entwickeln. Die Datenbasis sollte aus einer ausreichenden Datenmenge und -vielfältigkeit bestehen, um eine robuste und aussagekräftige KI zu trainieren. So können die verschiedenen möglichen Sicherheitsszenarien und Umstände abgedeckt werden, damit die KI auch in komplexen und unvorhersehbaren Cyberangriffen gut funktioniert.

Die Güte der Daten ist ebenfalls ausschlaggebend. Sie sollten sauber und präzise sein, und müssen vor der Verwendung sorgfältig überprüft, sowie korrekt gelabelt und annotiert werden. Darüber hinaus sollten die Daten aktuell und repräsentativ sein. Dies bedeutet, dass die Datenbasis regelmäßig aktualisiert und erweitert werden sollte, so dass die KI mit den neuesten Entwicklungen und Trends in der Cybersicherheit Schritt halten kann.

Algorithmen und Modelle für präzise Vorhersagen und Entscheidungsfindungen

Es gibt eine Vielzahl von Algorithmen und Modellen, die für unterschiedliche Aufgaben und Anwendungen geeignet sind, wie z.B. neuronale Netze, Entscheidungsbäume, Random Forests, Support Vector Machines (SVMs) oder Cluster-Analysen. Die Wahl des richtigen Algorithmus oder Modells hängt von der Art der Daten ab, die verarbeitet werden sollen, sowie von den spezifischen Anforderungen und Zielen der KI-Anwendung zur Cybersicherheit. Es ist wichtig, mehrere Modelle auszuprobieren und zu vergleichen, um das beste Ergebnis zu erzielen. Auch sollten die Parameter der Algorithmen und Modelle entsprechend angepasst und optimiert werden, um die bestmögliche Leistung zu erzielen. Dies erfordert eine sorgfältige Überwachung und Anpassung der KI während des Trainings und der Validierung, um sicherzustellen, dass sie optimale Ergebnisse liefert.

Fortlaufende Validierung und Überwachung

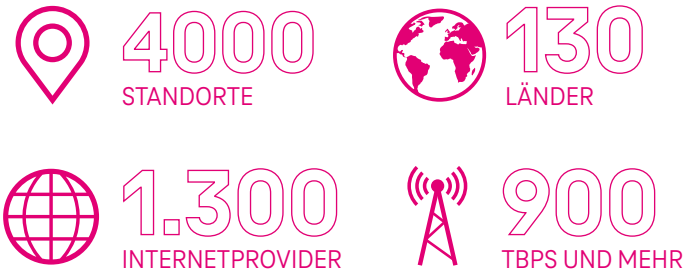
Bei der Validierung und Überwachung sollte besondere Sorgfalt darauf verwendet werden, dass die Ergebnisse genau sind und den Sicherheitsanforderungen entsprechen. Dabei ist das Fachwissen der Entwickler über die Dateninhalte, die als Basis für eine KI dienen, extrem wichtig, damit ihre Genauigkeit geprüft und Effektivität verbessert werden kann. Diese Ergebnisprüfung ist ein fortlaufender Prozess, der während der gesamten Lebensdauer der KI durchgeführt werden muss, und beinhaltet folgende Bereiche:

- **Trainingsvalidierung:** Die Leistung einer KI – inklusive Genauigkeit, Vorhersagefähigkeit und Fehlerquote – muss schon während des Trainings überprüft werden.
- **Validierung von Testdaten:** Nachdem die Trainingsdaten einer KI optimiert sind, muss sie auf unabhängige Testdaten überprüft werden. Nur so ist sie in der Lage, auch auf neue Daten effektiv zu reagieren und präzise Vorhersagen zu treffen.
- **Überwachung der Leistung:** Während der tatsächlichen Anwendung muss die Leistung einer KI kontinuierlich und in Echtzeit überwacht werden.
- **Überwachung der Datenqualität:** Die von der KI zu verarbeitenden Daten müssen allzeit korrekt und die KI auf dem neuesten Stand sein. Das erfordert eine kontinuierliche Überwachung der Qualität und Integrität der Daten.

5. FOKUS AKAMAI

Als Marktführer für sicherste KI-Modelle ist Akamai in allen drei Aspekten einer leistungsfähigen KI-Anwendung führend und damit in der Lage, KI-Modelle gezielt zur Abwehr von Cyberangriffen zu entwickeln und einzusetzen.

1. **Die Datenbasis**
Mit mehr als 4.000 Standorten in über 130 Ländern und einer Direktanbindung von mehr als 900 Tbps an über 1.300 Internetprovider betreibt Akamai die weltweit größte Plattform für Internet-Traffic. Diese umfangreichste „Sicht" auf den weltweiten Traffic bietet eine einzigartige Datenbasis zur Entwicklung hocheffektiver KI-Modelle. Das gilt sowohl für das Datenvolumen als auch in Bezug auf die Datenqualität. In Zahlen bedeutet das mehr als 300 TB an neuen Angriffsdaten täglich und eine konsolidierte Datenbasis von 9 Petabytes.



2. **Die Modelle und Methoden**
Akamai nutzt fortschrittliche KI-Modelle wie Deep Learning Neural Networks, Unsupervised Machine Learning und Adversarial Machine Learning Modelle. Die Modelle kommen in unterschiedlicher Weise zum Einsatz und bieten diverse Vorteile für die Effektivität in der Praxis.

A: DEEP LEARNING NEURAL NETWORK

Damit bezeichnet man eine Methode des maschinellen Lernens, die künstliche neuronale Netze mit zahlreichen Schichten zwischen Eingabe- und Ausgabeschicht einsetzt und dadurch eine umfangreiche innere Struktur herausbildet. Deep-Learning-Netzwerke sind in der Lage, komplexe Strukturen in Daten aufzuspüren. Sie haben den wesentlichen Vorteil, dass sie innerhalb von Minuten Abwehrmaßnahmen gegen neuartige Angriffe implementieren können – im Gegensatz zu anderen Methoden, die Tage oder sogar Wochen benötigen.

Bei Akamai kommen verschiedene Deep Learning Modelle zum Einsatz, wie zum Beispiel das Long Short Term Memory (LSTM) Model, ein künstliches neuronales Netz. Das LSTM wird eingesetzt, um sogenannte „Domain Generation Algorithms (DGAs)" zu erkennen. DGAs werden von Angreifern häufig verwendet, um das Erkennen von Exploits zu erschweren. Exploits maskieren böswillige Aktivitäten mithilfe von DGAs als gutartige Aktivitäten. In Kombination mit der Echtzeit-Datenbasis und dem Prozessieren von 1,5 Millionen DNS Abfragen pro Sekunde bietet der Einsatz von LSTM die Möglichkeit, nahezu in Echtzeit schädliche Domains zu erkennen.

Weitere Deep-Learning Modelle werden zur Identifikation von Bots genutzt, die menschliches Verhalten simulieren und nur durch ausgefeilte ML-Modelle und die Echtzeit-Datenbasis von Akamai effektiv erkannt werden können.

B: UNSUPERVISED MACHINE LEARNING

Das maschinelle Lernen unterscheidet grundsätzlich zwei Lernansätze. Zum einen können Verfahren des überwachten Lernens, nachfolgend als supervised Learning bezeichnet, angewendet werden. Dabei werden die Daten vor der Verarbeitung markiert. Zum anderen gibt es unüberwachtes Lernen, nachfolgend als unsupervised Learning bezeichnet, bei dem die KI selbst die Lösung findet.

Ziel des unsupervised Learning Ansatzes ist es, in Daten unbekannte Muster zu erkennen und Regeln abzuleiten. Für die Anwendung von unsupervised Learning Algorithmen werden in der Regel sehr viele Daten benötigt. Ohne eine ausreichende Datenmenge sind die Algorithmen nicht in der Lage, Clusterungen vorzunehmen und damit eine entsprechende Prognose über einen unbekannten Datensatz bzw. ein ungesehenes Datenset zu erstellen. Akamai arbeitet mit realen „first-party" Daten, was dafür den entscheidenden Vorteil ausmacht.

Das Unsupervised Machine Learning Modell lernt mit jedem neuen Echtzeit-Datensatz dazu und verfeinert gleichzeitig seine Berechnungen und Klassifizierungen. Das Ergebnis ist eine besondere Effektivität der resultierenden Modelle bei der Erkennung von Angriffsmethoden.

C: ADVERSARIAL MACHINE LEARNING

Adversarial Machine Learning (AML) beschäftigt sich mit dem Auffinden von potenziellen Sicherheitslücken in Verfahren des maschinellen Lernens (ML) inklusive der Entwicklung von geeigneten Gegenmaßnahmen. Da ML und insbesondere das sogenannte Deep Learning wesentlich für die aktuellen Erfolge im Bereich der KI verantwortlich sind, bedeuten Sicherheitslücken in ML-Verfahren eine erhebliche Bedrohung für KI-Systeme.

Wenn Trainingsdaten auf Open-Source-Daten, Verarbeitungsframeworks, Datenbibliotheken usw. basieren, birgt dies das Risiko, dass böswillige Akteure diese Open-Source-Datenbanken vergiften. So manipulieren sie, was das System lernt, und machen damit echte Angriffe unsichtbar. In den von Akamai eingesetzten ML-Verfahren werden diese potentiellen Gefahren systemisch eliminiert. Auch hier bildet Akamais besondere Datenbasis die Grundlage dazu, da sie reale „first-party" Daten beinhaltet und gegen Manipulationen immun ist.

3. Die Validierung und Überwachung

Das Fachwissen über die Dateninhalte, auf denen eine KI aufbaut, ist von entscheidender Bedeutung, um die Genauigkeit und Effektivität der KI zu verbessern. Dieses Verständnis ermöglicht es den Entwicklern, die Merkmale der Daten zu identifizieren und auszuwählen, die für das Training der KI am wichtigsten sind. Wenn die Ergebnisse der KI nicht den Erwartungen entsprechen oder nicht konsistent sind, können sie die Datenbasis und das Modell nach Bedarf anpassen, um bessere Ergebnisse zu erzielen.

400 SICHEHEITS-EXPERTEN IM EINSATZ

Hierzu investiert Akamai in 400 interne Sicherheitsexperten, die rund um die Uhr Angriffe verfolgen, untersuchen und abwehren. Diese Fach-Expertise in Kombination mit der enormen Echtzeit-Datenbasis bietet die ideale Grundlage zur Validierung und Überwachung der KI-Modelle.

Erkenntnisse aus den ML-Modellen bzw. deren Einsatz unterliegen wiederum einem strengen Freigabeprozess. Dieser besteht aus einer Reihe von Phasen, die verwendet werden, um Akamais Erkennungsgenauigkeit zu verbessern. Alle neuen Updates werden zunächst im Labor mit synthetischem Datenverkehr getestet, um sicherzustellen, dass sie Angriffe ordnungsgemäß abfangen und keine Fehlalarme verursachen. Anschließend werden diese Updates am Live-Produktionsdatenverkehr getestet, dann an Experten für maschinelles Lernen und menschliche Bedrohungen.

Wenn diese Prüfungen in jeder Phase bestanden wurden, stellt Akamai sie in einem kleinen Segment des Netzwerks bereit und überwacht sie – und setzt die Bereitstellung in Segmenten fort, bis das Update im gesamten Netzwerk verfügbar ist. Schließlich setzt Akamai die Überwachung bei einer 100 %-igen Bereitstellung fort, um sicherzustellen, dass die Erkennungen weiterhin wie erwartet funktionieren. Dabei sorgen Funktionen zur Selbstoptimierung dafür, dass alle verbleibenden Fehlalarme entfernt werden, die speziell für Ihren Datenverkehr bestimmt sind.

6. KI-GESTÜTZTE WEB-SICHERHEITS-DIENSTE

Das Ergebnis von Akamais ausgezeichneter Datenbasis und Expertise ist eine der effektivsten und fortschrittlichsten KI-Anwendung im Bereich Web-Security zum Schutz vor Angriffen, Betriebsstörungen und Datendiebstahl: die Adaptive Security Engine.

Die Power der Adaptive Security Engine

Die Adaptive Security Engine, kurz ASE, ist ein Herzstück der Web-Security Lösungen von Akamai.

1. FORTSCHRITTLICHSTE AUTOMATISIERUNG

ASE passt sich selbst an Ihre Umgebung und Ihren Datenverkehr an und stellt sich kontinuierlich auf neue und geänderte Regelsätze ein, die automatisch implementiert werden.

2. KI – MACHINE LEARNING

Innovatives ML analysiert den Datenverkehr, um Anomalien besser zu bewerten, die Genauigkeit zu erhöhen und die Anzahl an Fehlalarmen zu reduzieren.

4. 400 SICHERHEITS-EXPERTEN

Akamai investiert in 400 interne Sicherheitsexperten, die rund um die Uhr Angriffe verfolgen und untersuchen.

3. 9PB CLOUD-SECURITY-INTELLIGENCE-DATENBANK

Akamais umfangreiches globales Netzwerk produziert eine der größten Cloud-Security-Intelligence-Datenbanken.

ADAPTIVE BEDROHUNGSERKENNUNG

Die Datenbasis von Akamai über böswillige Aktivitäten in mehr als 1,3 Milliarden täglichen Kundeninteraktionen im Internet gibt tiefgehende Einblicke in Angreifer, die mit neuen Taktiken, Tools und Fähigkeiten ausgestattet sind. Die aus diesen Erkenntnissen abgeleiteten Informationen ermöglichen es, unterschiedliche Risikoprofile eingehender Anfragen zu verstehen, die versuchen, Ihre Anwendungen und APIs zu treffen.

Adaptive Erkennungen werden automatisch von der Bedrohungsforschung von Akamai aktualisiert, um sicherzustellen, dass der neueste und stärkste verfügbare Schutz verwendet wird. Umfangreiche Infrastruktur und Systeme führen alle neuen Erkennungen passiv aus – über den gesamten Akamai-Produktionsdatenverkehr hinweg. Die Analyse der Ergebnisse ist dank Machine Learning (ML)-Modellen besonders genau. Dies gibt Gewissheit, dass automatisierte Schutzmaßnahmen nicht nur im Labor gegen synthetischen Datenverkehr getestet werden, sondern auch unter realen Bedingungen.

EIGENSTÄNDIGE ANPASSUNG

Die ASE-Selbstoptimierung wurde entwickelt, um die Belastung durch manuelle Optimierung zu verringern. Maschinelles Lernen, statistische Modelle und Heuristiken werden auf alle Auslöser für jede Sicherheitsrichtlinie angewendet, um genau zwischen echten Angriffen und dem Datenverkehr von Endnutzern, der fälschlicherweise als Angriff identifiziert wird, zu unterscheiden.

Sicherheitsadministratoren können Empfehlungen mit einem Klick über die Benutzeroberfläche überprüfen und annehmen oder mithilfe von AppSec-APIs oder der Befehlszeilenschnittstelle (CLI) automatisieren. Über 96 % der Optimierungsempfehlungen werden von Akamai-Kunden akzeptiert, was ein hohes Maß an Genauigkeit beweist. Das führt zu mehr Vertrauen und betrieblicher Effizienz.

FLEXIBILITÄT BEI DER KONFIGURATION UND AUTOMATISIERUNG

Sicherheits- und DevOps-Teams können die Sicherheit auch operationalisieren, indem sie Aufrufe von Akamai-APIs über die CLI, Akamai Terraform oder Skripte in Ihre CI/CD-Automatisierungspipeline integrieren. Dies ermöglicht nicht nur ein schnelles Onboarden von Anwendungen, sondern auch ein einheitliches Management von Sicherheitsrichtlinien über große Anwendungsportfolios hinweg. Es zentralisiert die Sicherheitsdurchsetzung über Hybrid- und Multi-Cloud-Infrastrukturen und verbessert die Zusammenarbeit zwischen DevOps- und Sicherheitsteams in einem GitOps-Workflow für eine optimale Abdeckung. Konfigurations- und Automatisierungsflexibilität stellen sicher, dass leistungsstarke Sicherheit niemals die Entwicklungsgeschwindigkeit behindert. Dies bietet in der Praxis signifikante Vorteile für den Schutz einer Web-Präsenz vor Angriffen.

Die Vorteile der ASE für den Schutz von Webanwendungen

- Größtmöglicher aktueller Bedrohungsschutz
- Extrem niedrige False Positives und False Negatives
- Kein Bedarf an kontinuierlicher Wartung oder manuellem Tuning
- Kompatibel mit allen modernen DevOps-Modellen
- Schnellere Umsetzung und damit kürzeste ROI

KI-basierter Schutz vor einer Vielzahl von Bedrohungen auf Basis der Adaptive Security Engine

In der Praxis bietet die KI-basierte Adaptive Security Engine die fortschrittlichsten Web-Security Lösungen, die einen umfassenden Schutz gegen eine breite Palette von Bedrohungen gewähren.

APPLICATION AND API PROTECTOR

Akamais Web Application & API Protection-Lösung ist dafür ausgelegt, vollständige Web- und API-Bestände mit einem ganzheitlichen Set von leistungsstarken, speziell entwickelten Tools zu schützen. Die integrierte Selbstoptimierung nutzt maschinelles Lernen, statistische Modelle und Heuristiken, um alle Auslöser in jeder Richtlinie zu analysieren und genau zwischen echten und falsch positiven Ergebnissen zu unterscheiden.

BOT MANAGER

Die umfassende Bot-Management-Lösung bietet Unternehmen ein flexibles Instrument, um das breite Spektrum an automatisiertem Bot-Traffic besser zu verwalten. KI-basierte Machine-Learning-Modelle ermöglichen weitreichende Kontrolle darüber, wie Unternehmen mit verschiedenen Arten von Bots interagieren, um den Geschäftsnutzen zu maximieren und negative Geschäfts- oder IT-Auswirkungen zu minimieren.

ACCOUNT PROTECTOR

Durch die Nutzung von KI-basierten Machine-Learning-Modellen und darauf basierende Verhaltensanalysen identifiziert man authentische Nutzer und blockiert Betrüger. Die Lösung erkennt und unterbindet nicht-authentisches Nutzerverhalten, das zu Kontoübernahmen und anderem Missbrauch der Geschäftslogik führen kann.

PAGE INTEGRITY MANAGER

Diese Lösung schützt Websites vor JavaScript basierten „client-side“ Angriffen wie Web Skimming, Formjacking und Magecart-Angriffen, indem sie durch KI-basierte Modelle anfällige Ressourcen identifiziert, verdächtiges Verhalten erkennt und schädliche Aktivitäten blockiert.

AUDIENCE HIJACKING PROTECTION

Der Audience Hijacking Protection profitiert von KI-gestütztem maschinellem Lernen. Damit werden anfällige Ressourcen schnell identifiziert, verdächtige Verhaltensmuster erkannt und unerwünschte Anzeigen, Pop-ups, Affiliate-Betrug und andere böswillige Aktivitäten blockiert, die darauf abzielen, Ihre Nutzer abzuwerben.

FAZIT

KI wird von Cyberkriminellen zunehmend als Werkzeug für die Durchführung von Angriffen eingesetzt. Die Nutzung von KI zur Abwehr von Cyberangriffen ist daher unerlässlich, um effektiv auf die Bedrohungslage reagieren zu können. Eine leistungsfähige KI für die Abwehr von Cyberangriffen zeichnet sich durch eine umfangreiche und zuverlässige Datenbasis, fortschrittliche Algorithmen und Modelle sowie eine kontinuierliche Validierung und Überwachung aus.

Sicherheit ist einer der Kernwerte der Deutschen Telekom. Um ein breitmöglichstes Sicherheitsspektrum abzudecken, geht die Deutsche Telekom neben der Bereitstellung ihrer eigenen Netze und Services auch Partnerschaften mit anderen führenden Unternehmen ein. Ein Beispiel für eine erfolgreiche Partnerschaft im Bereich Cybersicherheit ist die Zusammenarbeit mit Akamai Technologies.
Die Firma Akamai hat aufgrund ihrer Content Delivery Infrastructure und ihrer einzigartigen Position im Internetverkehr eine umfangreiche und zuverlässige Datenbasis. Die Kombination dieser Datenbasis mit dem Know-how der Akamai Sicherheitsexperten ermöglicht die Entwicklung fortschrittlicher Algorithmen und Modelle für die Abwehr von Cyberangriffen. Die tägliche Validierung und Überwachung der KI-Modelle durch die Experten von Akamai stellt sicher, dass die Abwehrmechanismen auf dem neuesten Stand der Technik bleiben und somit stets effektiv auf sich ändernde Bedrohungslagen reagieren können.

Die Web-Sicherheitsdienste, die von der Deutschen Telekom gemeinsam mit Akamai angeboten werden, nutzen diese leistungsfähigen KI-Technologien, um Kunden vor einer Vielzahl von Cyberangriffen zu schützen. Mit unseren Produkten bieten wir ein umfassendes Portfolio zur Cybersicherheit, das auf spezifische Bedürfnisse zugeschnitten ist. Kunden können somit ihrem Tagesgeschäft nachgehen, ohne sich Sorgen um potenzielle Cyberangriffe zu machen.

Kontakt:
telekom-cdn-solutions@telekom.de

Internet:
https://globalcarrier.telekom.com/

Herausgeber:
Telekom Deutschland GmbH
Deutsche Telekom Global Carrier

Erleben,
was verbindet.

Quellenverzeichnis

1. Data science is the foundation for contemporary threat intelligence (White Paper, Status: Public)
https://www.akamai.com/resources/product-brief/data-science-is-the-foundation-for-contemporary-threat-intelligence
Unterquelle zu LSTM: https://en.wikipedia.org/wiki/Long_short-term_memory
2. Akamai Unveils Machine Learning That Intelligently Automates Application And API Protections And Reduces Burden On Security Professionals (Status: Public)
https://www.akamai.com/newsroom/press-release/-akamai-unveils-machine-learning-that-intelligently-automates-ap
3. New Security Enhancements That Intelligently Automate Application and API Security, Mitigate Online Fraud, and Reduce Burden on Security Professionals (Status: Public)
https://www.akamai.com/blog/news/akamai-platform-update-new-security-enhancements-that-intelligently
4. Akamai's platform security enhancements strengthen protection for web apps, APIs and user accounts (Status: Public)
https://www.helpnetsecurity.com/2021/06/17/akamai-platform-security-enhancements/
5. The Adaptive Security Engine — A Quantum Leap Forward for Application and API Protection (Status: Public)
https://www.akamai.com/blog/security/the-adaptive-security-engine-a-quantum-leap-forward-for-application
6. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade (Status: Public)
https://ieeexplore.ieee.org/document/9277523
7. Artikel in Security Insider: „Gute" KI gegen „böse" KI (Status: Public)
https://www.security-insider.de/gute-ki-gegen-boese-ki-a-87a5a112d79e771022f25b8b278e34c0/