mimecast

White Paper

KI und Cybersecurity:

Das Versprechen und die Wahrheit der KI-Sicherheitsrevolution

Überblick

Im Bereich künstliche Intelligenz und maschinelles Lernen herrscht unter IT-Experten ein regelrechter Hype. Dies zeigt sich deutlich im Hype Cycle for Artificial Intelligence von Gartner, wo aufgezeigt wird, dass die meisten KI-Anwendungen sich noch auf dem Weg zum "Gipfel überzogener Erwartungen" befinden.[1] Leider ist die Cybersicherheitsbranche ähnlich betroffen. Viele Sicherheitsanbieter setzen stark auf KI-Funktionen und preisen ihre Lösungen als universelle Heilmittel an, obwohl zahlreiche Hindernisse und Herausforderungen den Weg zu den hohen Erwartungen, die in diese Technologien gesetzt werden, noch versperren.

Dennoch wäre es für Cybersicherheitsexperten fahrlässig, das Potenzial von Künstlicher Intelligenz zu ignorieren. Angesichts einer sich täglich komplexer entwickelnden Bedrohungslandschaft und zunehmend fortschrittlicher KI-Anwendungen werden KI und verwandte Disziplinen schnell zu unverzichtbaren Werkzeugen für die Cybersicherheit. Der Bedarf an KI in der Cybersicherheit – und bald auch an Maschinellem Lernen (ML) und Natürlicher Sprachverarbeitung (NLP) – wird weiter steigen. Deshalb ist es entscheidend für Unternehmen, KI mit traditionellen Cybersicherheitsansätzen zu integrieren, um das Risiko von Cyberbedrohungen so gering wie möglich zu halten.

Wie kann ein Sicherheitsexperte jedoch zwischen Realität und Hype unterscheiden und die richtigen Entscheidungen treffen, um die Kommunikation, Mitarbeiter und Daten seines Unternehmens zu schützen?

Dieses Whitepaper wird diese Frage umfassend beantworten, indem es die Bedeutung von Künstlicher Intelligenz (KI) für die Cybersicherheit beleuchtet. Es wird erklären, warum KI eine entscheidende Rolle spielt, wie sie erfolgreich in bestehende Sicherheitssysteme integriert werden kann, welche spezifischen Anwendungsfälle existieren und einen Ausblick auf die zukünftige Entwicklung dieser Technologien geben.

Dieses Whitepaper wird erforschen:

- **Die Entwicklung**
  Die fortschreitende Entwicklung von Geschäftstechnologien und die zunehmend raffinierten Methoden der Cyberkriminellen machen Künstliche Intelligenz (KI) für die Cybersicherheit unverzichtbar.
- **Vorteile & Gefahren**
  Die Potenziale und Risiken von Künstlicher Intelligenz für die Cybersicherheit.
- **KI-Anwendungen für die Cybersicherheit**
  Konkrete Anwendungsfälle, in denen KI-Fähigkeiten die Resilienz von Unternehmenslösungen gegen Cyberangriffe stärken.
- **Bewährte Praktiken**
  Die effektivsten Methoden, wie KI die Cybersicherheit verbessern kann – unter Berücksichtigung des aktuellen Entwicklungsstands von KI.
- **Blick nach vorn**
  Wie werden sich die KI-Fähigkeiten in der Cybersicherheit entwickeln?

1. Gartner identifiziert vier Trends, die in naher Zukunft Innovationen im Bereich der künstlichen Intelligenz vorantreiben, Gartner Inc.

Die Entwicklung

Steigender Sicherheitsdruck durch Konsolidierung von Unternehmen auf weniger Plattformen

Die Realität, mit der sich Cybersecurity-Experten konfrontiert sehen, ist, dass alles überall gleichzeitig vernetzt ist. Hybride Arbeitsumgebungen haben sich für Unternehmen als schwer rückgängig zu machen erwiesen und eine permanente Welt mit verteilten Mitarbeitern, Systemen, Geräten und Daten geschaffen.

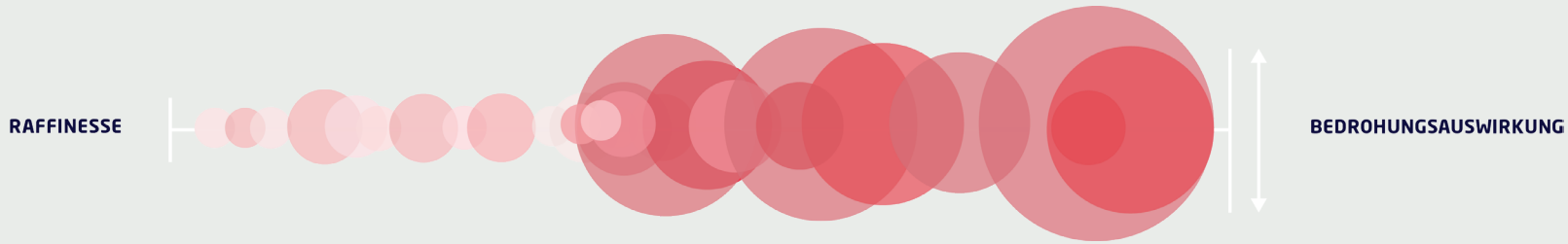
Gleichzeitig setzen sich die Veränderungen bei Technologien und Arbeitsmustern fort. Generative KI hat sich rasant verbreitet und den Zugang zu einer unglaublich leistungsstarken Technologie für alle zugänglich gemacht. Dieses Potenzial wird von allen genutzt, von nicht-technischen Mitarbeitern bis hin zu den raffiniertesten Bedrohungsakteuren.

Auch die Kommunikationskanäle werden weiter ausgebaut. E-Mail bleibt der wichtigste Kanal, aber Collaboration-Tools wie Microsoft Teams und Slack sind inzwischen ein fester Bestandteil des Arbeitsalltags. Auch Tools wie SharePoint und OneDrive sind fest integriert. Das Ergebnis ist eine größere und anfälligere Angriffsfläche als je zuvor.

Dieses Risiko wird durch die zunehmende Vereinheitlichung noch verstärkt, da Millionen von Nutzern weltweit die gleichen Tools verwenden. Der potenzielle Gewinn aus dem Zugriff auf große Datenmengen hat Anbieter wie Microsoft und Google zu unwiderstehlichen Zielen gemacht, und die Auswirkungen auf die Opfer sollten nicht unterschätzt werden. Die durchschnittlichen Kosten einer Datenpanne stiegen 2023 auf 4,45 Millionen Dollar – der höchste Wert in der 19-jährigen Geschichte des IBM-Berichts “Cost of a Data Breach”.[2]

> “Die Konsolidierung digitaler Werkzeuge ist einer der bedeutendsten Faktoren, die die heutige Bedrohungslandschaft prägen. Der weitverbreitete Umstieg auf Plattformen wie Microsoft 365 hat Bedrohungsakteuren die Möglichkeit gegeben, raffiniertere Angriffe zu entwickeln. Ein Beispiel hierfür ist, dass einige Phishing-as-a-Service-Gruppen jetzt Phish-Kits im Microsoft-Stil verkaufen. Gleichzeitig wurde die Effektivität menschlicher Abwehrmaßnahmen durch den Missbrauch legitimer Dienste und die Nutzung kompromittierter Konten von vertrauten Plattformen erheblich beeinträchtigt.”
>
> **Dr. Kiri Addison - Senior Manager, Produktmanagement, Mimecast**

Es gibt keine Möglichkeit, der Bedrohung aus dem Weg zu gehen. Organisationen stehen einem Kampf gegenüber.
Laut dem aktuellen State of Email Security Report von Mimecast bereiten sich 76% der Unternehmen auf die Folgen eines E-Mail-Angriffs im kommenden Jahr vor, und 97% haben in den letzten 12 Monaten mindestens einen Phishing-Angriff erlebt.



2. Kosten einer Datenpanne 2023, IBM

Die Vorteile und Gefahren
von KI in der Cybersicherheit

Angesichts der zunehmenden Geschwindigkeit, des Umfangs und der Komplexität von Angriffen entsteht der Mythos, dass KI ein Allheilmittel für die Sicherheit von Kommunikation, Menschen und Daten sei. Viele setzen große Hoffnungen in KI – sie erscheint als Rettungsanker für IT- und Sicherheitsteams, die mit begrenzten Ressourcen, steigender Komplexität und wachsenden Risiken konfrontiert sind. Doch die Realität ist differenzierter. Es steht außer Frage, dass KI für eine moderne Cyberverteidigungsstrategie unverzichtbar ist. Trotzdem ist sie wie jede neue Sicherheitsinnovation nur ein Werkzeug – wenn auch ein äußerst leistungsfähiges.

Vorteile

Trotz der komplexen Algorithmen, die unter der Haube arbeiten, lassen sich die Vorteile von KI einfach und klar erklären. KI:

- Kann riesige Datenmengen verarbeiten – viel mehr, als ein Mensch verstehen könnte.
- Ist schnell – sie verarbeitet Informationen deutlich schneller als jeder Mensch.
- Kann im Laufe der Zeit "intelligenter" Entscheidungen treffen. Sie kann lernen, solange ein Data-Science-Team die Modelle überwacht und bei Bedarf neu trainiert.
- Kann einige Aufgaben vereinfachen und/oder automatisieren.

Im Bereich der Cybersicherheit, wo große Datenmengen anfallen und ein paar zusätzliche Minuten Reaktionszeit den Unterschied zwischen einem abgewehrten Angriff und einem katastrophalen Einbruch bedeuten können, können diese Vorteile einen erheblichen Mehrwert für Unternehmen schaffen.

Die Auswirkungen der generativen KI

Generative KI ist schon lange ein bekanntes Diskussionsthema, doch die Einführung von Chat GPT Ende 2022 hat die Diskussion zweifellos verändert. Mit der weitreichenden Zugänglichkeit dieses mächtigen Werkzeugs für jeden mit Internetanschluss explodierte die Experimentierfreude, begleitet von Ängsten darüber, welche Möglichkeiten generative KI letztendlich bieten könnte.

Die Cybersicherheitsbranche bildet da keine Ausnahme, und die Vorstellung, dass Chat GPT über eingebaute Sicherheitsvorkehrungen verfügt, ist leider wenig beruhigend. Im Dark Web werden bereits Varianten angeboten, die auf böswillige Zwecke abgestimmt sind.[3] Es gibt noch viele Unbekannte darüber, wie genau diese Technologien eingesetzt werden, aber erste Trends zeichnen sich ab.

Für böswillige Akteure scheint die Erstellung realistischer Phishing-E-Mails in großem Stil einer der Hauptanwendungsfälle zu sein. Diese E-Mails enthalten keine Rechtschreib- oder Grammatikfehler mehr, keine Tippfehler und wirken nicht mehr gestelzt. Zudem unterstützen sie mehrere Sprachen, um bisher schwer zugängliche Regionen ins Visier zu nehmen.

Es ist schwer zu sagen, wie weit generative KI bereits in diesem Bereich genutzt wird, da noch unklar ist, ob Menschen oder Maschinen konsequent erkennen können, ob eine E-Mail, ob Phishing oder nicht, von KI generiert wurde. Sicher ist jedoch, dass die Zahl der Phishing-Angriffe steigt, wobei 98 % der Angriffe per E-Mail erfolgen.[5] Ein Teil dieses Anstiegs dürfte auf den Einsatz generativer KI zurückzuführen sein.

3. https://cybersecuritynews.com/black-hat-ai-tools-xxxgpt-and-wolf-gpt/ I 4. https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year
5. Verizon Data Breach Report 2023

KI-Anwendungen für die Cybersicherheit

Der Mimecast-Ansatz: Mehrschichtige, KI-gestützte Sicherheit

In der Cybersicherheit ging es schon immer um Entscheidungen, bei denen viel auf dem Spiel steht. Was sollte durchgelassen werden? Was sollte blockiert werden? Welche Risiken sollten eingegangen werden? KI ändert nichts an diesen Fragen, aber wenn sie intelligent eingesetzt wird, kann sie helfen, diese Fragen schneller, in größerem Umfang und effizienter zu beantworten.

Mimecast, seit 20 Jahren führend im Bereich der E-Mail-Sicherheit, war immer Vorreiter in der Einführung neuer Technologien und Strategien zur Verteidigung gegen eine Vielzahl von Gegnern. Dazu zählt auch Künstliche Intelligenz, die wir in jeder Ebene unserer Lösungen einsetzen, wo die Technologie angewendet werden kann. Diese Entscheidung maximiert die Verteidigung unserer Kunden, neutralisiert eine Vielzahl von Bedrohungen und entlastet ihre Sicherheitsteams. Allerdings ist KI kein Allheilmittel. Unser Erkennungsstack nutzt die richtigen Inspektionen zur richtigen Zeit, wobei KI-Algorithmen mit bewährten Technologien zusammenarbeiten, die wir über fast 20 Jahre hinweg kontinuierlich verbessert haben.

Wir kombinieren Dutzende verschiedener Ansätze, die durch KI ergänzt werden, um die branchenführende Sicherheitseffizienz zu erreichen, für die Mimecast bekannt ist.

> KI und maschinelle Lerntechniken sind keine magischen schwarzen Kästen, die einfach so für Sicherheit sorgen. Letztlich sind sie Werkzeuge, die uns dabei unterstützen, Probleme zu lösen. Der entscheidende Faktor für ihren sicheren und effektiven Einsatz in der Cybersicherheit ist die richtige Anwendung dieser Werkzeuge durch sachkundige Personen und unter Verwendung hochwertiger Daten."
>
> **Robin Moore - Leitender Produktmanager für KI und Machine Learning, Mimecast**

> Große Sprachmodelle und Techniken zur Verarbeitung natürlicher Sprache haben sich im letzten Jahr stark weiterentwickelt, was Cyberkriminelle zu immer raffinierteren Angriffen veranlasst hat. KI wird benötigt, um effektiv gegen diese Bedrohungen vorzugehen und den Bedrohungsakteuren einen Schritt voraus zu sein, die diese Technologien missbrauchen würden."
>
> **Guhan Sukumaran - Senior Manager, Data Science and Machine Learning, Mimecast**

Ein anschauliches Beispiel: Erkennung bösartiger URLs

Die URL-Erkennung von Mimecast veranschaulicht perfekt die KI-Philosophie des Unternehmens. Die URL-Erkennungsfunktion von Mimecast erfüllt eine einzelne wichtige Aufgabe - die Identifizierung bösartiger URLs - aber sie ist sicherlich nicht isoliert als eine einzelne Funktion oder ein einzelnes Produkt. Vielmehr kombiniert sie Dutzende von Scan-Ebenen, die zusammenarbeiten, um risikoreiche URLs so effektiv und effizient wie möglich zu erkennen.

Einige dieser Ebenen umfassen einfache Suchvorgänge, die grundlegende Bedrohungen abfangen. Andere nutzen regelbasierte Algorithmen, um komplexere, jedoch häufige Angriffe zu erkennen. KI-Algorithmen kommen dann zum Einsatz, wenn schnelle Entscheidungen erforderlich sind, insbesondere in Situationen, in denen andere Technologien keinen eindeutigen Wert liefern können, ob das Risiko gering genug ist, um die Seite zu öffnen, oder ob eine weitergehende Überprüfung notwendig ist.

Warum setzt Mimecast nicht ausschließlich auf KI-Algorithmen? Letztlich liegt die Stärke der Lösung nicht in einer einzelnen isolierten Funktion. Vielmehr liegt sie in der Synergie aller dieser Funktionen, sei es KI-basiert oder anderweitig.

Wenn Mimecast sich für den Einsatz von KI in einem Produkt entscheidet, bietet dies klare Vorteile: Je mehr Trainingsdaten den Algorithmen zur Verfügung stehen, desto besser können sie lernen. Mimecast schützt weltweit mehr als 42.000 Kunden und analysiert täglich 1,7 Milliarden E-Mails. Dies bildet die Grundlage für die KI, die dazu beiträgt, die erstklassige E-Mail-Sicherheit bereitzustellen, die unsere Kunden benötigen, um sicher zu sein.

Das Data-Science-Team von Mimecast nutzt diese Daten, um KI-Modelle in die Mimecast-Lösungen zu integrieren. Es überwacht kontinuierlich die Leistungsfähigkeit dieser Modelle im Kontext der sich ständig weiterentwickelnden Bedrohungslandschaft und entscheidet, wann eine Neuausbildung der Modelle erforderlich ist, um ihre Spitzenleistung zu erhalten.

Ausgewählte Mimecast AI-Funktionen

Im Folgenden finden Sie eine Übersicht über einige der Möglichkeiten, wie KI-Algorithmen die branchenführende Sicherheit von Mimecast unterstützen.

Verteidigung gegen Geschäftsemail-Kompromittierung und Bereitstellung von Informationen für Mitarbeiter am Risikopunkt

Selbst erfahrene Nutzer eines Unternehmens können durch eine bösartige E-Mail getäuscht werden, insbesondere da Angreifer fortschrittliche Technologien einsetzen, um Informationen über Mitarbeiter zu sammeln und diese in überzeugenden Spear-Phishing-Angriffen zu verwenden. Mimecast verwendet KI-Algorithmen und NLP, um gezielte E-Mail-Bedrohungen effektiv zu erkennen, Benutzer mit relevanten Informationen zu versorgen und die Möglichkeiten der Angreifer zur Informationsbeschaffung einzuschränken. Wie die meisten KI-Lösungen von Mimecast lernt auch diese Lösung kontinuierlich dazu und verbessert ihre Effektivität mit jedem vereitelten Angriff.

So funktioniert es

- Nutzt Social Graphing-Technologie, die auf maschinellem Lernen basiert, um die Kommunikation zu visualisieren und typische Kommunikationsmuster zu verstehen, die als Referenz für die Erkennung abweichenden Verhaltens dienen.
- Analysiert den aus E-Mail-Text extrahierten Inhalt mit NLP, um anhand von Risikokategorien, Nachrichtenmerkmalen oder Regeln den Schweregrad zu bestimmen. Nachrichten können entsprechend ihrer Richtlinienstufe entweder abgelehnt oder einer administrativen Überprüfung unterzogen werden.
- Fügt bei Bedarf kontextbezogene Warnbanner in E-Mails ein, um Mitarbeiter zu alarmieren. Diese Banner werden in Echtzeit auf allen Geräten aktualisiert, wenn sich die Risikostufen ändern.
- Erkennt und blockiert Tracker, die in E-Mails von Mitarbeitern eingebettet sind, um die versehentliche Weitergabe von Informationen an Angreifer zu verhindern.

Verhindern, dass ausgehende E-Mails und sensible Daten in falsche Hände geraten

Angreifer stellen nicht die einzige Bedrohung für Ihr Unternehmen dar. Mitarbeiter können versehentlich oder absichtlich eine E-Mail an die falsche Adresse senden, was nicht nur peinlich sein kann, sondern auch schwerwiegende Folgen haben könnte, wie Geldstrafen, Rufschädigung und Verstöße gegen Compliance-Richtlinien. Mimecasts Misaddressed Email Protection nutzt KI, um die Kommunikation der Benutzer zu überwachen, Anomalien zu erkennen und Mitarbeiter zu warnen, wenn sie kurz davor stehen, eine E-Mail an eine neue oder unbekannte Adresse zu senden.

So funktioniert es

- Erkennt abnormale Kommunikationsaktivitäten mithilfe von Social Graphing, das auf maschinellem Lernen basiert, um die typischen Verhaltensmuster eines Benutzers zu erkennen.
- Hält falsch adressierte E-Mails am Gateway zurück und benachrichtigt den Absender über das mögliche Problem.
- Bietet dem Absender eine zweite Chance, zu bestätigen, dass die E-Mail an die richtige Adresse gesendet wird, und trägt so dazu bei, dass E-Mail-Daten angemessen und im Einklang mit gesetzlichen Bestimmungen behandelt werden.

Abfangen von bösartigen E-Mails, die als legitime Nachrichten von glaubwürdigen Quellen getarnt sind

Das Abfangen von Anmeldeinformationen ist auf dem Vormarsch, besonders da immer mehr Unternehmen File-Sharing-Dienste wie Microsoft OneDrive und SharePoint für die Remote-Zusammenarbeit nutzen. Angreifer verweisen in bösartigen E-Mails auf diese Websites, um Erkennung zu umgehen, und locken Opfer auf URLs, wo sie unwissentlich ihre Geschäftslogins preisgeben könnten.

Der Mimecast-Schutz gegen das Sammeln von Anmeldeinformationen – Credential Harvesting - nutzt maschinelles Lernen und fortschrittliche Computer Vision, um zu prüfen, ob eine URL legitim ist. Die Analysen sind so genau, dass sie sogar kleinste Abweichungen auf einer vermeintlich sicheren Webseite erkennen können.

So funktioniert es

- Computer-Vision-Algorithmen erkennen Anomalien in den auf dem Bildschirm angezeigten Informationen wie Branding, Anmelde- oder Zahlungsformulare.
- Abhängig von der Schwere des Verdachts und des Risikos werden Benutzer entweder gewarnt oder der Zugang zur Seite wird gesperrt. Der KI-Algorithmus lernt aus jeder Analyse, um mit der Zeit immer präziser zu werden - und ist viel weniger anfällig für ausgeklügelte Markenimitationen als der durchschnittliche Benutzer.

Verdächtige E-Mails kategorisieren und klassifizieren

So funktioniert es

Wenn Benutzer verdächtige E-Mails an das SOC von Mimecast melden, verwendet Mimecast KI, um sie automatisch zu kategorisieren, zu sortieren und für die Untersuchung zu priorisieren. Die Metadaten jeder verdächtigen E-Mail werden automatisch mit einer Risikobewertung und Informationen über das bisherige Meldeverhalten des Benutzers angereichert. Diese Informationen unterstützen die Analysten dabei, schnell zu entscheiden, ob eine E-Mail bösartig ist oder nicht. Die Entscheidungen der Analysten fließen wiederum in unsere KI-Modelle ein.

Websites kategorisieren

So funktioniert es

Überwachtes Lernen kategorisiert Websites als bösartig oder unangemessen, so dass die Inspektions-Engines von Mimecast den Zugriff auf diese Seiten blockieren.

Identifizierung von Bildern, die “nicht sicher für die Arbeit” bzw. unangemessen sind

So funktioniert es

Nicht jedes per E-Mail empfangene Bild ist unangemessen. Die Herausforderung besteht darin, zwischen geeigneten und “unangemessenen” Bildern zu unterscheiden. Deep Learning und Bildverarbeitungsalgorithmen arbeiten zusammen, um solche Bilder in E-Mails zu erkennen, insbesondere solche mit pornografischem Inhalt. Dies trägt dazu bei, eine sichere und professionelle Arbeitsumgebung zu gewährleisten. Die Kontrolle über solche Inhalte, ob beim Empfangen oder Senden, ist entscheidend für den Ruf der Marke, da die E-Mail-Adresse eines Mitarbeiters das Unternehmen repräsentiert.

QR-Code Erkennung

So funktioniert es

QR-Codes sind mittlerweile ein verbreitetes Mittel für den schnellen und bequemen Austausch von Informationen geworden, aber sie können auch ein Sicherheitsrisiko darstellen. QR-Codes können Links zu Malware, unangemessenen Websites oder anderen schädlichen Inhalten enthalten. Mimecast ist in der Lage, nicht nur QR-Codes mithilfe unserer Deep Learning- und Computer-Vision-Algorithmen zu erkennen, sondern auch den Link hinter dem QR-Code aufzulösen und an die URL-Erkennungsfunktion von Mimecast weiterzuleiten, um risikoreiche URLs zu identifizieren. Diese Technologien, einschließlich maschinellem Lernen, helfen dabei zu bestimmen, ob QR-Code-Links bösartig sind, und tragen dazu bei, E-Mails abzulehnen, um vor solchen Phishing-Angriffen zu schützen.

Malware und Zero-Day-Schutz

So funktioniert es

Mimecast nutzt KI in unseren Inspektions-Engines, um Schutz vor bisher unbekannten Bedrohungen wie APTs, Zero-Day-Attacken und Ransomware zu bieten. Die maschinellen Lernalgorithmen, die in die verschiedenen Dateiprüfungsfunktionen integriert sind, extrahieren Merkmale aus vorhandenen Malware-Mustern oder -Familien. Dadurch wird die Vorhersage zukünftiger Malware auf Basis gemeinsamer ähnlicher Merkmale ermöglicht.

Die Sandbox von Mimecast verwendet Technologien für maschinelles Lernen und Verhaltenserkennung, um sicherzustellen, dass nur Dateien, die einer vertieften Analyse bedürfen, zur Prüfung weitergeleitet werden. Dies verbessert die Analyseresultate erheblich. Dateien, die an die Sandbox gesendet werden, unterliegen einer Analyse durch fortschrittliche maschinelle Lernalgorithmen sowie Köder-, Anti-Evasionstechniken, Anti-Exploit-Maßnahmen und einer aggressiven Verhaltensanalyse. Dies führt zu einer effizienten Erkennung von Malware. Durch die Integration von maschinellen Lernalgorithmen sind diese Technologien effektiver als signaturbasierte Systeme, da sie die Erkennungsraten für neue Malware-Varianten erhöhen können.

Bewährte Praktiken

Die entscheidende Strategie besteht darin, KI-Funktionen in eine umfassende Verteidigungsstrategie zu integrieren. Das bedeutet, KI nicht isoliert, sondern als integralen Bestandteil von Sicherheitslösungen einzusetzen, die ihre Stärken optimal ausspielen können. Diese Lösungen sollten dann mit anderen Sicherheitsmechanismen kombiniert werden, um eventuelle Schwachstellen abzudecken. Das Ziel ist ein vielschichtiges Cyber-Verteidigungssystem, das auf der fortschrittlichen maschinellen Intelligenz basiert, gleichzeitig aber auch von bewährten regelbasierten Ansätzen und anderen Sicherheitskontrollen profitiert. Im Bedarfsfall können erfahrene Analysten aus dem Security Operations Center (SOC) ihre Expertise einbringen, um komplexe Entscheidungen zu treffen und die Effektivität der gesamten Sicherheitsstrategie zu optimieren.

KI kann häufig auftretende Bedrohungen in großem Umfang identifizieren und wirksam neutralisieren, oft genauer als menschliche Analysten. Dennoch ist eine umfassende Sicherheitsarchitektur erforderlich, um wirklich gefährliche Angriffe zu stoppen. Diese Architektur sollte KI-gestützte Filter verwenden, die von Data-Science-Experten entwickelt wurden. Diese Experten kennen die Feinheiten, um zwischen eindeutig schädlichen Bedrohungen und legitimen E-Mails oder Links zu unterscheiden, die für den Geschäftsbetrieb wichtig sind. Da kein Erkennungsmodell perfekt ist, ist kontinuierliches Feedback entscheidend, um schnell zu erkennen, wo die KI-Modelle Schwächen zeigen und Verbesserungen erforderlich sind.

In der Praxis bedeutet dies, dass KI zunächst dort eingesetzt wird, wo große Mengen an Daten verfügbar sind. In der Cybersicherheit wurde KI beispielsweise zunächst verwendet, um Anomalien im Benutzerverhalten zu erkennen oder um verdächtigen Netzwerkverkehr zu identifizieren. Diese Anwendungen nutzen umfangreiche Datensätze, um potenzielle Bedrohungen oder Einbrüche frühzeitig zu erkennen.

> Im Bereich der künstlichen Intelligenz und des maschinellen Lernens treibt die tiefe Synergie zwischen menschlichem Fachwissen und algorithmischen Fähigkeiten die Innovation zu neuen Höhen. Die symbiotische ‘Human-in-the-Loop’-Unterstützung bildet nicht nur den Rahmen, sondern ist der zentrale Baustein, der für unübertroffene Präzision und Anpassungsfähigkeit sorgt. Während Algorithmen sich durch die Datenlandschaft bewegen, bringt der Mensch kontextuelles Verständnis und ethisches Urteilsvermögen ein. Diese dynamische Zusammenarbeit gestaltet eine Zukunft, in der die Verschmelzung von künstlicher Intelligenz und menschlicher Intuition bahnbrechende Fortschritte ermöglicht und eine Harmonie schafft, die nicht nur automatisierte Fähigkeiten übertrifft, sondern auch im Einklang mit der Essenz unserer gemeinsamen menschlichen Erfahrung steht.
>
> **Vedant Ruparelia - Senior Applied Machine Learning Scientist, Mimecast**

> Künstliche Intelligenz und maschinelle Lerntechnologien sind nicht per se überlegen. Die Effektivität des maschinellen Lernens hängt stark von der Qualität der zugrunde liegenden Trainingsdaten ab. Dabei gilt der Grundsatz “Garbage in, garbage out”: Schlechte Daten können zu fehlerhaften Ergebnissen führen. Zusätzlich spielt menschliche Intelligenz eine entscheidende Rolle in der Entwicklung dieser Technologien. Falsche Entscheidungen während des Trainings können zu verzerrten oder ungenauen Modellen führen. Es ist überraschend einfach, in diesen Fallen beim maschinellen Lernen zu landen.”
>
> **Navya Vats - Senior Data Scientist, Mimecast**

Blick nach vorn

Wie werden sich die KI-Fähigkeiten in der Cybersicherheit entwickeln?

In der Welt der Science-Fiction wimmelt es von epischen Cyber-Schlachten zwischen automatisierten guten und bösen künstlichen Intelligenzen. Ein Autor, der maßgeblich zur Verbreitung des Begriffs “Cyberspace” beigetragen hat, ist William Gibson, der in seiner wegweisenden Romantrilogie, beginnend mit “Neuromancer” im Jahr 1984, solche faszinierenden Handlungsstränge eingeführt hat.

Die Realisierung solcher Szenarien liegt nach allgemeiner Einschätzung der Branche noch viele Jahre in der Zukunft. Doch jüngste Entwicklungen deuten darauf hin, dass die KI schneller Fortschritte macht, als viele erwartet haben.

Es ist entscheidend, die Bedeutung der KI realistisch einzuschätzen. Heute ist KI ein unverzichtbarer Bestandteil komplexer Cybersicherheitslösungen, die Unternehmen einsetzen, um ihre Kommunikation, Mitarbeiter und Daten zu schützen. Die Anwendung von KI erfordert eine ausgewogene Herangehensweise, die ihre Stärken optimal nutzt und ihre Grenzen berücksichtigt.

Der Einsatz von KI in der Cybersicherheit wird zweifellos weiter zunehmen, obwohl aktuell noch mehr Fragen als Antworten existieren. Das Potenzial der KI ist enorm, und es bleibt spannend zu sehen, wie weit die menschliche Vorstellungskraft und technologische Innovationen uns in dieser Hinsicht noch bringen werden.

WORK PROTECTED.™

Advanced Email & Collaboration Security

mimecast®