ENJOY SAFER TECHNOLOGY™

Die Medien sind voll von Berichten über die Vorteile, die die Nutzung sogenannter AI/KI (Artificial Intelligence/Künstliche Intelligenz) und Machine Learning/Maschinellem Lernen (ML) für die Internetsecurity mit sich bringen sollen. Zukunftsorientierte Anbieter bringen mehr und mehr KI-basierte Internetsecurity-Produkte auf den Markt und versprechen, diesen mithilfe solcher neuartigen Technologien komplett zu revolutionieren. Tatsächlich stellt der KI/ML-Markt ein interessantes Betätigungsfeld für Organisationen dar – scheinen diese Technologien doch die Möglichkeit zu eröffnen, Malware bereits vor jeglicher Beeinflussung eines Netzwerks zu erkennen und Risiken zu minimieren.

Die Wahrheit ist jedoch, dass derartige Versprechen vom Nutzen der KI irreführend sein können und dass der Hype um diese letztlich negative Auswirkungen auf Unternehmen haben kann.

In diesem Artikel soll diskutiert werden, wie nützlich ML sich bereits seit Jahren im Bereich der Malware-Erkennung erwiesen hat und dass Künstliche Intelligenz im tatsächlichen Wortsinn so nicht existiert. Die Marketingtricks der Next-Gen-Anbieter sorgen lediglich dafür, dass sich die Dinge für Entscheider ungleich komplexer darstellen und es umso schwieriger erscheint, eine widerstandsfähige IT-Security aufzubauen – die jedoch gerade in Zeiten zunehmender Gefahr umso wichtiger ist.

INHALT

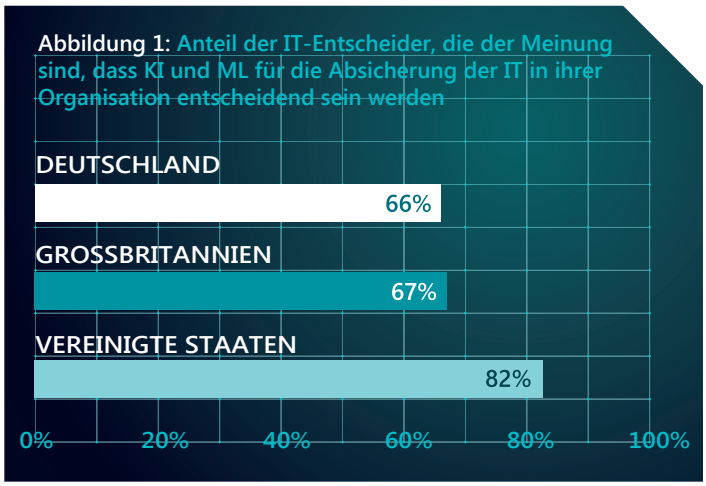
Ein Thema – viele Meinungen

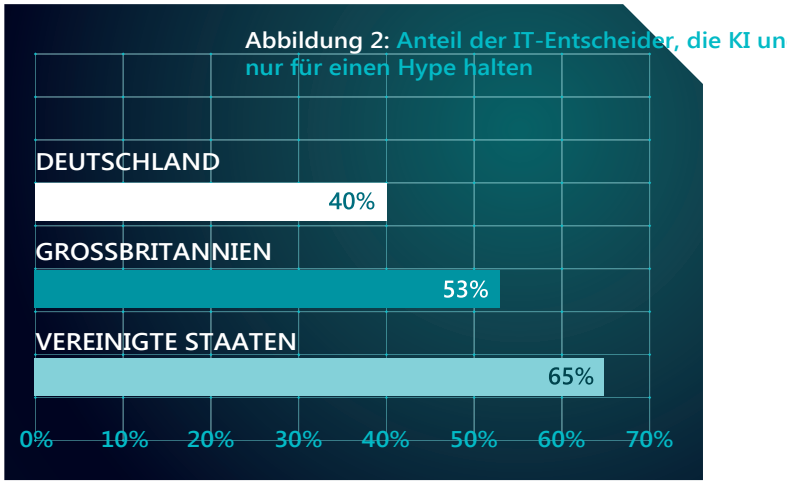
Wir befragten IT-Entscheider in deutschen, britischen und US-amerikanischen Unternehmen zu ihren Einstellungen zu und ihrem Umgang mit KI und ML in Bezug auf die IT-Security in ihrer Organisation. Hierbei wurde vor allem deutlich, dass viele IT-Entscheider in Bezug auf die Konzepte „Maschinelles Lernen" und „Künstliche Intelligenz" ein wenig klares Bild vor Augen haben und dass die Meinungen in Bezug auf entsprechende Technologien sehr weit auseinandergehen.

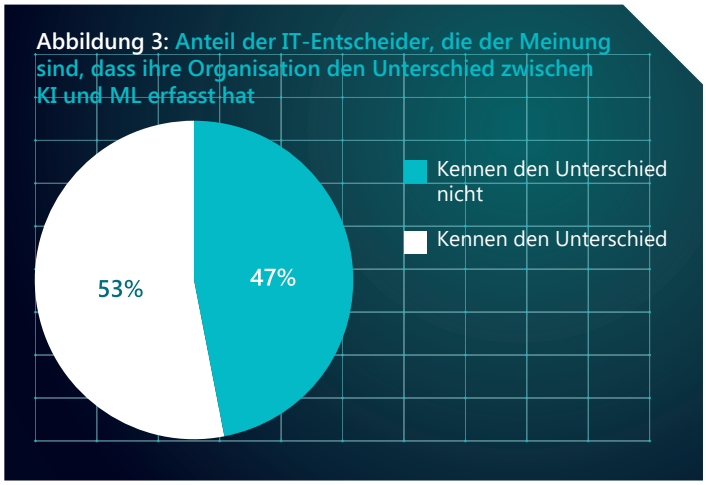
Während ein Großteil der Befragten KI und ML als entscheidende Faktoren zur Lösung bestehender IT-Security-Probleme betrachten, hält ein ebenfalls großer Anteil die gesamte Diskussion für einen zeitlich begrenzten Hype. US-amerikanische Entscheider stellen hierbei einen besonders großen Anteil derjenigen, die in KI und ML einen entscheidenden Erfolgsfaktor für ihre IT-Sicherheit sehen. 82% stimmen zu, dass KI und ML die Lösung für ihre IT-Probleme sein werden, wohingegen in Deutschland der Anteil mit nur 66% um einiges geringer ausfällt (siehe Abbildung 1).

Nichtsdestotrotz sind es ebenfalls mehrfach US-amerikanische Entscheider, die die Diskussionen um KI und ML für ein kurzlebiges Phänomen halten – 65% im Vergleich zu 53% der britischen und 40% der deutschen Befragten (siehe Abbildung 2).

Die Frage drängt sich auf, ob IT-Entscheider sich überhaupt im Klaren darüber sind, was sie glauben sollen. Zudem scheint Verwirrung darüber zu herrschen, worum es sich bei KI und ML genau handelt und worin der Unterschied zwischen beiden Konzepten besteht (siehe Abbildung 3).





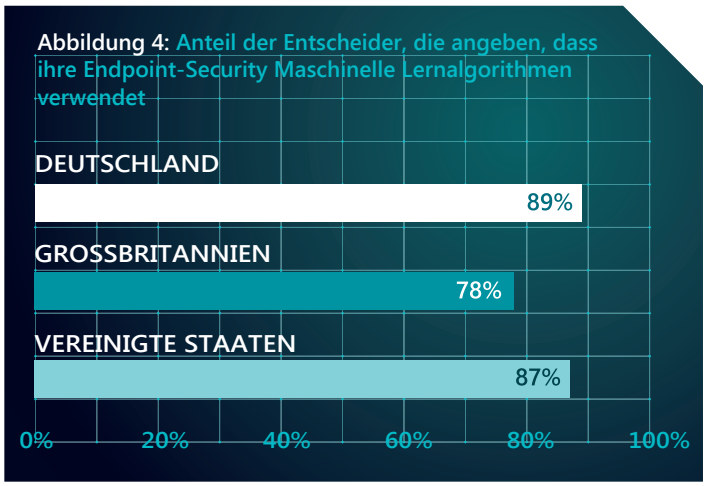


Nichts Neues

Die aktuell in den Medien und im Marketing verwendete Terminologie ist leider häufig irreführend. Vielfach wird der Begriff „Maschinelles Lernen" mit dem der „Künstlichen Intelligenz" gleichgesetzt, während es sich tatsächlich um verschiedene Konzepte handelt. Einfach ausgedrückt, bezeichnet „Künstliche Intelligenz" die Ausführung von Aufgaben durch Maschinen, ohne dass diese vorher hierfür programmiert oder trainiert werden müssen. Im Gegensatz dazu ist „Maschinelles Lernen" die Bezeichnung für das Training von Computern mithilfe von Algorithmen, sodass diese in großen Datenmengen wiederkehrende Strukturen erkennen können. Dies geschieht immer auf Basis von dem Rechner bekannten Regeln und Informationen. ML ist hierbei keineswegs eine neue Technologie; in der IT-Sicherheit ist ihre Anwendung seit den 90er Jahren verbreitet.

Interessanterweise verwendet die Mehrheit der von uns Befragten ML bereits als Teil ihrer IT-Sicherheits-Strategie: 89% der deutschen, 87% der US-amerikanischen und 78% der britischen Befragten geben an, dass ihr Endpoint-Security-Produkt Maschinelle Lernalgorithmen verwendet, um das Unternehmen vor Angriffen zu schützen.

Insbesondere in Hinblick auf die Tatsache, dass Hacker immer neue und komplexere Möglichkeiten finden, um in Netzwerke einzudringen, sind die Marketing-Teams von Next-Gen-Anbietern in der Pflicht, ihre Werbeversprechen eindeutiger zu formulieren. Die Darstellung von KI und ML als heiliger Gral, mit dem jede Form von IT-Sicherheitsfragen geklärt werden kann, macht es umso schwerer informierte Entscheidungen zu treffen und so Unternehmensnetzwerke und -daten zu schützen.



Die aktuell in den Medien und im Marketing verwendete Terminologie ist häufig irreführend

Der Stand heute

Um Missverständnissen vorzubeugen sei hier erwähnt, dass Maschinelles Lernen durchaus ein wichtiges und leistungsfähiges Werkzeug im Kampf gegen Cyberkriminalität darstellt, insbesondere für die Erkennung von Malware.

ML-Algorithmen helfen dabei, potentielle Gefahren zu identifizieren, sodass die betroffenen Nutzer viel schneller zu deren Beseitigung aktiv werden können. „Maschinelles Lernen" bezeichnet hierbei meist Teile der Schutzlösung, welche mit großen, korrekt in „gutartig" und „bösartig" unterteilte Datenmengen trainiert wurden, um so neue und unbekannte Elemente automatisch einer der beiden Kategorien zuzuordnen. Das Training stellt also die Basis, mögliche Gefahren automatisch zu erkennen und zu beseitigen.

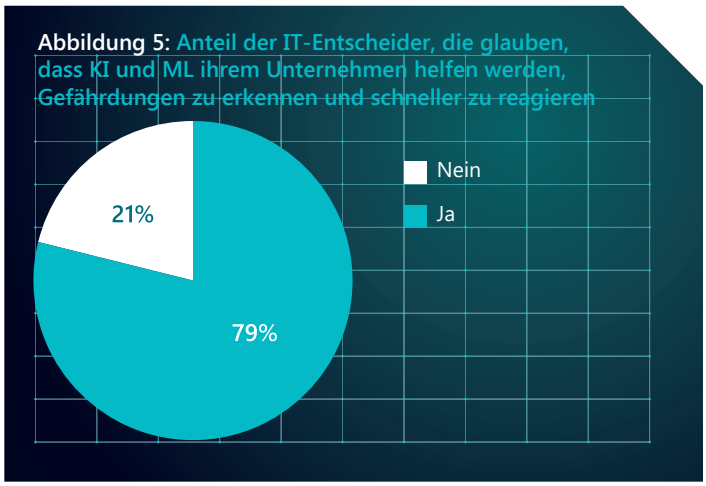
Zusätzlich kann die Erkennungsrate weiter zunehmen, da auch mithilfe von als gut- bzw. bösartig identifizierten neuen Elemente weiter gelernt werden kann. Kaum verwunderlich, dass der Einsatz dieser Technologie für IT-Entscheider sehr attraktiv erscheint.

Jedoch wird durch das Marketing vielfach verschwiegen, dass ML – selbst wenn sie korrekt angewendet wird – auch Schwierigkeiten mit sich bringen kann und keinesfalls grenzenlos in ihrem Anwendungsbereich ist.

1. Überwachtes Training

Für Maschinelles Lernen werden große Mengen an Inputdaten benötigt – wobei jedes Element korrekt kategorisiert sein muss. Das bedeutet, dass bereits im Voraus eine riesige Anzahl von Elementen gegeben sein muss, die in drei Kategorien unterteilt wurde – gut- und bösartig sowie potentiell unerwünscht. Bereits seit über 30 Jahren sammeln wir bei ESET entsprechende Daten um sie dann zu kategorisieren und passende Elemente für das Training unseres ML-Systems auszuwählen.

Anders als vielfach dargestellt ist keineswegs garantiert, dass ein Algorithmus neue Elemente korrekt labelt, nur weil er vorher mit großen Datenmengen gefüttert wurde. Menschliche Verifizierung bleibt zwingend notwendig. Bleibt diese aus, können sich Schneeballeffekte schon durch ein einziges fehlerhaft gelabeltes Element ergeben, da dieses in den Pool der Lerndaten eingeht. Derartige Effekte wiederum können das System derart beeinträchtigen, dass es schließlich komplett versagt.



Einige Next-Gen-Anbieter behaupten scheinbar, dass ihr System vor derartigen Effekten gefeit sei. Derartigen Aussagen zufolge könne ihr Algorithmus „durch simple Mathematik" jedes Element bereits vor dessen Ausführung als gut- oder bösartig identifizieren. Unserem Kenntnisstand nach sind derartige Aussagen jedoch nicht haltbar.

Der folgende Absatz soll helfen, Unsicherheiten auf Seiten der IT-Entscheider zu verringern.

2. „Simple Mathematik" reicht nicht aus

Selbst eine fehlerfrei agierende Maschine ist nicht in der Lage zu entscheiden, ob ein ihr unbekanntes Element in der Zukunft zu unerwünschtem Verhalten führen wird.[1] Wenn ein Next-Gen Anbieter also behauptet, dass sein Algorithmus in der Lage sei, jedes Element vor dessen Ausführung zu kategorisieren, müsste dieser präventiv eine Vielzahl nicht kategorisierbarer Daten blockieren. Die IT-Abteilungen der Unternehmen würden mit falsch positiv als bösartig identifizierten Daten überschwemmt.

Selbstverständlich führt nicht jeder Fehlalarm zum Zusammenbruch der gesamten IT-Infrastruktur. Nichtsdestotrotz kann das reibungslose Funktionieren von Unternehmensabläufen empfindlich gestört werden – was letztlich noch schwerwiegendere Auswirkungen haben kann.

Der menschliche Faktor bleibt zentral. ML-Systeme müssen in der Lage sein, Mitarbeiter über nicht anhand gelernter Daten kategorisierbare Elemente zu informieren und um eine Entscheidung zu bitten.

[1]Bekannt als das „Halteproblem" der Theoretischen Informatik und bewiesen durch den englischen Mathematiker und Kryptoanalytiker Alan Turing, welcher im Zweiten Weltkrieg den Enigma-Verschlüsselungsmechanismus knackte.

3. Hacker brechen die Regeln – Maschinen nicht

Malware entwickelt sich stets weiter – sind doch auch Black-Hat-Hacker stets darum bemüht, dazuzulernen. Unternehmen sind gefragt, dieser Entwicklung zu folgen, um sich und die Mitarbeiter zu schützen. Ein typisches Werbeversprechen von Next-Gen-Anbietern ist, maschinelles Lernen als die Lösung anzupreisen, die mithilfe von mathematischen Modellen in der Lage ist, jede neue Variante von Schadsoftware zu erkennen. Leider hat jedoch jeder ML-Algorithmus, so „klug" er auch sein mag, einen begrenzten Fokus und lernt, wie oben erläutert, anhand eines spezifischen Datensets und festgelegter Regeln.

Angreifer spielen jedoch nicht nach den Regeln. Schlimmer noch: Sie können und haben in der Vergangenheit oftmals das gesamte Spielfeld umgestaltet.

Im Gegensatz zur Maschine ist der (menschliche) Hacker in der Lage, aus Kontexten zu lernen und kreativ zu agieren – etwas, zu dem kein noch so weit entwickelter Algorithmus fähig ist. Zusätzlich sind Autoren von Malware in der Lage, den tatsächlichen Zweck ihres Codes geschickt zu verschleiern, sodass sie für eine Maschine, die lediglich einem Algorithmus folgt, wie gutartige Software erscheint.

So kann ein Angreifer beispielsweise bösartigen Code in einzelnen Pixeln einer harmlosen Bilddatei verstecken. Ebenso ist es möglich, Codeschnipsel bösartiger Software in einzelnen Dateien zu verstecken. Für den Algorithmus erscheint jede Datei „sauber" – erst wenn die einzelnen Elemente an einem Endpoint oder in einem Netzwerk zusammengefügt werden, zeigt sich das schädliche Verhalten. Ist der ML-Algorithmus nicht in der Lage, hinter diese „Masken" zu blicken, fällt er im Zweifel eine falsche Entscheidung und kategorisiert Schadsoftware als gutartig – ein potentiell hochgefährlicher Fehler.

Es ist also unabdingbar, dass Mensch und Maschine zusammenarbeiten, um aktiv schädliche Aktivitäten zu verhindern und entsprechende Software zu beseitigen.

Angreifer spielen nicht nach den Regeln. Schlimmer noch – sie gestalten ohne Vorwarnung das gesamte Spielfeld um

Welchen Einfluss haben KI und ML auf das Spiel?

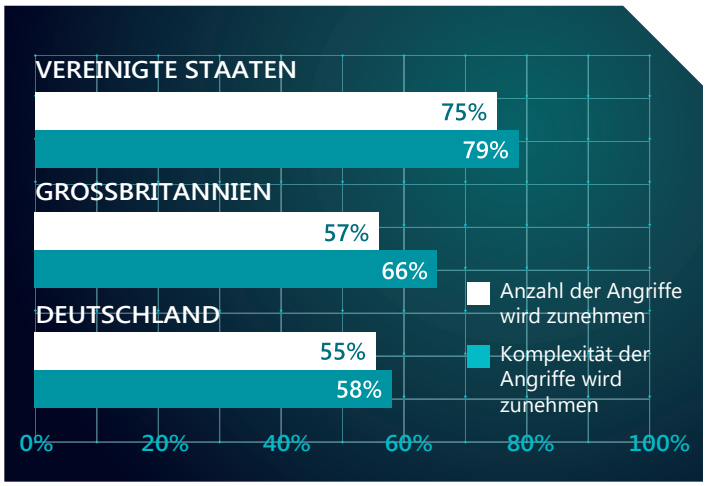
Keine Frage: Maschinelles Lernen, stets unterstützt durch menschliche Akteure, ist ein wertvolles Werkzeug zur Verteidigung eines Unternehmens. Dennoch warnen Experten und Forscher davor, dass auch Angreifer ML zu ihren Gunsten einsetzen um ihre Software zu verbessern oder Aktivitäten zu automatisieren. Die Kehrseite technologischen Fortschritts, welcher im Kampf gegen Cyberkriminalität wertvolle Hilfe bietet, ist, dass entsprechende Entwicklungen potentiell auch von Kriminellen eingesetzt werden können.

Die Sorge von IT-Entscheidern, dass Angreifer zunehmend KI für ihre Zwecke nutzen werden, erscheint daher nicht unbegründet. Unsere Befragungen zeigten allerdings, dass diese Sorge je nach Region unterschiedlich ausgeprägt ist. Für uns stellte sich daher die Frage, wie informiert sich IT-Entscheider fühlen, wenn es um die Nutzung von KI durch Angreifer geht.

US-amerikanische IT-Entscheider beispielsweise erscheinen wesentlich besorgter darüber, dass die Nutzung von KI im Schadsoftware-Bereich zu einer Zunahme von Angriffen führen wird. Die Entscheider vermuten zudem, dass KI die Angriffe und entsprechend deren Abwehr komplexer machen wird. Vergleichsweise wenige IT-Entscheider in Großbritannien und Deutschland glauben, dass der Einfluss von KI auf die Art der Angriffe, denen ihr Unternehmen ausgesetzt sein wird, besonders groß ausfallen wird.

Es ist jedoch davon auszugehen, dass Hacker ML nutzen könnten, um potentielle Opfer auszuspähen. So ließe sich beispielsweise in Erfahrung bringen, ob das Opfer eine virtuelle Maschine nutzt oder ob sein Rechner unter Beobachtung durch einen Malware-Analysten steht. Weiterhin ergibt sich die Frage, ob bereits existierende Angriffstypen in der nahen Zukunft zunehmen könnten.

ML-Systeme sind einfach skalierbar und arbeiten sehr effizient – ebenso wie die potentiell darauf aufbauenden KIs. Es erscheint also nur logisch anzunehmen, dass es zunehmend einfacher werden wird, kostengünstig vormals arbeitsintensive Cyberattacken durchzuführen. Darunter fallen zum Beispiel Angriffe auf Basis von Social Engineering wie das sogenannte Spear Phishing. Indem nicht-triviale Aufgaben, welche vor dem Angriff notwendig sind, durch KI-Systeme automatisch ausgeführt werden, wird es für Angreifer einfacher und kosteneffizienter, entsprechende Attacken zu fahren. Zusätzlich können realistisch wirkende Chatbots „Freunde" imitieren und so großflächige Spear Phishing Attacken auf einer zusätzlichen Ebene unterstützen.



Nicht zuletzt bieten Schwachstellen in den ML-Systemen selbst mögliche Angriffspunkte. So ist es beispielsweise möglich, Daten zu verunreinigen, um so herauszufinden, wie ein Lernalgorithmus im Detail arbeitet oder woher er seine Ausgangsdaten erhält. Hacker sind so nicht nur in der Lage, Daten abzugreifen, sondern können auch Einfluss darauf nehmen, welche Elemente als „gut" oder „böse" gelabelt werden.

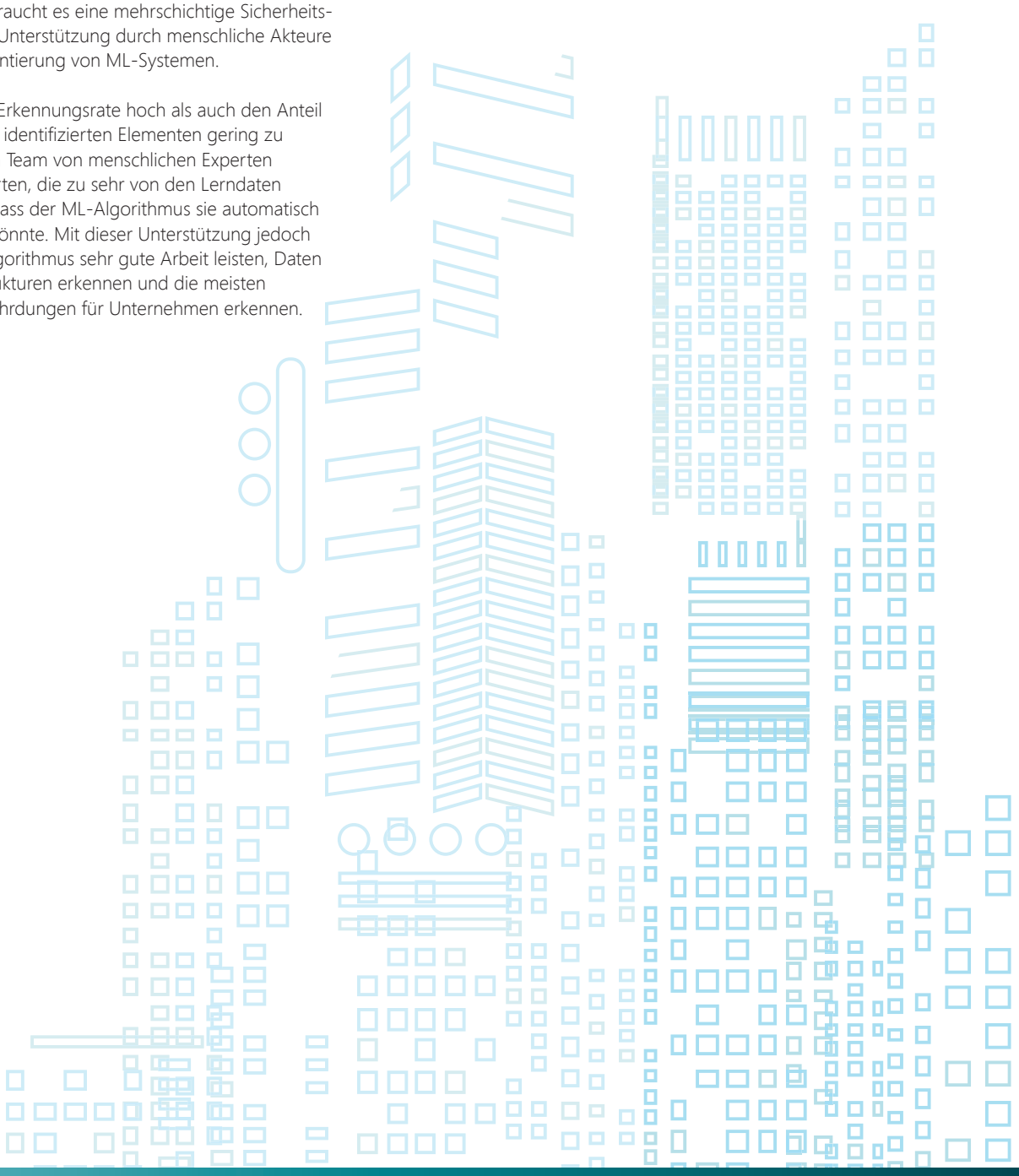
Mensch und Maschine

Die Welt der Internetsicherheit ist stets im Wandel begriffen – es ist also schlichtweg unmöglich, die perfekte Absicherung gegenüber den daraus erwachsenden Risiken zu finden, wenn diese sich lediglich auf ML-Algorithmen stützt. Fußt die Internetsecurity eines Unternehmens allein auf Maschinellem Lernen, öffnet jeder erfolgreiche Angriff durch jedwede Schadsoftware Ihre Endpoints für eine ganze Armee von Gefahren.

Entsprechend braucht es eine mehrschichtige Sicherheitslösung und die Unterstützung durch menschliche Akteure für die Implementierung von ML-Systemen.

Um sowohl die Erkennungsrate hoch als auch den Anteil an falsch positiv identifizierten Elementen gering zu halten, muss ein Team von menschlichen Experten Elemente bewerten, die zu sehr von den Lerndaten abweichen als dass der ML-Algorithmus sie automatisch kategorisieren könnte. Mit dieser Unterstützung jedoch kann ein ML-Algorithmus sehr gute Arbeit leisten, Daten analysieren, Strukturen erkennen und die meisten möglichen Gefährdungen für Unternehmen erkennen.

Die Automatisierung dieses Prozesses beschleunigt die Sicherheitslösung und hilft somit Ihrem IT-Team, die zunehmende Anzahl von Elementen, mit denen dieses täglich konfrontiert ist, zu kategorisieren.



Was steckt hinter dem Hype?

Auch wenn der Gedanke, dass es einen „heiligen Gral" gibt, der alle Internetsecurity-Probleme auf einmal löst, schön sein mag, entspricht er schlichtweg nicht der Realität. Egal, was die Hochglanzprospekte der Marketingabteilungen versprechen mögen – tatsächliche künstliche Intelligenz ist noch immer Science Fiction und Maschinelles Lernen ist noch nicht weit genug entwickelt, um als einzige Verteidigungslinie zwischen Ihnen und den Angreifern zu genügen.

Blumige Versprechen führen lediglich dazu, dass IT-Entscheider den Überblick verlieren und potentiell Unternehmen noch stärker gefährden als dies sowieso der Fall ist. In der heutigen Unternehmenswelt erscheint es nicht angeraten, sich allein auf eine Technologie zu verlassen, um ihre Netzwerke und Daten zu schützen. Unternehmen müssen sich der Einschränkungen von ML bewusst sein um sich entsprechend abzusichern.

Für den Aufbau einer zuverlässigen und widerstandsfähigen Internetsecurity-Lösung müssen alle Herausforderungen, denen ihr Unternehmen ausgesetzt ist, genau verstanden werden, um im Anschluss Lösungen für deren Bearbeitung zu entwickeln, die den spezifischen Anforderungen Ihres Unternehmens entsprechen. Jedes Unternehmen ist einzigartig und eine Universallösung kann den sich daraus ergebenen Ansprüchen nicht gerecht werden. Aus mehreren Schichten bestehende Lösungen, in Kombination mit talentierten und gut ausgebildeten Teams, werden die einzige Möglichkeit sein, den Hackern immer den entscheidenden Schritt voraus zu sein.

Das vergangene Jahrzehnt hat uns eines gezeigt: Vor allem im Cyberspace gibt es Herausforderungen, die sich nicht auf die Schnelle bewältigen lassen, will man zu einer nachhaltigen Lösung gelangen, die mit der sich ständig verändernden Umwelt Schritt halten kann. Statt die Versprechen, die in Bezug auf die Künstliche Intelligenz oder Maschinellem Lernen gemacht werden, als „Heiligen Gral" zu betrachten, muss über den Hype hinausgeblickt und sich darauf konzentriert werden, was das Richtige für Ihr Unternehmen ist. Welches sind die verwundbarsten Punkte und wie kann man diese absichern, sodass sie nicht zum Einfallstor für Angreifer werden? Wissen Sie, wo die sensibelsten Daten in Ihrem Unternehmen liegen und wie diese geschützt werden?

Maschinelles Lernen kann nicht die einzige Antwort auf derartige Fragen sein. Natürlich ist es zwingend notwendig, Malware aufzuspüren – es darf jedoch nicht vergessen werden, die Erwartungen der IT-Entscheider mit dem abzugleichen, was die Technologie leisten kann. Jede Minute kann den Spielverlauf von Grund auf ändern. Ihre Aufgabe ist es, im Blick zu behalten, dass Ihre Verteidigung steht, um möglichst jede Art von Angreifer fernzuhalten.

Egal, was die Hochglanzprospekte der Marketingabteilungen versprechen mögen – tatsächliche künstliche Intelligenz ist noch immer Science Fiction. Auch Maschinelles Lernen ist noch nicht weit genug entwickelt, um als einzige Verteidigungslinie zwischen Unternehmen und Angreifern zu genügen