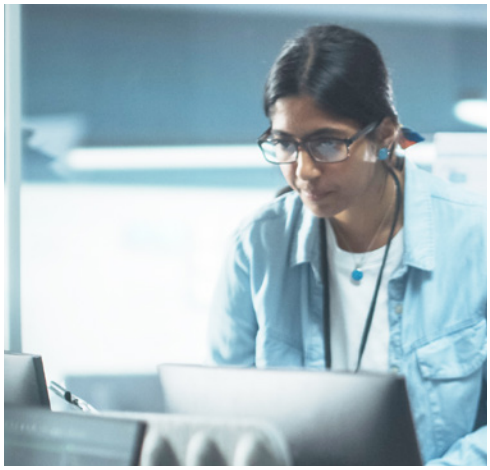
KI und Automation bei der Cybersicherheit

Wie Führungskräfte mit der Kombination aus Technologie und Talent Erfolge erzielen

IBM

So kann IBM helfen

IBM Security wendet KI-Technologien wie maschinelles Lernen und die Verarbeitung natürlicher Sprache an, damit Analytiker für sicherheitsbezogene Vorgänge den Bedrohungen immer einen Schritt voraus sind und dabei Reaktionszeiten und Kosten reduzieren. Weitere Informationen finden Sie unter: ibm.com/de-de/security/artificial-intelligence.



Die wichtigsten Erkenntnisse

Durch die Auslagerung von Routinearbeiten können Teams für Cybersicherheit durch KI plus Automation ihr Fachwissen gezielt dort einsetzen, wo es am dringendsten benötigt wird.

Tempo und schiere Menge von Sicherheitsvorfällen verlangen einen neuen operativen Ansatz

KI plus Automation erhöht Transparenz und Produktivität bei allen sicherheitsbezogenen Vorgängen. Erfolgreiche KI-Adopter überwachen 95 % der Netzwerkkommunikation und verkürzen die Zeit zur Erkennung von Sicherheitsvorfällen um ein Drittel.

KI bei der Sicherheit gewinnt an Zugkraft

Führungskräfte berichten von einer allgemein gestiegenen Akzeptanz der KI bei sicherheitsbezogenen Vorgängen, wobei 93 % der Unternehmen für diesen Zweck bereits KI nutzen oder über eine Implementierung nachdenken.

Wer schon früh KI im Sicherheitsbereich eingeführt hat, verbessert seine Leistungskennzahlen

Top-Performer steigerten die Sicherheitsrendite um mind. 40 % und senkten die Kosten von Datenschutzverletzungen um mind. 18 %. Die freigesetzten Mittel wurden in Personal für Cybersicherheit investiert.

Schnelle Veränderungen machen Cyberangriffe wahrscheinlicher

Moderne digitale Abläufe sind wertsteigernd, schaffen aber auch neue Schwachstellen.

Im Jahr 2021 gab es einen Anstieg der Cybersicherheitsbedrohungen, die unter anderem auf Colonial Pipeline und andere Unternehmen der Wasserwirtschaft in den USA abzielten.[1] Laut einer aktuellen Studie hat Ransomware zwischen 2020 und 2021 um 105 % zugenommen. Am stärksten war die Fertigungsbranche betroffen.[2] Im vergangenen Jahr ereigneten sich einige der bislang schwerwiegendsten Angriffe auf Lieferketten. Die Attacken auf SolarWinds und Microsoft Exchange Server sowie die Schwachstellen bei Apache Log4j machten Schlagzeilen und sensibilisierten – und alarmierten – Wirtschaftsführer und ihre Kunden.[3]

Was unterscheidet die heutige Situation so grundlegend von früher?

Kurz gesagt: Die Pandemie hat die digitale Transformation beschleunigt und ihre Chancen verstärkt – aber auch ihre Risiken.[4] Die Zahl der Beschäftigten im Homeoffice ist deutlich gestiegen. Mehr Cloudbenutzer. Mehr Cloud-Services. Die Integration wesentlicher Systeme mithilfe von Drittanbietern. Eine beeindruckende Anzahl von Edge-Geräten, die IoT-Daten an die Cloud weiterleiten. Alles ist miteinander verbunden und greift ineinander, bietet hochentwickelte Konnektivität und schafft Werte in einer Geschwindigkeit und Größenordnung, die noch vor wenigen Jahren unmöglich waren.

Die Vorteile der Innovation haben jedoch auch ihren Preis: Neue Geräte, neue Partner und neue Integrationen machen Unternehmen offener und verwundbarer, da sich ihre Angriffsfläche radikal vergrößern kann. Es gibt immer neue Bedrohungsvektoren – vom unwissenden Lieferanten bis hin zu verärgerten Beschäftigten, von der Datenexfiltration über Denial-of-Service-Attacken bis hin zu Ransomware. Erschwerend kommt hinzu, dass Bedrohungsakteure die eigenen Taktiken, Techniken und Verfahren fortlaufend weiterentwickeln – sie setzen künstliche Intelligenz (KI) und Automation ein, um nach Schwachstellen zu suchen und effizientere Angriffe zu starten (siehe Abb. 1).[5]

Das Ergebnis zeichnet für viele Führungskräfte ein ernüchterndes Bild: Der heutige hoch verfügbare Digitalbetrieb steigert zwar den Unternehmenswert, erzeugt aber auch neue Schwachstellen. Bei aller Effizienz, die durch moderne Technologie ermöglicht wird, erkennen viele Unternehmen allmählich, dass ihr Digitalisierungsprofil auch voller Komplexitäten und Unbekannten steckt. Hinzu kommt, dass unterbesetzte Sicherheitsteams mit zu vielen Daten aus heterogenen Quellen und einer Fülle an Tools überschüttet werden, es ihnen aber oft an entscheidenden Informationen fehlt. Diese Herausforderungen können schnell die Fähigkeiten selbst der fachkundigsten Sicherheitsexperten und die Kapazitäten großer fähiger Teams für Cybersicherheit übersteigen.

Die aktuelle operative Realität erfordert einen neuen Ansatz

Um ihre Teams auf Erfolgskurs zu bringen, müssen Führungskräfte im Bereich Cybersicherheit stärker präventiv und proaktiv agieren, um zentrale Geschäftsabläufe zu schützen. Unsere Untersuchungen lassen vermuten, dass sich immer mehr Unternehmen für einen zukunftsorientierten Ansatz beim Bedrohungsmanagement entscheiden und KI-basierte Automatisierung einsetzen, um bessere Erkenntnisse, Produktivität und Skaleneffekte zu erlangen.

Es gibt vier entscheidende Möglichkeiten, wie KI-Technologien die Sicherheit transformieren können:

- Funktionen des maschinellen Lernens helfen bei der Erkennung von Mustern, der Bestandsaufnahme neuer Anlagen und Services sowie bei der Verfeinerung von KI-Modellen.
- Reasoning-Funktionen unterstützen die Datenanalyse, verbessern die Modellierung von Szenarien und antizipieren neue Angriffsvektoren.
- Die Verarbeitung natürlicher Sprache kann zur Auswertung von Textdatenquellen, zur Verbesserung von Bedrohungsinformationen und zur Anreicherung von Wissensressourcen eingesetzt werden.
- Automation kann zum Orchestrieren zeitintensiver Aufgaben, zu kürzeren Reaktionszeiten und zu weniger Arbeitsbelastung für Analytiker beitragen.

Zusammengenommen besitzen diese Funktionen das Potenzial, den Sicherheitsbetrieb zu transformieren.

In diesem Bericht zeigen wir, wie diese Kombination aus KI und Automation eine wesentliche Leistungsverbesserung ermöglichen kann – ob bei Geschwindigkeit, Erkenntnissen oder Flexibilität. Mithilfe dieser Leistungsverbesserungen können Cybersicherheitsteams sich auf die wirklich wichtigen Dinge konzentrieren: proaktiv vor Bedrohungen schützen, sie erkennen, auf sie reagieren und die nachfolgende Wiederherstellung bei gleichzeitiger Reduzierung von Kosten und Komplexität.

ABB. 1

Radikale Veränderungen im Sicherheitsumfeld

Sicherheitsteams stehen vor neuen Herausforderungen

Kapitel 1

KI bei der Sicherheit gewinnt schnell an Zugkraft

Das IBM Institute for Business Value (IBV) wollte verstehen, wie KI zur Unterstützung von Sicherheitsabläufen eingesetzt wird und ihre Auswirkungen auf die Cybersicherheitsleistung quantifizieren. Dazu hat es in Zusammenarbeit mit dem APQC (American Productivity and Quality Center) 1.000 Führungskräfte befragt, die die Gesamtverantwortung für die Cybersicherheit in den Bereichen IT und Betriebstechnologie ihres Unternehmens tragen. Sie repräsentieren 16 Branchen und 5 Weltregionen (siehe Studien- und Forschungsmethodik auf Seite 32).

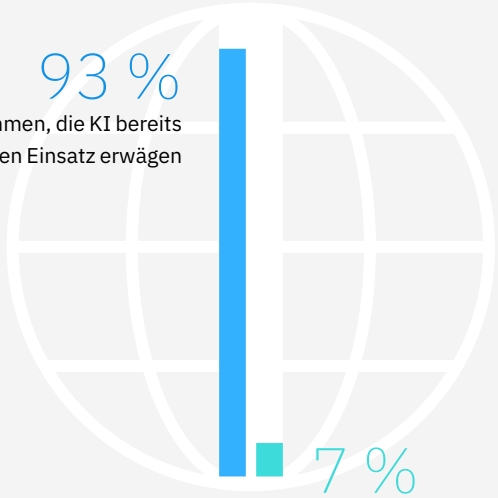
Wir haben die Befragten gebeten, Angaben zur Leistung der Sicherheitsfunktion ihres Unternehmens zu machen und das Ausmaß, in dem KI und Automation von ihnen zur Bewältigung von Cyberrisiken und Compliance-Aspekten genutzt werden, zu nennen. Sie beschrieben auch, wie sie KI zur Unterstützung von sicherheitsbezogenen Vorgängen zum Schutz und zur Prävention von Bedrohungen sowie für Prozesse zur Bedrohungserkennung und -reaktion einsetzen. Wir haben mithilfe dieser Erkenntnisse die Auswirkungen von KI auf die Cybersicherheitsleistung bewertet, wobei der Schwerpunkt auf Produktivität, Resilienz und die damit verbundenen geschäftlichen Vorteile gelegt wurde.

Insgesamt konnten wir feststellen, dass die Mehrheit der Unternehmen – weltweit und branchenübergreifend – die Einführung von KI plus Automation in ihren Sicherheitsfunktionen bereits umsetzt oder in Erwägung zieht. 64 % der Befragten haben KI für Sicherheitsfunktionen in mindestens einem der Prozesse bei einem Sicherheitsvorfall implementiert und 29 % ziehen dies in Betracht. Mit anderen Worten: KI bei der Sicherheit könnte bald ein Quasi-Standard für Sicherheitslösungen sein (siehe Abb. 2). Die verbleibenden 7 %, die den Einsatz von KI plus Automation im Bereich Sicherheit nicht in Betracht ziehen, bringen sich in eine prekäre Lage und haben höchstwahrscheinlich Schwierigkeiten, mit dem Tempo und der schieren Menge von Sicherheitsvorfällen Schritt zu halten.

ABB. 2

Allgemeine Akzeptanz

Nur eine kleine Gruppe erwägt keinen Einsatz von KI in ihren sicherheitsbezogenen Vorgängen



93 %
Unternehmen, die KI bereits nutzen oder den Einsatz erwägen

7 %
Unternehmen, die keinen Einsatz von KI erwägen

Wir bezeichnen die 64 %, die derzeit KI-Sicherheitslösungen erproben, implementieren, betreiben oder optimieren, als „KI-Adopter“. Obwohl die Anwendung von KI im Bereich Sicherheit noch in den Kinderschuhen steckt – die meisten nutzen sie erst seit weniger als 2 Jahren im Geschäftsalltag – wird mit einer schnell steigenden Akzeptanz gerechnet. Was die Art der Nutzung von KI betrifft, wird der Prozentsatz der KI-Adopter, die sie unterstützend bei Schutz und Prävention von Bedrohungen einsetzen, in den nächsten drei Jahren im Durchschnitt um etwa 40 % steigen, wobei ein gleiches Wachstum für die Bereiche Bedrohungserkennung und -reaktion erwartet wird.

Diese zu erwartende beschleunigte Akzeptanz von KI im Sicherheitsbereich stimmt mit den Ergebnissen anderer Studien überein. Eine kürzlich durchgeführte Studie prognostiziert, dass die Ausgaben für KI im Zusammenhang mit der Cybersicherheit bis 2027 jährlich um durchschnittlich 24 % zunehmen und einen Marktwert von 46 Mrd. USD erreichen.[6]

Technologie plus Talent ermöglicht positive Ergebnisse

KI-Adopter begreifen sofort, wie erfolgreich sich KI-basierte Erkenntnisse und Automation sowie die Identifizierungs- und Reaktionsfähigkeit ihrer Sicherheitsexperten ergänzen. Sie beobachten, dass KI-Sicherheitssysteme genau wie ein erfahrener Sicherheitsanalytiker anomales Verhalten erkennen, Schwachstellen systematisch bewerten und Abweichungen kennzeichnen, die auf neue Bedrohungen hinweisen könnten. 65 % der KI-Adopter geben an, dass diese Anwendung der KI sich sehr positiv auf ihre sicherheitsbezogenen Vorgängen ausgewirkt hat (siehe Abb. 3 auf Seite 7). Doch im Gegensatz zu einem menschlichen Analytiker nutzt KI maschinelles Lernen und Automation, um der unerbittlichen Geschwindigkeit und der Größenordnung hybrider Multi-Cloud-Vorgänge gerecht zu werden – mit einer Konsistenz und Tiefe, die selbst die Fähigkeiten der begabtesten und qualifiziertesten Sicherheitsexperten weit übersteigt. (Siehe Perspektive „Was macht KI-Sicherheit so wirkungsvoll?“)

Mit KI werden beispielsweise normale Verhaltensweisen nachverfolgt und automatisch Modelle erstellt. Dazu kennzeichnen KI-Sicherheitslösungen Abweichungen vom erwarteten Verhalten und analysieren das Bedrohungspotenzial möglicher Ausnahmen. Eine Verbesserung der Bedrohungsreaktion zur automatischen Eindämmung und optimierten Geschäftskontinuität wird von 57 % der KI-Adopter als sehr wichtig eingestuft. KI-Sicherheitslösungen verstehen anomale Aktivitäten im Kontext und können so feststellen, welche Sicherheitsrichtlinien und -kontrollen gefährdet sind, eine Warnmeldung um relevante Einblicke ergänzen und dann vorgeschriebene Abhilfemaßnahmen einleiten.

Ein solcher „Cyberassistent“ für menschliche Experten unterstreicht einen der wichtigsten Vorteile von KI-Sicherheit: die Entlastung von Sicherheitsteams angesichts des anhaltenden Fachkräftemangels. 60 % der KI-Adopter geben an, dass die automatische Datenanreicherung und eine zweite Sicht auf die Vorfälle, durch die die Analytiker effizienter arbeiten können, von großem Nutzen für ihre Sicherheitsfunktionen sind. Da KI-Bedrohungsmodelle weitaus mehr Vorfälle über längere Zeiträume und eine Vielzahl von Betriebsbedingungen hinweg referenzieren, können sie Expertenfähigkeiten bei genau den Bedrohungen einsetzen, die menschlichen Analytikern wahrscheinlich entgangen wären.

Angereichert durch KI-generierte Erkenntnisse können KI-basierte Automatisierungsfunktionen Bedrohungen nach Benutzer, Gerät oder Standort isolieren und dann geeignete Benachrichtigungs- und Eskalationsmaßnahmen einleiten, während menschliche Experten entscheiden, wie eine Bedrohung am besten untersucht und behoben wird. Bei Unternehmen, die diese Fähigkeiten entwickelt haben, können sich die Cybersicherheitsanalytiker auf das wirklich Wichtige konzentrieren: sich die nötigen Fertigkeiten und das Fachwissen für komplexe Probleme aneignen, die menschliches Urteilsvermögen erfordern.

Perspektive

Was macht KI-Sicherheit so effektiv?

KI-Sicherheit und Automation spielen bei der Verteidigung wachsender Angriffsflächen und der Reaktion auf die enorme Zunahme von Sicherheitsereignissen eine immer wichtigere Rolle. Was macht KI so wirkungsvoll? Kurz gesagt, ist es die Kombination aus iterativem maschinellem Lernen und der Optimierung (dem „Verfeinern“) des Analysemodells.

Beim Verfeinern geht es um die Leistungsoptimierung eines Analysemodells, ohne es zu sehr von Variablen abhängig zu machen, die sich situationsabhängig ändern können. Hinter den Kulissen verwenden Algorithmen des maschinellen Lernens unzählige Beispiele, um Muster zu erkennen und zu lernen, wie am besten auf verschiedene Variablen reagiert werden sollte. Dieser Trainingsprozess ist der Schlüssel zur Leistungsverbesserung des KI-Modells.

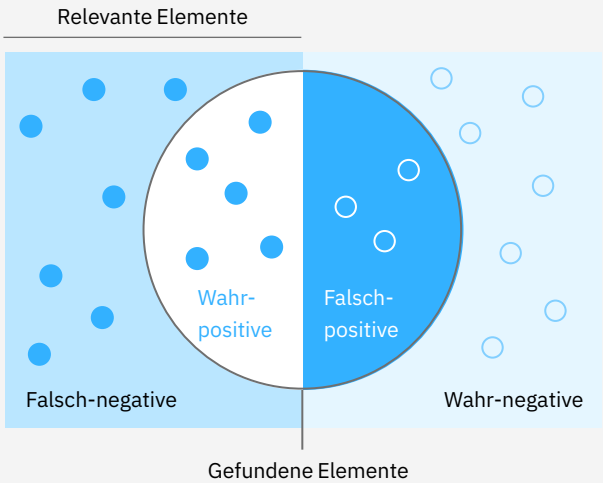
Durch maschinelles Lernen werden Genauigkeit und Trefferquote von Modellen gesteigert. Sie wirken dem Ermüden der menschlichen Aufmerksamkeit gegenüber Alarmen entgegen, weil sie tatsächliche Sicherheitsbedrohungen – wahr-positive Meldungen – von gewöhnlichen Vorfällen – falsch-positiven und wahr-negativen Meldungen – abgrenzen (siehe Abbildung). Diese Lösungen helfen bei der Vorauswahl der meisten Sicherheitsvorfälle, reichern sie mit kontextbezogenen Daten an und unterstützen die Analytiker dann bei Auswertung und Untersuchung. Wenn die KI sozusagen die Spreu vom Weizen trennt, können sich die Analytiker auf die tatsächlichen Bedrohungen konzentrieren, die das größte Risiko darstellen.

Wie viele der gefundenen Elemente sind relevant?

Genauigkeit = $\frac{\text{◐}}{\text{◑}}$

Wie viele der relevanten Elemente werden gefunden?

Trefferquote = $\frac{\text{◐}}{\text{◖}}$



Quelle: Nach https://en.wikipedia.org/wiki/F-score

KI plus Automation schafft letztlich bereicherndere Arbeitsumgebungen, weil die Analytiker sich wieder auf komplexe Probleme konzentrieren können, die menschliches Urteilsvermögen erfordern.

Da KI sowohl strukturierte als auch unstrukturierte Datenquellen analysiert – indem interne und externe Daten mit Threat Intelligence Services und Open Source Intelligence (OSINT) synthetisiert werden – kann sie ein umfassendes Bild der Situationsvariablen und Bedrohungen im Kontext liefern. Darum können Cybersicherheitsanalytiker Vorfälle schneller erkennen, auf sie reagieren und ihre Folgen beheben.

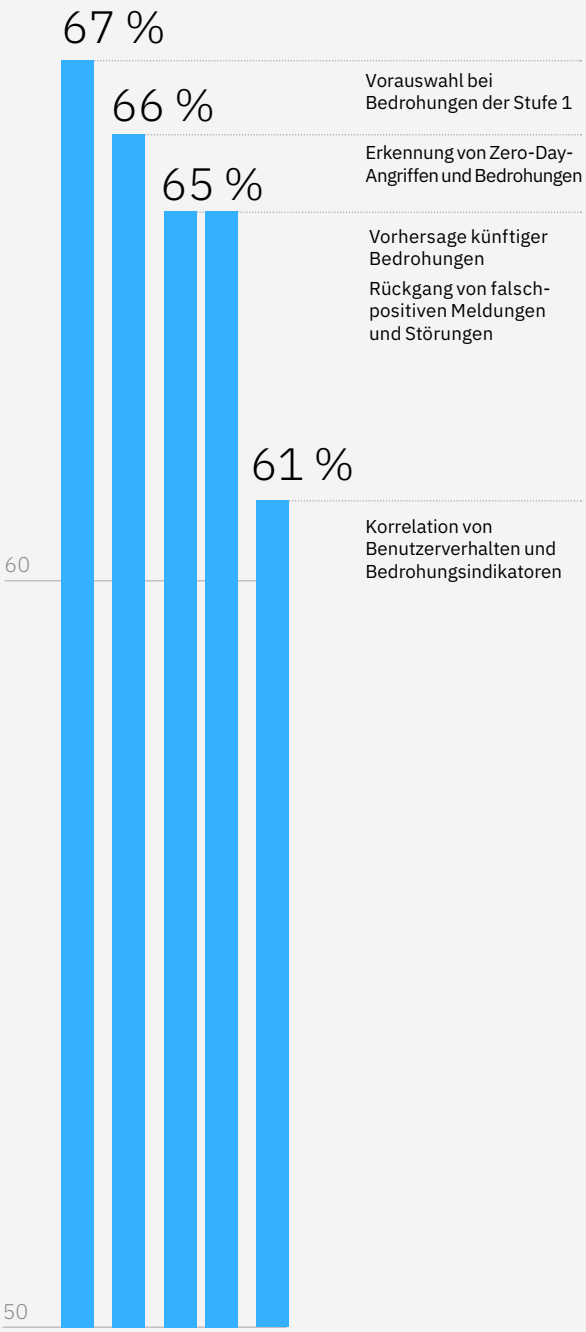
Dank effizienterer Eskalations-, Überprüfungs- und Behebungsverfahren verbessert KI die Sicherheitsgovernance und -konformität. Durch die Automatisierung sich wiederholender, zeitraubender Aufgaben kann KI Ermüdungserscheinungen entgegenwirken, damit die Analytiker in kürzerer Zeit und mit weniger Fehlern bessere und fundiertere Entscheidungen treffen. Durch das Weiterleiten der schieren Vorfallsmenge an sicherheitsbezogene KI- und Automatisierungslösungen können Führungskräfte ihre Analytiker und deren stark nachgefragtes Expertenwissen bestmöglich nutzen. Daraus resultiert ein bereichernderes, befriedigenderes Arbeitsumfeld – etwas, das angesichts des Fachkräftemangels im Bereich Cybersicherheit einen wichtigen Unterschied bewirken kann.

KI-Adopter, die erfolgreich KI-Erkenntnisse und Automation mit dem Fachwissen ihrer Beschäftigten verknüpft haben, beschreiben zusätzliche positive Auswirkungen von KI-Anwendungen auf die Sicherheitsergebnisse (siehe Abb. 3). 67 % geben an, dass durch die effektivere Vorauswahl von Bedrohungen der Stufe 1 weniger Kosten und Zeitaufwand für die Basiserkennung anfallen. Weitere 65 % bestätigen, dass durch die Reduzierung von falsch-positiven Meldungen und nicht sicherheitsrelevanten Störungen weniger Untersuchungen durch menschliche Analytiker anfallen. Und bei 65 % der Befragten erleichtert der Einsatz von Verhaltensanalysen die Vorhersage zukünftiger Bedrohungen, was ein wichtiger Schritt zu mehr Proaktivität ist.

ABB. 3

Vorteile von KI

KI-Adopter verbessern die Leistung mithilfe von KI-Lösungen für kritische Funktionen



Frage: Welche der folgenden KI-Anwendungen hat sich am meisten auf Ihre sicherheitsbezogenen Vorgänge ausgewirkt? (Wählen Sie die 5 wichtigsten aus.)

KI-Investitionen zahlen sich aus

Eine Quelle schätzt, dass die Cyberkriminalität die Weltwirtschaft ab 2025 jährlich bereits durchschnittlich 10,5 Bio. USD kosten wird.[7] Laut des Jahresberichts von Ponemon Institute und IBM, „Cost of a Data Breach“, erreichten die durchschnittlichen Kosten einer Datenschutzverletzung 2021 einen historischen Höchststand, während die Zahl der Datenschutzverletzungen um erschreckende 68 % anstieg, was die Kosten noch weiter in die Höhe trieb.[8]

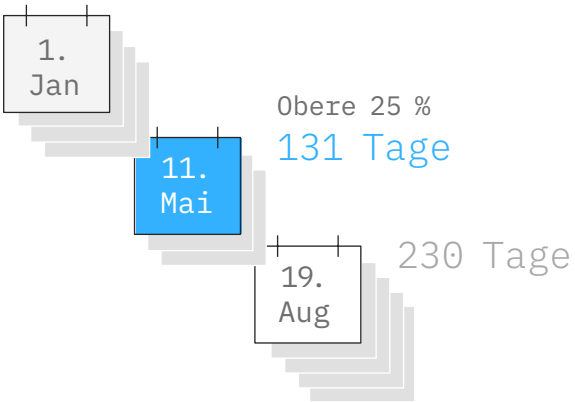
Die Ergebnisse unserer Studie zeigen, dass Anfangsinvestitionen in die KI im Verlauf eines Sicherheitsvorfalls eine effizientere Bekämpfung der Cyberkriminalität unterstützen, was sich auch in der Bewertung der Sicherheitskosten widerspiegelt. Die führenden 25 % der KI-Adopter – die bei jeder Kennzahl im 75. oder 25. Perzentil liegen – schreiben KI plus Automation signifikante Verbesserungen bei drei wichtigen Leistungskennzahlen zu, die zu einer grundlegenden Leistungsverbesserung bei der Sicherheitseffektivität führen. (Weitere Informationen zur Messung von Top-Performern finden Sie unter Studien- und Forschungsmethodik auf Seite 32.) Sie haben Folgendes erreicht:

- Senkung der Gesamtkosten für Cybersicherheit um mindestens 15 %, was eine Effizienz- und Produktivitätssteigerung in allen Prozessen eines Sicherheitsvorfalls zu Schutz vor und Prävention von Bedrohungen sowie zu Bedrohungserkennung und -reaktion bedeutet.
- Senkung der durch Datenschutzverletzungen verursachten Kosten um mindestens 18 %, was auf effizientere Erkennungs- und Reaktionsprozesse hindeutet. Dies spiegelt sich in einer Reduzierung – oder Vermeidung – der damit verbundenen Betriebskosten und Rufschädigung wider, einschließlich potenziell entgangener Aufträge (Kunden und Lieferanten), Investitionen und zukünftiger Geschäftsmöglichkeiten.
- Verbesserung ihrer Sicherheitsrendite um mind. 40 %, was auf eine Reduzierung oder Vermeidung von Cyberrisiken und der damit verbundenen Betriebskosten und Rufschädigung hinweist.

Unsere Untersuchungen decken sich mit anderen Studien, die ähnliche Vorteile durch den Einsatz von KI festgestellt haben. Das Ponemon Institute und IBM berichteten, dass die Kombination aus KI und Automation den größten Einzelfaktor bei der Reduzierung der Gesamtkosten einer Datenschutzverletzung darstellt.[9] Eine IBV-Studie über Zero-Trust-Sicherheit hat herausgefunden, dass 61 % der führenden Unternehmen Sicherheitsautomatisierung und -orchestrierung einsetzen, um die Investitions- und Betriebskosten für Sicherheit zu senken.[10]

Diese Ergebnisse belegen in überzeugender Weise, warum Sicherheitsverantwortliche den Einsatz von KI und Automation im gesamten Verlauf eines Sicherheitsvorfalls begrüßen. Als Nächstes untersuchen wir, wie Führungskräfte die Leistung in zwei wichtigen Bereichen steigern: Schutz und Prävention sowie Erkennung und Reaktion.

Benötigt ein Unternehmen ohne den Einsatz von KI 230 Kalendertage zur Erkennung von, Reaktion auf und Wiederherstellung nach Cybervorfällen, sind es mit KI nur noch 99 Tage.



Kapitel 2

KI steigert die Leistung im gesamten Verlauf eines Sicherheitsvorfalls

Zusammen mit dem Modell der gemeinsamen Verantwortung, das ein integraler Bestandteil der Cloud-Sicherheit ist, und der IT-Integration, ohne die ein Zero-Trust-Ansatz nicht funktioniert, stellt KI plus Automation grundlegende Funktionalitäten für zukünftige sicherheitsbezogene Abläufe zur Verfügung.

KI-Sicherheit plus Automation kann aussagekräftige Erkenntnisse generieren, die mit Kontext und historischen Daten angereichert werden und dann Koordination und Zusammenarbeit mit Partnern innerhalb und außerhalb des Unternehmens verbessern. Dadurch haben Fachkräfte mehr Zeit, um Bedrohungen zu untersuchen, bevor sie zum Problem werden. Durch die Leistungsverbesserung sowohl bei Schutz und Prävention als auch bei Erkennung und Reaktion gegen Bedrohungen kann KI plus Automation eine erhebliche Auswirkung auf die allgemeine Cyberresilienz des Unternehmens haben.

Um diesen Einfluss besser zu verstehen, haben wir untersucht, wie KI-Adopter KI und Automation bei Sicherheitsabläufen in ihren Prozessen zu Schutz und Prävention als auch zu Erkennung und Reaktion einsetzen. Anhand dieser Erkenntnisse konnten wir beurteilen, wie die Kombination dieser Technologien die betriebliche Effizienz und Effektivität steigert. Außerdem konnten wir erklären, wie eine bessere Leistung zu nachgelagerten Geschäftsvorteilen wie z. B. höherer Produktivität und besserer Erfahrung für Beschäftigte führt.

Durch die Verbesserung der Betriebsleistung trägt KI plus Automation zur Stärkung der allgemeinen Cyberresilienz bei.

Schutz und Prävention: KI zur Risikominimierung, Kostenkontrolle und Vertrauensbildung

Die Herausforderungen

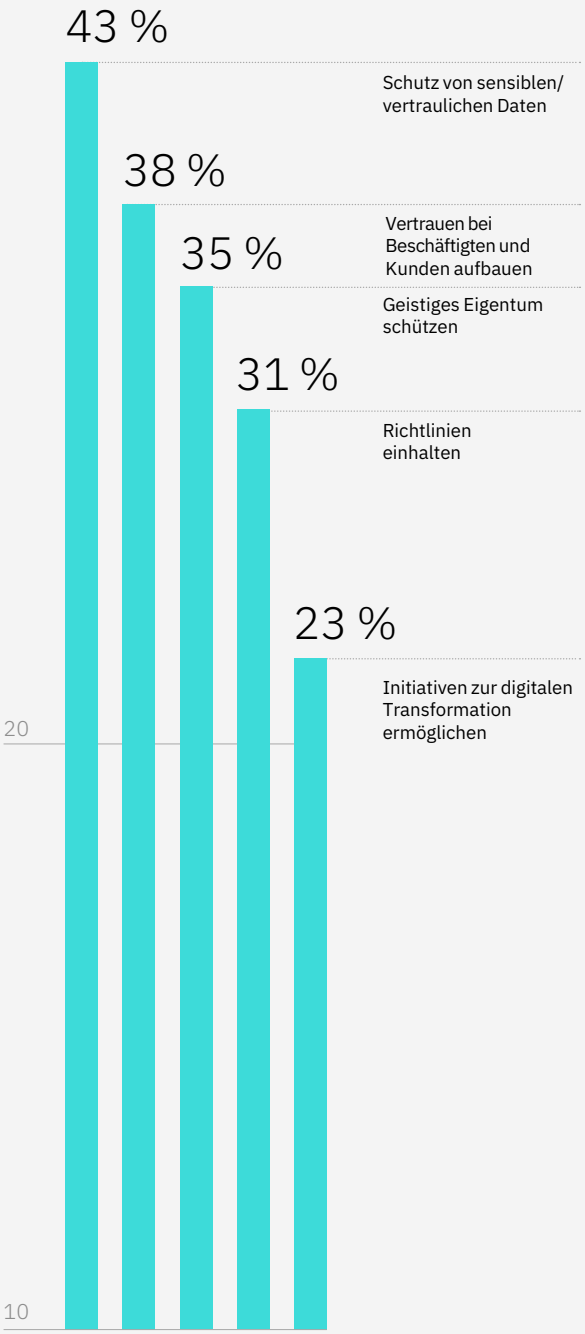
Da in den letzten Jahren die Zahl der Beschäftigten im Homeoffice sowie der cloudbasierten Anwendungen und Server gestiegen ist, haben auch die zu überwachenden Endpunkte und Anwendungen zugenommen. Cyberkriminelle nutzen vernetzte Services aus, um neue Bedrohungsvektoren zu schaffen, woraus sich Angriffe von opportunistischem Phishing bis hin zu koordinierten Ransomware-Kampagnen entwickeln können – bei denen ein Unternehmen solange als Geisel gehalten wird, bis es bezahlt. Ransomware war laut IBM X-Force® im Jahr 2021 die am häufigsten beobachtete Angriffsart; wobei Phishingattacken in 41 % der Fälle der primäre Angriffsvektor waren.[11]

Diese immer ausgefeilteren Bedrohungen der Cybersicherheit betreffen sowohl Unternehmen als auch ihre Kunden. Um das Vertrauen von Kunden, Partnern und Beschäftigten zu gewinnen und auszubauen, setzen KI-Adopter proaktiv auf die Verringerung von Risiken, den Schutz sensibler Daten und die Bewahrung geistigen Eigentums (siehe Abb. 4).

ABB. 4

KI als Wächter

KI-Adopter wollen Geschäfts- und Kundendaten schützen und Vertrauen bewahren



Frage: Wie lauten die wichtigsten Impulse für den Einsatz von KI in Ihrem Unternehmen? (Ziele mit dem Schwerpunkt auf Schutz und Prävention.)

Das KI-Nutzenversprechen

Der vielleicht bedeutendste Geschäftsvorteil ergibt sich, wenn KI plus Automation mit einem Zero-Trust-Modell kombiniert wird. Zum Schutz und zur Vorbeugung brechen diese Funktionen operative Silos auf und verbessern die Transparenz in allen digitalen Beständen des Unternehmens. Dazu zählen Daten, Geräte, Benutzer, Netzwerk, Workloads, Anwendungen und Partnerinteraktionen im gesamten Ökosystem.

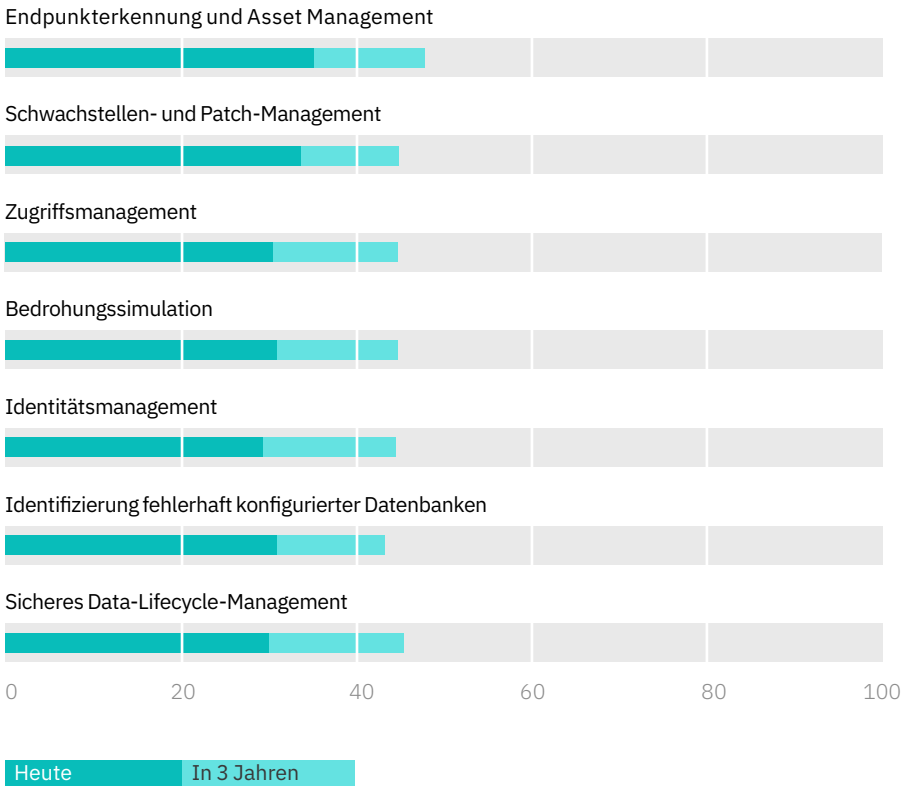
KI plus Automation kann die Transparenz erhöhen, indem regelmäßig eine Erkennung und Klassifizierung sensibler Daten durchgeführt wird – lokal, am Endpunkt der Übertragung und in der Cloud. Durch die Technologien können Unternehmen mit Quell- und Metadaten den vollständigen Kontext für jede beliebige Interaktion wiederherstellen und verstehen, wo sich die sensibelsten Daten befinden, wer auf sie zugreifen darf (und wie), wer darauf zugreift (und wann) und was damit gemacht wird. Dies trägt zur Konformität mit Datenschutz- und Compliance-Standards bei und unterstützt die Überwachung und Kontrolle des Zugriffs auf hochsensible Datenbestände.

Auf der Suche nach einer ganzheitlicheren Sicht auf ihre digitale Landschaft haben KI-Adopter die Endpunkterkennung und das Asset Management als wichtigste KI-Anwendungsfälle identifiziert. 35 % wenden derzeit KI plus Automation zu diesem Zweck an und planen, die Anwendung in 3 Jahren auf fast 50 % auszubauen (siehe Abb. 5). Dicht darauf folgt das Schwachstellenmanagement mit 34 %. KI-Adopter erwarten, dass sie den Einsatz von KI zum Schutz vor und zur Prävention von Bedrohungen in den nächsten 3 Jahren um durchschnittlich 40 % erhöhen werden. (Siehe Perspektive „Wie KI zu Schutz und Prävention beiträgt“.)

ABB. 5

Einsatz von KI bei Schutz und Prävention

Mit KI vergrößern KI-Adopter die Sicht auf einen immer größeren digitalen Bestand



Frage: Welche Anwendungsfälle der KI-Automation werden heute bereits umgesetzt? Und in 3 Jahren? (Anwendungsfälle, die sich auf den Schutz vor und die Prävention von Bedrohungen konzentrieren.)

Perspektive

Wie KI zu Schutz und Prävention beiträgt

Mit diesen Top-5-Anwendungsfällen investieren KI-Adopter in den Schutz des zugrunde liegenden Werts ihres jeweiligen Unternehmens, wobei der Schwerpunkt auf der Risikominderung und der Prävention von Angriffen liegt, was wiederum Vertrauen schafft.

KI bei Endpunkterkennung und Asset Management. Unbefugte Geräte arbeiten unter dem Radar der traditionellen Sicherheitsrichtlinien von Unternehmen und sind daher schwer erkennbar. KI kann den Kontext, die Umgebung und das Verhalten in Verbindung mit bestimmten Anlagetypen, Netzwerkdiensten und Endpunkten erlernen. Unternehmen können dann den Zugriff auf befugte Geräte einschränken und für unbefugte bzw. nicht verwaltete verhindern.

KI beim Schwachstellenmanagement. Mit KI-basierten Schwachstellenbewertungen können falsch konfigurierte Geräte identifiziert werden, um sie zu entfernen oder neu zu konfigurieren. Aktives Scannen auf Sicherheitslücken in betriebstechnischen Umgebungen kann Systeme destabilisieren. Stattdessen können Unternehmen mit KI plus Automation eine passive Überwachung durchführen. Außerdem ist KI eine Möglichkeit, um Prioritäten beim Patchen von Sicherheitslücken zu setzen: Mit Informationen über das Ausnutzen von Schwachstellen können die Kunden einen risikobasierten Ansatz für das Schwachstellenmanagement wählen.

KI beim Zugriffsmanagement. Unternehmen können mithilfe von KI den Zugriff auf Daten und Services durch Benutzer und Anwendungen überprüfen. Sobald die Berechtigungen für sensible Ressourcen festgelegt sind, kann KI die Aktivitäten auf der gesamten Kontrollebene koordinieren, Verhalten überwachen, Anomalien markieren, kontextbezogene Erkenntnisse generieren, Warnmeldungen senden und Korrekturmaßnahmen einleiten.

KI bei der Bedrohungssimulation. Bedrohungssimulatoren können sich mit Softwareendpunkten im gesamten Netzwerk eines Unternehmens verbinden, um den Ablauf eines Cybersicherheitsvorfalls zu simulieren. So wird die Sicherheitsabwehr im laufenden Betrieb getestet, ohne dass eine Interaktion mit Produktionsservern oder -endpunkten erforderlich ist. Unternehmen erkennen und beheben also Lücken in der Abwehr, ohne den Betriebsablauf zu beeinträchtigen.

KI beim Identitätsmanagement. Sicherheitsbezogene Zero-Trust-Vorgänge stellen höhere Anforderungen an IT-Infrastruktur und Sicherheitsauthentifizierungsfunktionen – insbesondere die Notwendigkeit, Identitäten nahezu in Echtzeit zu klären. Während Zero Trust die Betriebsfunktionen erheblich verbessern kann, bedeutet es auch neue Herausforderungen für die Betriebskapazität und -koordinierung (z. B. die Unterstützung von Homeoffice-Beschäftigten, die mehrere Geräte von verschiedenen Standorten aus verwenden). KI kann Authentifizierungsdienste durch die Erstellung eines eindeutigen Benutzerprofils verbessern, das auf einer Kombination aus historischem Verhalten, kontextbezogenen Daten und rollenbasierten Richtlinien aufbaut.

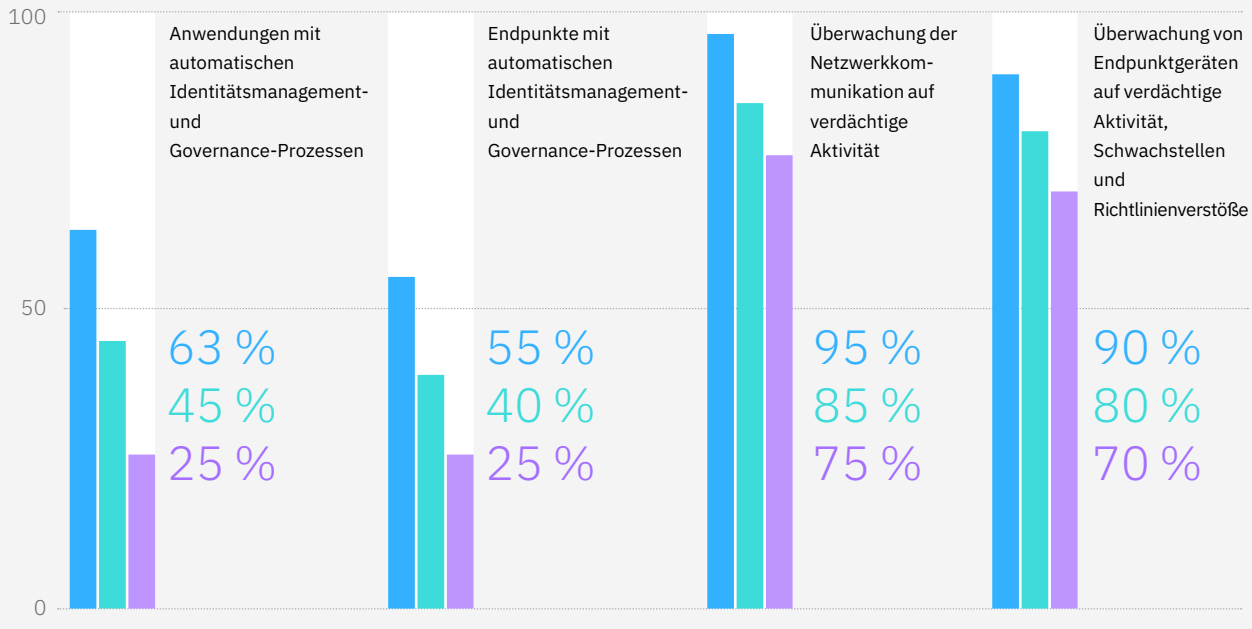
KI-fähige Automation hilft Unternehmen beim Schutz einer größeren Anzahl von Endgeräten und Anwendungen sowie bei der intensiveren Überwachung der Netzwerkkommunikation (siehe Abb. 6). Die Top-Performer unter den KI-Adoptern berichten, dass sie automatisches Identitätsmanagement und Governance auf 63 % ihrer Applikationen und 55 % ihrer Endpunkte anwenden. Diese Werte entsprechen einem durch KI gewonnenen Anstieg von 67 % bei den Anwendungen und 50 % bei den Endpunkten. Dies ermöglicht eine bessere Transparenz über eine wachsende operative Fläche, die sich auf in mehreren Clouds ausgeführte Services stützt.

ABB. 6

Mehr Transparenz

Mit Automation können KI-Adopter mehr Ressourcen verwalten und überwachen

Prozentsatz der mit KI verwalteten und überwachten Ressourcen



Obere 25 % der KI-Adopter
Durchschnitt der KI-Adopter
Untere 25 % der KI-Adopter

Selbst die für diese Bereiche gemeldeten mittleren Prozentsätze spiegeln eine solide Anzahl von Anwendungen und Endpunkten wider, die automatisiert verwaltet werden, wobei mit zunehmender Leistungssteigerung noch deutlich mehr Potenzial freigesetzt wird. KI-Adopter berichten von noch größeren Fortschritten bei der Nutzung von KI plus Automation zur Überwachung von Netzwerkkommunikation und Endpunktgeräten auf verdächtige Aktivitäten. Die Top-Performer unter den KI-Adoptern geben an, dass sie KI zur Überwachung von 95 % der Netzwerkkommunikation und 90 % der Endpunktgeräte einsetzen.

Der wahre Wert von Schutz und Prävention liegt in etwas begründet, das von Natur aus schwer zu messen ist: Vermeidung. Dank relevanterer und zeitnaher Einblicke in die Leistung aller digitalen Ressourcen können Sicherheitsteams Bedrohungen effektiver vermeiden, Risiken mindern sowie Gewinn und guten Ruf ihres jeweiligen Unternehmens schützen und bewahren.

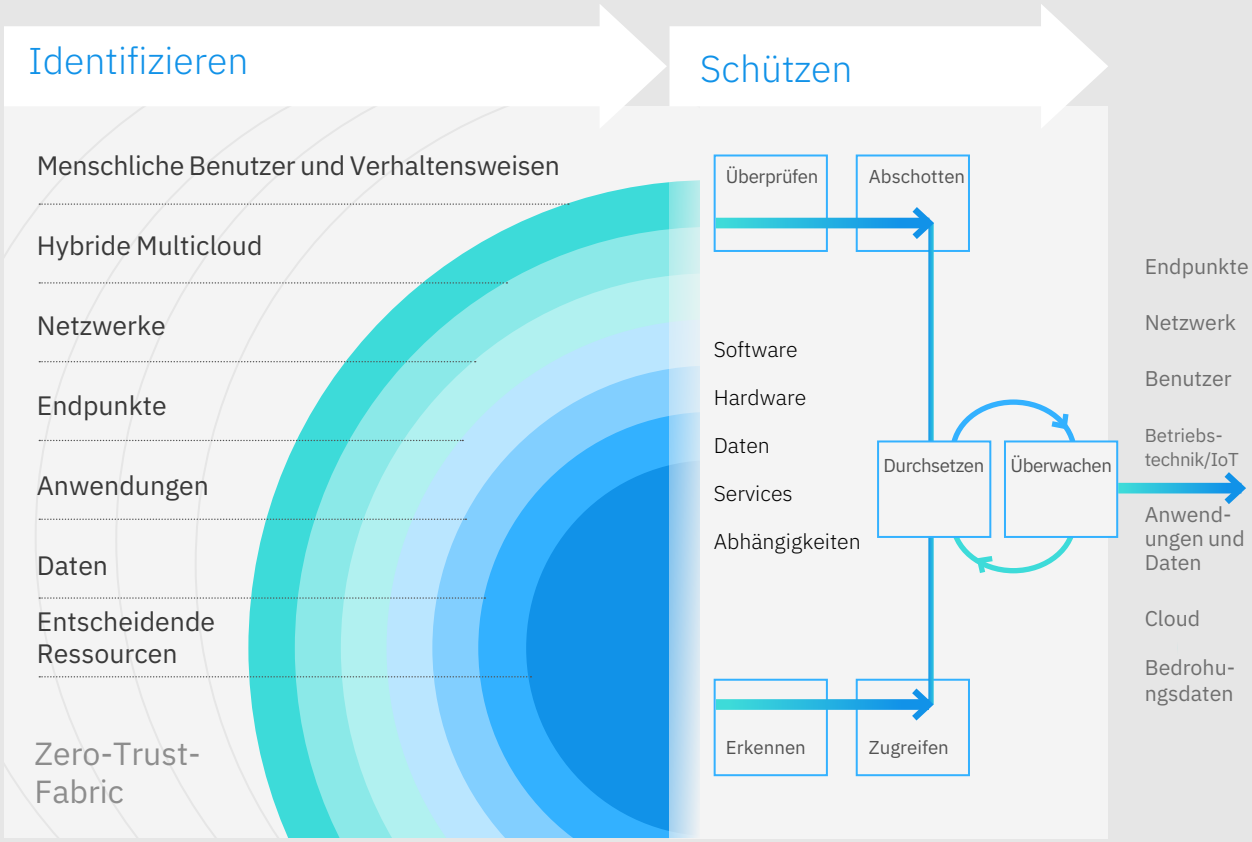
Führende KI-Adopter nutzen Automation, um 63 % ihrer Anwendungen und 55 % ihrer Endpunkte zu verwalten.

Perspektive

Die Kombination aus KI und Automation verbessert die Sicherheitskontrollen

Schutz und Prävention

KI unterstützt die Überwachung mehrerer Ebenen in Multi-Cloud-Umgebungen

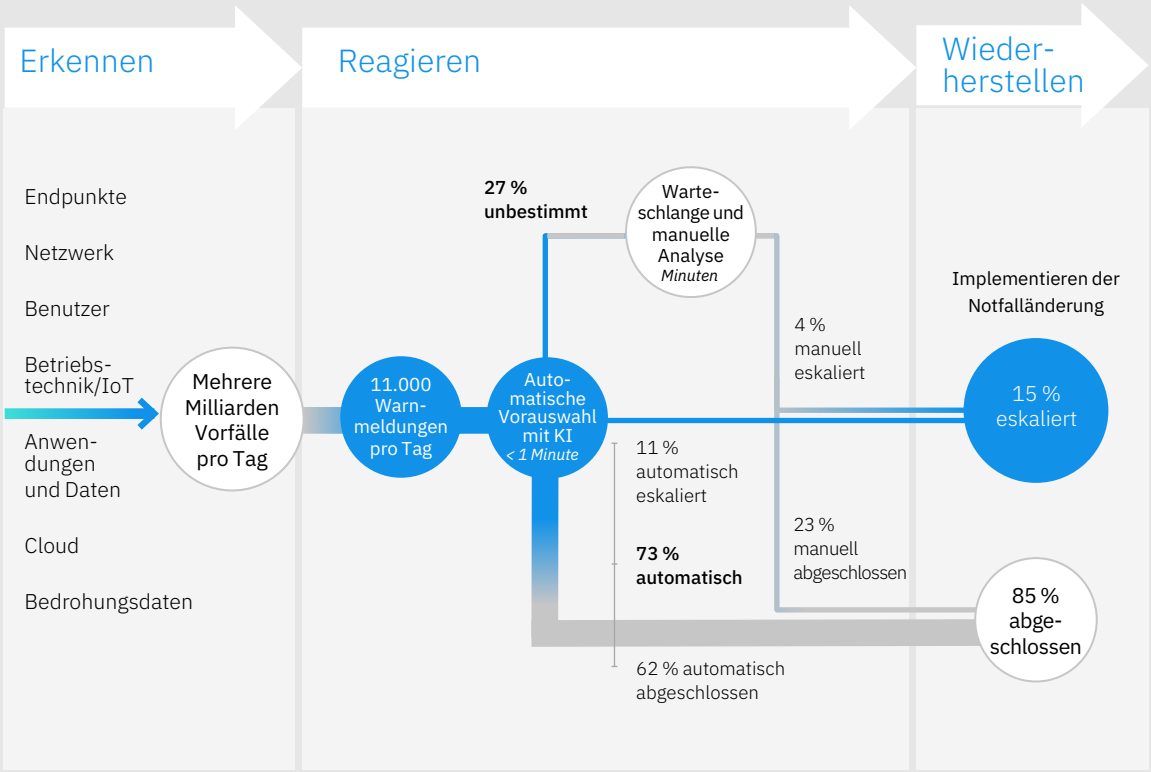


Perspektive

Die Kombination aus KI und Automation verbessert die Leistung sicherheitsbezogener Vorgänge

Bedrohungserkennung und -reaktion

Der Einsatz von KI und Automation kann Leistungsmetriken optimieren



Erfahrung des zukünftigen Analytikers

Ohne KI	**Mit KI plus Automation**
8 Tools/Bildschirme	1 Bildschirm
19 Schritte	6 Schritte
Reaktionszeit in Stunden/Tagen	Reaktionszeit in Minuten

Quelle: IBM Security Services basierend auf einer Analyse aggregierter Leistungsdaten von 2021.
Anmerkung: Bei den dargestellten Leistungsschwellenwerten wird von einer kontinuierlichen Verbesserung ausgegangen.

Erkennen und reagieren: KI zur Produktivitätssteigerung und beschleunigten Wiederherstellung nutzen

Die Herausforderungen

Das Wohlergehen des Unternehmens basiert nicht nur auf Schutz- und Präventivmaßnahmen gegen Vorfälle, sondern auch darauf, wie schnell sie Vorfälle erkennen, darauf reagieren und sich davon erholen. Das Grundprinzip des Zero-Trust-Designs besagt, dass Sicherheitsexperten davon ausgehen sollten, dass ihr jeweiliges Unternehmen bereits angegriffen wurde und in Zukunft erneut angegriffen werden kann.

Die Hauptgründe für den Einsatz von KI bei Erkennungs- und Reaktionsmaßnahmen ergeben sich aus mehreren Faktoren. Wie bereits erwähnt, führen die schnell wachsende digitale Fläche der meisten Unternehmen, der Übergang zu immer offeneren Geschäftsmodellen und die stark steigende Zahl von Homeoffice-Beschäftigten zu einer Flut neuer Sicherheitsvorfälle. Viele Sicherheitsunternehmen sind einfach nicht in der Lage, alle diese Daten manuell zu überwachen, zu verwalten sowie schnell und effektiv abzuarbeiten.

Ein Fachkräftemangel bei der Cybersicherheit verschärft die Situation. Der Fachkräftemangel hat erhebliche Auswirkungen auf den Sicherheitszustand des Unternehmens – sowohl im Hinblick auf einen effizienteren Ressourceneinsatz zur Verbesserung der Reaktionszeiten als auch bezüglich der Nutzung von Fachwissen zur Qualitätsverbesserung der Sicherheitsergebnisse.

Laut Angaben von EMSI, einem nationalen Unternehmen für Arbeitsmarktanalysen, kommen auf 100 zu besetzende Stellen im Bereich Cybersicherheit nur 68 qualifizierte Bewerber, von denen viele bereits in einem Arbeitsverhältnis stehen.[12] Eine kürzlich durchgeführte IBV-Studie ergab, dass Unternehmen 150 Tage benötigen, um eine offene Stelle im Bereich Cybersicherheit mit einem qualifizierten Kandidaten zu besetzen.[13] Neue Analytiker, die zusätzliche operative Unterstützung bei der effektiven Erledigung ihrer Arbeit benötigen, tragen nicht unbedingt zur Behebung des Fachkräftemangels bei – im Gegenteil. Sie sind oft noch unerfahren in der Branche und benötigen Zeit, um Sicherheit und Erfahrung bei der Bewertung von Bedrohungen und der Untersuchung von Fällen zu entwickeln.

KI plus Automation kann diesen Analytikern mit Wissensmanagement, Fallmanagement und operativer Unterstützung unter die Arme greifen (z. B. Chatbots und Wissensdatenbanken für natürliche Sprache). Das Ergebnis ist bahnbrechend: verbesserte Erkenntnisse, die durch die Kombination aus menschlichem Urteilsvermögen und KI plus Automation ermöglicht werden. (Siehe Perspektive „KI plus Automation – eine Talentrevolution“.)

Perspektive

KI plus Automation – eine Talentrevolution

Cyberkulturelles Bewusstsein und Fachkräfte für Cybersicherheit spielen eine entscheidende Rolle beim Erzielen von Sicherheits- und Geschäftsergebnissen. Erfolgreiche KI-Programme machen Beschäftigte nicht überflüssig. Sie verbessern die Effizienz und Effektivität von Sicherheitsanalytikern und die Reichweite von Sicherheitsexperten. Da KI ein flexibleres Interaktionsmodell ermöglicht, verringert sie manche der Ressourcen- und Qualifikationsbeschränkungen, die ein entscheidender Faktor für positive und negative Sicherheitsergebnisse sind.[14]

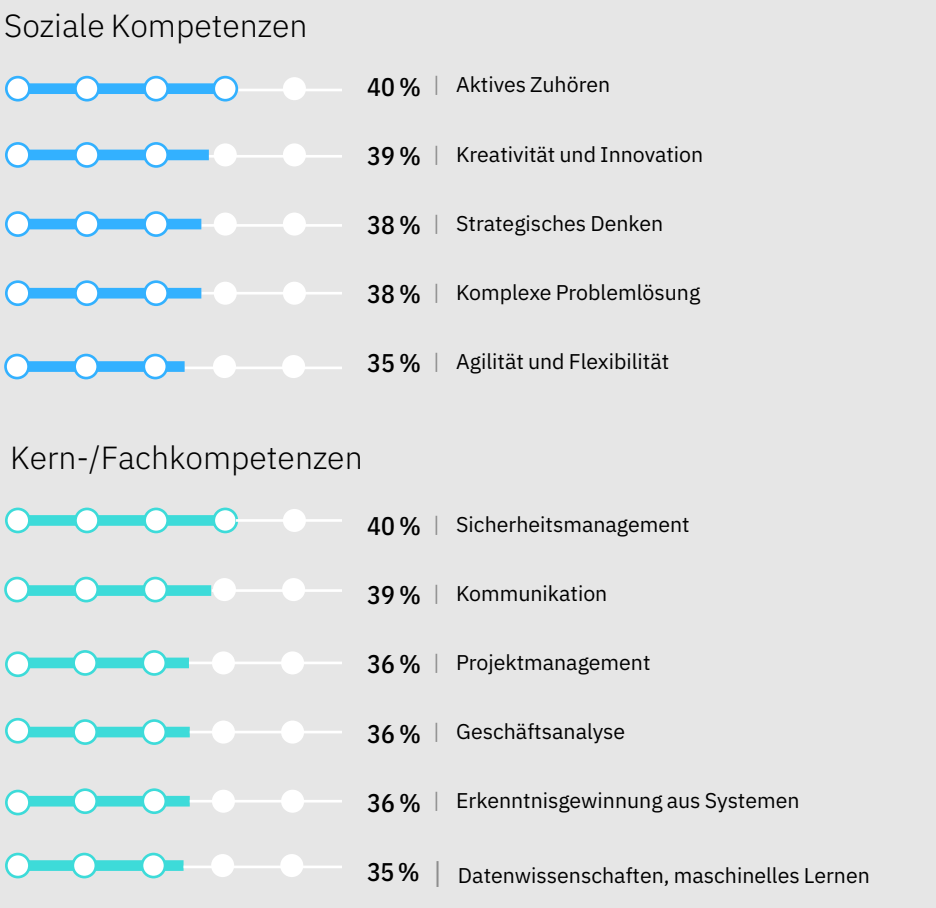
KI-Adopter haben einen akuten Bedarf an neuen Talenten. In den letzten 12 Monaten haben sie netto 15 % neue Beschäftigte im Bereich Cybersicherheit eingestellt und führen 40 % dieser Veränderung auf den Einsatz von KI im Sicherheitsbereich zurück. Die Befragten gaben an, dass sich bei 34 % der Sicherheitsfunktionen die Qualifikationsanforderungen geändert haben, wobei 35 % der Veränderungen direkt oder indirekt auf die Einführung von KI zurückzuführen sind.

Durch die Kombination von menschlichen Faktoren mit Technologie können KI-Adopter die Ressourcenlücke direkt schließen, indem sie in ihre Arbeitskräfte für Cybersicherheit investieren. Unternehmen können Talente auf natürliche Weise fördern, indem sie bei der Automation weniger auf Kostenoptimierung als vielmehr auf Spezialisierung und eine bessere Arbeitserfahrung setzen sowie den Beschäftigten beim Erweitern ihrer Kompetenzen helfen.

KI-Adopter legen bei ihren Beschäftigten Wert auf eine Kombination aus sozialen und fachlichen Kompetenzen. Bezüglich der sozialen Kompetenzen nennen 40 % der Befragten aktives Zuhören als die wichtigste, die Beschäftigte durch KI benötigen. Bei 39 % sind das die Aspekte Innovation und Kreativität. Aus fachlicher Sicht halten 40 % der Befragten Fähigkeiten im Bereich des Sicherheitsmanagements für besonders wichtig, während 39 % hohen Wert auf Kommunikationsfähigkeit legen (siehe Abbildung). Diese größere Flexibilität bei der Integration von sozialen und fachlichen Kompetenzen ist einer der aussichtsreichsten Bereiche für neue KI-Nutzenversprechen.

KI erfordert einen Mix aus verschiedenen Fähigkeiten

Beschäftigte im Bereich Cybersicherheit benötigen sowohl fachliche als auch soziale Kompetenzen, um erfolgreich mit KI zu arbeiten.



Frage: Welche Kompetenzen müssen/werden Ihre Beschäftigten im Bereich Cybersicherheit mithilfe von KI entwickeln/verbessern?

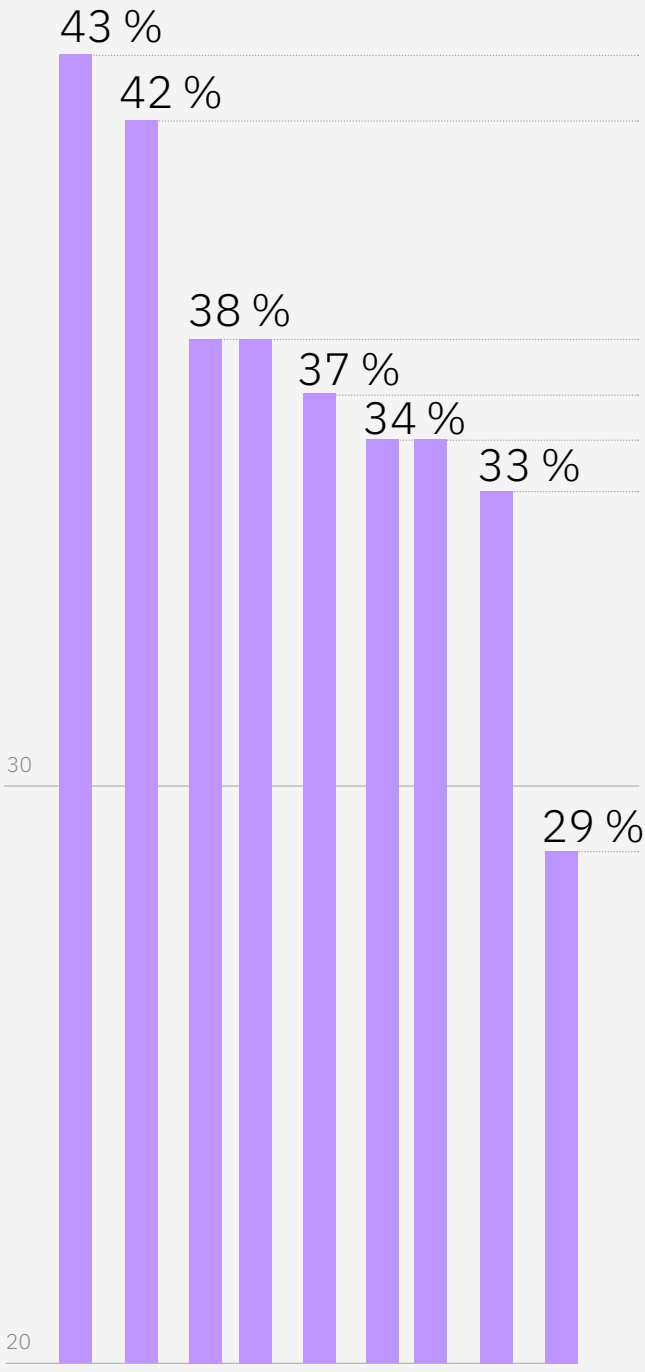
Als Reaktion auf die personellen Herausforderungen setzen KI-Adopter KI plus Automation ein, um die Produktivität und die Arbeitserfahrung der überlasteten Ressourcen zu verbessern. Tatsächlich nennen 43 % die Produktivitätssteigerung von Cyberressourcen als Hauptgrund für den Einsatz von KI. 42 % geben an, dass die Reduzierung von Sicherheitsereignissen, -vorfällen und -verletzungen ein Ziel ist, und 38 % konzentrieren sich auf den Einsatz von KI, um die Genauigkeit von Cybersicherheitsanalytikern zu verbessern (siehe Abb. 7).

Insgesamt betrachtet, können KI und Automation die Fähigkeit zur Bewältigung der schieren Menge und des Tempos von Sicherheitsvorfällen drastisch verbessern – ein Schlüsselfaktor zur Verbesserung der Arbeitsumgebung von Sicherheitsanalytikern. Wenn Analytiker besser verstehen, welche Bedrohungen mehr Aufmerksamkeit erfordern, können sie sich statt der routinemäßigen Vorauswahl höherwertigen Tätigkeiten zur Untersuchung von Bedrohungen widmen. Das ultimative Ergebnis: ein Zuwachs an Kapazität und Spezialisierung aller Arbeitskräfte im Bereich Cybersicherheit.

ABB. 7

Höhere Produktivität

KI-Adopter wollen, dass die Analytiker Bedrohungen effizienter erkennen und verhindern



Höhere Produktivität der Ressourcen für Cybersicherheit

Weniger Ereignisse, Vorfälle und Verstöße im Bereich der Cybersicherheit

Genauere Arbeitsleistung der Analytiker für Cybersicherheit

Schnellere Bedrohungserkennung und kürzere Antwortzeiten

Weniger Abhängigkeit/Neubereitstellung von Ressourcen für Cybersicherheit

Transparentere Unternehmensdaten zur Cybersicherheit

Vorhersage von Cyberangriffen

Identifizierung potenzieller Probleme in der Cybersicherheit, die für Menschen nicht sichtbar sind

Geringere Kosten für Cybersicherheit

Frage: Wie lauten die wichtigsten Impulse für den Einsatz von KI in Ihrem Unternehmen? (Ziele mit dem Schwerpunkt auf Betriebsabläufe, Bedrohungserkennung und -reaktion.)

Das KI-Nutzenversprechen

Das Geheimnis der Produktivitätssteigerung liegt in der Unterstützung der Arbeitskräfte durch den Einsatz von Technologie, und zwar genau dort, wo sie am effektivsten ist. Beispielsweise ist die Bedrohungserkennung ein idealer Anwendungsfall, um manuelle Vorgänge zu reduzieren und durch KI plus Automation effizienter zu werden. Automatische, KI-basierte Untersuchungsprozesse schützen hochwertige Daten und Technologiebestände, Netzwerksegmente und Cloud-Services selektiv. Wenn Netzwerkkommunikation, Datenverkehr und Endpunktgeräte transparenter sind, werden mit KI plus Automation potenzielle Bedrohungen besser erkannt und Cyberressourcen können durchgängig bessere und fundiertere Entscheidungen treffen.

KI-Adopter erkennen das Potenzial von KI plus Automation beim Bedrohungsmanagement. 34 % geben an, dass es ihr wichtigster KI-Anwendungsfall für Erkennungs- und Reaktionsaktivitäten ist (siehe Abb. 8). Dicht gefolgt von der automatischen Bedrohungserkennung und -reaktion, die nach Ansicht von 49 % in drei Jahren der am weitesten verbreitete Anwendungsfall sein wird. Wie bei den Schutz- und Präventivmaßnahmen erwarten die KI-Adopter, dass sie KI auch im Bereich der Erkennung und Reaktion in den nächsten 3 Jahren um durchschnittlich 40 % häufiger einsetzen. (Siehe Perspektive „Einsatz von KI bei einer schnelleren Erkennung von und Reaktion auf Bedrohungen“.)

ABB. 8

Einsatz von KI zur Bedrohungserkennung und -reaktion

Mit KI erkennen KI-Adopter Bedrohungen schneller und reagieren proaktiv auf Cyberangriffe

Frage: Welche Anwendungsfälle der KI-Automation werden heute bereits umgesetzt? Und in 3 Jahren? (Anwendungsfälle, die sich auf Bedrohungserkennung und -reaktion konzentrieren.)

Perspektive

Mit KI schneller erkennen und reagieren

Mit KI plus Automation machen KI-Adopter ihre Beschäftigten im Bereich Cybersicherheit deutlich produktiver, gemessen an mehreren wichtigen Leistungsindikatoren. Diese 5 Anwendungsfälle zeigen, wie das geht.

Automatische Bedrohungserkennung und -reaktion. KI-Sicherheit plus Automation automatisiert die Erfassung, Integration und Analyse von Daten aus Hunderten, ja sogar Tausenden von Kontrollpunkten, wobei Systemprotokolle, Netzwerkflüsse, Endpunktdaten, Cloud-API-Aufrufe und Benutzerverhalten zusammengeführt werden. Zusammen mit dem Threat Management und der Priorisierung von Warnmeldungen können bestehende Telemetrielösungen mit Funktionen wie Endpoint Detection and Response (EDR) sowie Extended Reaction and Response (XDR) ergänzt werden. Dadurch kann das Sicherheitsteam den Kontext von Sicherheitsausnahmen vollständig verstehen, Prioritäten festlegen und ausreichende Ressourcen zur Untersuchung von Bedrohungen mit erheblichen Auswirkungen bereitstellen.

Bedrohungsdaten. KI-basierte Sicherheitsinformationen ermöglichen die Analyse von Live-Datenströmen, um abnormales Verhalten in Echtzeit zu erkennen. Die bereichsübergreifende Kombination von Sicherheitsinformationen durch die Integration interner Telemetriesignale mit externen Informationsquellen liefert verwertbare Informationen in einem handlungsfähigen Zeitfenster. Sicherheitsmaßnahmen, insbesondere im Zusammenhang mit neu auftretenden Bedrohungen, werden dadurch effektiver. Darüber hinaus können die Protokollerfassungsfunktionen erweitert werden, indem die gleichen Verfahren in Cloud-Umgebungen angewendet werden – Scannen nach auffälligen Konfigurationen, die u. a. auf schwer erkennbare Angriffssignaturen wie Zero Days und Advanced Persistant Threats (APTs) hinweisen.

Fallmanagement. Mit der Funktion des Sicherheitsvorfallsmanagements werden Informationen zu verdächtigen Aktivitäten gesammelt und Untersuchungen mit detaillierten, fallbezogenen Informationen und Protokollen eskaliert. Mit KI können mehr Daten schneller verarbeitet und Data-Science-Techniken integriert werden, um Daten in Dokumenten automatisch zu identifizieren und zu klassifizieren. Da KI den Kontext versteht, kann sie Daten ohne vorherige Klassifizierung nach Themen gruppieren. So lassen sich mit als zusammengehörig erkannten Daten Rückschlüsse ziehen und Ähnlichkeiten finden, die nicht ohne Weiteres sichtbar sind.

Threat Management. Mit KI treffen Analytiker bei einer Warnmeldung eine effektive Vorauswahl, indem sie sich zuerst auf die wichtigsten konzentrieren und so zwischen falsch-negativen und falsch-positiven unterscheiden. Das macht es deutlich unwahrscheinlicher, dass kritische Vorfälle übersehen werden. Darüber hinaus werden Bedrohungen klassifiziert und priorisiert, um Warnmeldungen auf der Grundlage von Angriffserkennung, Kompromittierungsindikatoren und Verhaltensindikatoren auszulösen.

Verhaltensmodellierung und Anomalieerkennung. Automatische KI-Sicherheitsmodelle können abnormale Verhaltensweisen erkennen, Schwachstellen dynamisch bewerten und anomale Aktivitäten kennzeichnen – alles potenzielle Indikatoren für eine Sicherheitsverletzung. Anschließend kann das maschinelle Lernen auf der Grundlage eines breiten Spektrums von Faktoren wie situationsbedingten Variablen, historischen Präzedenzfällen oder Quellen für Bedrohungsdaten Abhilfemaßnahmen vorschlagen – gefolgt von Aktualisierungen der Richtlinienverwaltung an bestimmten Kontrollpunkten.

KI-Adopter berichten, dass sie die Zeit zur Erkennung und Reaktion auf Vorfälle erfolgreich verkürzen konnten (siehe Abb. 9). Im Vergleich zu Leistungsschätzungen vor der KI-Implementierung berichten sie, dass sie durchschnittlich 12 % weniger Tage zur Erkennung von Vorfällen und 11 % weniger zur Reaktion auf Vorfälle und die nachfolgende Wiederherstellung brauchen. Beim Blick auf die führenden Unternehmen sehen wir eine echte Chance, dass KI plus Automation eine Verbesserung bewirkt. Die oberen 25 % der KI-Adopter geben an, dass sie mithilfe von KI fast ein Drittel weniger Zeit zur Untersuchung von Vorfällen und fast ein Viertel weniger zur Reaktion auf Vorfälle und die nachfolgende Wiederherstellung brauchen. Außerdem wurde die Haltezeit um 45 % reduziert.

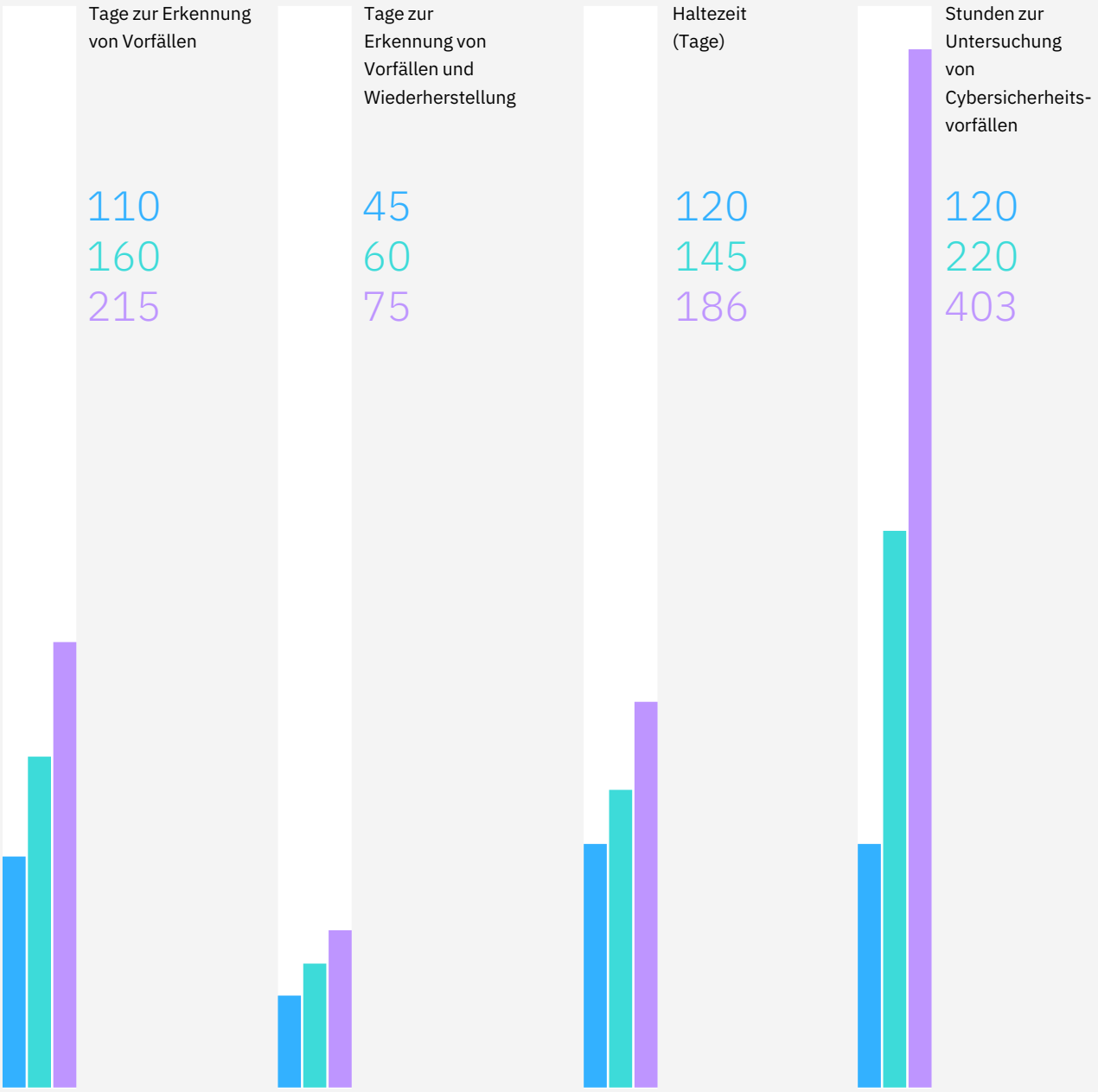
KI-Adopter zeigen, dass KI plus Automation im gesamten Sicherheitsablauf nicht nur besseren Schutz und Prävention, sondern auch leistungsstärkere Erkennung und Reaktion bedeutet. Ihr Erfolg verdeutlicht, wie die allgemeine Cyberresilienz in schwierigen Zeiten mit KI gestärkt werden kann. (Siehe Fallstudie „KI plus Automation – Bessere Arbeitsumgebung, bessere Leistung“.)

Die Top-Performer der KI-Adopter sind knapp 30 % schneller bei der Untersuchung von Cybersicherheitsvorfällen.

ABB. 9

Schnellere Wiederherstellung

Top-Performer vermelden eine deutlich schnellere Erkennung und Reaktion bei Sicherheitsvorfällen



Obere 25 % der KI-Adopter

Durchschnitt der KI-Adopter

Untere 25 % der KI-Adopter

Kürzere Balken bedeuten eine bessere Leistung

Fallstudie

Globaler Anbieter von verwalteten Sicherheitsdiensten

KI plus Automation – Bessere Arbeitsumgebung, bessere Leistung

Ein Anbieter von verwalteten Sicherheitsservices mit Hunderten globaler Kunden verschiedener Branchen hatte wiederkehrende Kapazitätsprobleme, obwohl der Sicherheitsbetrieb mit Hybrid-Cloud- und Zero-Trust-Funktionen modernisiert war. „Die Angriffsfläche wird immer größer“, sagte einer der führenden Sicherheitsanalytiker dieses Kunden. „Wir sehen beide Seiten des Problems: entweder zu viele Informationen aus zu vielen Quellen oder zu wenig relevante Informationen zu dem Zeitpunkt, wenn es am wichtigsten ist.“

Erschwerend kam hinzu, dass Qualifikationen und Spezialisierung Mangelware waren. „Wir konkurrieren um die Vermittlung schwer zu findender Talente – daher kann jeder Pluspunkt uns bei der Gewinnung von Beschäftigten den gewissen ausschlaggebenden Vorteil verschaffen“, berichtete der Kundenbetreuer. Mithilfe der Methoden von Design Thinking und IBM Garage™ bei der Zusammenarbeit begannen die Führungskräfte des Kunden, die Möglichkeiten im Hinblick auf ihre Geschäftsergebnisse auszuloten. „Wir wollten unseren Analytikern eine bessere Arbeitserfahrung bieten. Darüber hinaus interessierte uns, wie mehr Automation die Leistung des Teams verbessern könnte“, so der Kundenbetreuer.

Ein integriertes Entwicklungs- und Betriebsteam formulierte vier Hauptziele:

- weniger niederschwellige Aufgaben für die Analytiker, damit sie sich auf die wichtigen Warnmeldungen konzentrieren können
- weniger Zeitaufwand für die Vorauswahl, indem Kontextdaten, Metadaten und Serviceprotokolle zur originalgetreuen Nachbildung der Bedrohungslage zusammengestellt werden
- schnellere Untersuchungen durch mehr Kontext und angereicherte Daten/Metadaten
- punktgenaue Empfehlungen mit Erklärungen und Begründungen

Nach einem knappen Jahr sind die Betriebsabläufe des Kunden deutlich effizienter, und zwar wegen folgender Maßnahmen:

- automatische Vorauswahl bei 73 % der Warnmeldungen – vormals 40 % – mit einem Zuverlässigkeitsgrad von 90 %
- um ca. 50 % reduzierte Gesamtangriffsfläche und damit verbundene Risiken durch arbeitslastspezifische Zero-Trust-Kontrollen
- 50 % kürzere Haltezeit von Angreifern und Zeitfenster für Sicherheitslücken
- 75 % weniger Sicherheitsvorfälle und Halbierung der mittleren Zeit bis zur Erkennung

Die Automation beruht zwar auf KI, doch die Auswirkungen der Lösung auf die menschlichen Beschäftigten ist vielleicht noch stärker. Durch die Kombination von KI und Automation können sich Analytiker auf wichtigere Bedrohungen konzentrieren z. B. Zero Days, APT-Erkennung, Threat Hunting und Forensik. Sicherheitsanalytiker geben laufend Feedback, um die Lösung intelligenter, aber auch benutzerfreundlicher zu gestalten. Der Kundenbetreuer fasst die Auswirkungen auf das Unternehmen zusammen: „Der entscheidende Unterschied war für uns, dass wir Automation mit einer besseren Arbeitsumgebung für unsere Teams kombinieren konnten.“

Kapitel 3

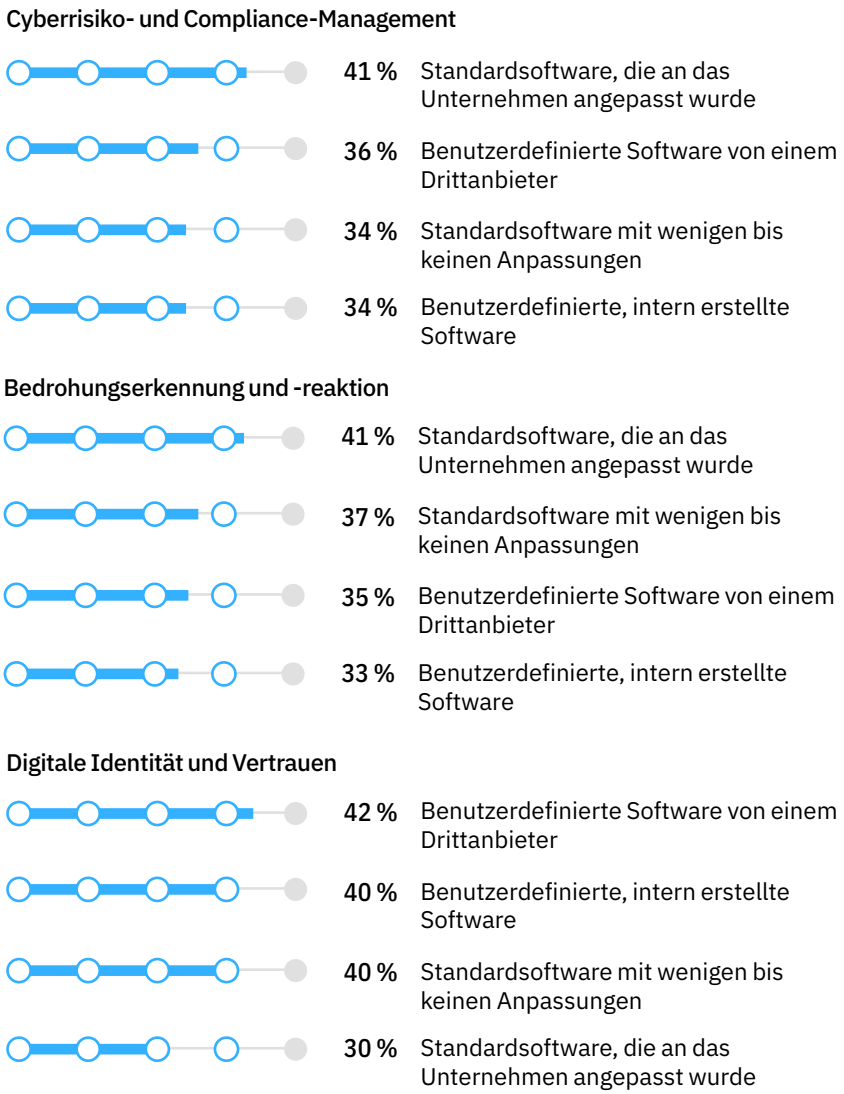
Aufstellung eines Zeitplans zur Einführung Ihrer KI-Sicherheit

Bei der Integration von KI-Erkenntnissen und Automation in Ihre Sicherheitsabläufe sollten Sie bedenken, wie eine erfolgreiche Implementierung aussehen könnte. KI-Adopter verwenden eine Mischung aus Standardlösungen und individuellen Tools. Soweit es um Cyberrisiken und Compliance sowie um die Bedrohungserkennung und die Reaktion auf Vorfälle geht, halten mehr KI-Adopter konfigurierbare Standardsoftware für die erfolgreichste Bereitstellungsart (siehe Abb. 10). Was jedoch das digitale Identitäts- und Vertrauensmanagement anbelangt, so berichten KI-Adopter, dass benutzerdefinierte Software, die entweder intern oder von einem Drittanbieter entwickelt wurde, zu erfolgreicheren Ergebnissen geführt hat.

ABB. 10

Bereitstellung von Sicherheits-KI

Die erfolgreichsten Implementierungen beinhalten in der Regel einige kundenspezifische Anpassungen



Frage: Wie würden Sie den Einsatz von KI-Technologie bei Cyberrisiko und Compliance-Management in Ihrem Unternehmen beschreiben? (Wählen Sie die 3 zutreffendsten Antworten aus.)

Frage: Wie würden Sie den Einsatz von KI-Technologie in Ihrem Unternehmen bei Bedrohungserkennung und Vorfallmanagement beschreiben? (Wählen Sie die 3 zutreffendsten Antworten aus.)

Frage: Wie würden Sie die Bereitstellung von KI-Technologie in Ihrem Unternehmen beim digitalen Identitätsmanagement und Trust-Management beschreiben? (Wählen Sie die 3 zutreffendsten Antworten aus.)

Speziell konfigurierte und individualisierte Sicherheitslösungen können mehr Funktionen und Vorteile bieten. Doch die mit der Entwicklung und dem Support verbundenen laufenden Kosten müssen in Ihrem Budget für Ihren Sicherheitsbetrieb berücksichtigt werden.

Zwar können einige Branchen von spezialisierten KI-Sicherheitsanwendungen profitieren (z. B. Banken und Finanzmärkte), allerdings müssen laufende Supportkosten, Personalbedarf und Patch-Zeitpläne gründlich bedacht werden. Das gilt insbesondere für das Wartungs- und Schwachstellenmanagement. Die Entscheidung, eine Lösung zu individualisieren, sollte einen überzeugenden operativen Grund widerspiegeln, wie den sich weiterentwickelnden Risikozustand des Unternehmens und potenzielle Schwachstellen.

Eine benutzerdefinierte KI-Lösung sollte die laufenden Kosten für den Support berücksichtigen.

Maßnahmenvorschläge

Einsatz von KI plus Automation bei der Sicherheit, um Geschäftswert zu schaffen

Selbst die erfolgreichste Sicherheitsabteilung darf niemals stillstehen. Wegen der Dynamik der Vorgänge und ständig neuen Bedrohungsvektoren müssen Sie der Einsatzbereitschaft und Resilienz Priorität einräumen. Die Frage ist nicht, ob eine Bedrohung in Ihr Unternehmen eindringt, sondern wann und in welchem Umfang.

Ebenso sollten Sie sich im Klaren darüber sein, dass KI-Modelle ständig dazulernen und Ihre Sicherheitsteams sie laufend mit neuen Leistungseinblicken versorgen müssen. Das kontinuierliche Lernen beeinflusst die Ergebnisse, die Sie erzielen können.

Für KI-Adopter wirkt sich die Sicherheitsleistung sowohl auf die betriebliche Effizienz als auch auf den Geschäftswert aus und schafft gleichzeitig eine leistungsfähigere, anpassungsfähigere Arbeitsumgebung für Sicherheitsanalytiker. Zusammengenommen können diese Faktoren einen erheblichen Einfluss auf die allgemeine Cyberresilienz des Unternehmens haben.

Unabhängig davon, ob Sie diese Funktionen zum ersten Mal nutzen oder die Funktionalität bereits bestehender Anwendungen erweitern, können Sie sich an drei Empfehlungen orientieren.

01

Bewerten Sie Ihre Leistung anhand entscheidender Sicherheitsmetriken.

Identifizieren Sie die Treiber zur Verbesserung der Sicherheit.

- Verstehen Sie die dringenden strategischen Gründe für die Einführung von KI- und Automatisierungsfunktionen in die Sicherheitsabläufe und aktualisieren Sie die Cyberrisiko- und Cybersicherheitsstrategie, um diese Prioritätenänderung zu berücksichtigen. Geht es um die Reduzierung von Cybersicherheitsvorfällen und -verletzungen oder um Kostensenkungen durch betriebliche Effizienz? Oder vielleicht darum, das Vertrauen von Kunden, Beschäftigten oder Partnern zu stärken?

Identifizieren Sie Verbesserungsbereiche auf der Grundlage von Benchmarkvergleichen.

- Untersuchen Sie die wichtigsten Risiko- und Sicherheitsmesswerte – sowohl zu Schutz und Prävention als auch zu Erkennung und Reaktion – und vergleichen Sie die Leistung Ihres Unternehmens mit der von anderen. Lücken stellen Bereiche dar, auf die Sie Verbesserungsinitiativen konzentrieren können. Bearbeiten Sie gezielt Bereiche, in denen KI plus Automation am besten helfen kann.
- Um Vergleiche anzustellen, bieten einige Unternehmen institutionalisierte Benchmarkservices an. Alternativ dazu können Sie Sicherheitsmetriken über Onlinequellen wie das Ponemon Institute, Gartner, Forrester, IDC, SANS Institute, Cloud Security Alliance (CSA) u.a. finden.

02

Priorisieren Sie Sicherheitsverbesserungen, die den größten Nutzen bringen und Ihre wichtigsten Sicherheitsziele abdecken.

Legen Sie Prioritäten gemäß Auswirkungen und angestrebten Verbesserungen bei den wichtigsten Leistungskennzahlen fest.

- Bewerten Sie den potenziellen Nutzen, der sich aus der Leistungsverbesserung jeder Ihrer wichtigsten Leistungskennzahlen ergeben kann. So können Sie feststellen, welche Bereiche in Bezug auf betriebliche Faktoren wie Kosten, Effizienz, Qualität und Zeit den größten Nutzen bringen. Vorausgesetzt, die potenziellen Bereiche stimmen mit Ihrer Sicherheitsstrategie überein, dann sollten Maßnahmen in diesen Bereichen am meisten zum Erreichen Ihrer strategischen Ziele beitragen.

Identifizieren Sie die KI-Anwendungen, die die Leistung am ehesten verbessern.

- Verstehen Sie die Leistungskennzahlen, die am ehesten mit Schutz und Prävention sowie Erkennung und Reaktion zusammenhängen. Bei Schutz und Prävention ist beispielsweise die von einem automatischen Identitäts- oder Endpunktmanagement verwaltete Anzahl der Anwendungen und Endpunkte ein wichtiger Maßstab. Die Haltezeit ist eine wichtige Kennzahl bei der Bedrohungserkennung und -reaktion.
- Überlegen Sie sich, welche KI-Anwendungen in beiden Bereichen am ehesten die für Sie wichtigsten Leistungsverbesserungen und Geschäftsvorteile bieten. Definieren Sie mit diesen Prioritäten die KI- und Automatisierungsstrategie für die Sicherheit Ihres Unternehmens. Bestimmen Sie Ihre Stärken und finden Sie heraus, wo Sie Ihr Fachwissen mithilfe von Partnern erweitern können. Wählen Sie schließlich das KI-Bereitstellungsmodell aus, das am ehesten erfolgreich ist – ob Sie eine vorhandene Lösung konfigurieren oder eine spezielle Lösung entwickeln – und inwieweit Sie bei Entwicklung und Support auf Dritte zurückgreifen möchten.

03

Entwickeln Sie Schlüsselfaktoren für Initiativen zur Verbesserung der Sicherheit.

Definieren Sie eine KI-Sicherheitsstrategie und einen entsprechenden Betriebsplan.

- Implementieren, steuern und verwalten Sie die KI-Anwendungen im Einklang mit den allgemeinen Strategien Ihres Unternehmens für Cyberrisiken und -sicherheit. Stellen Sie sicher, dass diese Strategien sich in den betrieblichen Richtlinien, Kontrollen und Prozessen widerspiegeln.

Ermitteln und entwickeln Sie die sozialen und fachlichen Kompetenzen, die Ihr Unternehmen benötigt, um erfolgreich zu sein.

- Berücksichtigen Sie die Auswirkungen der Automation auf die Beschäftigten im Bereich Cybersicherheit. Werden sie Automation als Bedrohung oder Chance wahrnehmen? Wie wird ein solches Gespräch am besten geführt?
- Bei der Überlegung, was den Erfolg von KI plus Automation im Sicherheitsbereich ausmacht, müssen auch Entwicklungs- und Loyalitätskomponenten wie das Arbeitsumfeld, die Nachfrage nach Spezialisierung und Fachwissen sowie die damit verbundene Weiterbildung bzw. Umschulung berücksichtigt werden. Welche Mischung von Kompetenzen wird in einer Arbeitsumgebung mit KI plus Automation benötigt?
- Ermitteln Sie, wo KI plus Automation den größten Nutzen für Ihre Beschäftigten im Bereich Cybersicherheit bringen kann. Identifizieren Sie Lücken und bieten Sie rollenbasierte Schulungen an, um die erforderlichen sozialen und fachlichen Kompetenzen aufzubauen und zu verbessern. Berücksichtigen Sie menschliche Faktoren wie erfahrungsbasiertes Lernen und Cybersicherheitssimulationen, um Kompetenzen aufzubauen und gleichzeitig praktische Erfahrungen zu ermöglichen, indem Sie interne oder externe Partnerservices für den Personalbereich nutzen.
- Und schließlich sollten Sie Ihre Fortschritte überwachen. Validieren Sie die tatsächliche Leistung bei der Einführung neuer KI-Anwendungen und -Funktionen anhand von Ziel-Benchmarks, um die relative Effizienz verschiedener Investitionen zu ermitteln.

Über
die Autorin und Autoren

Sridhar Muppidi

Chief Technology Officer
IBM Security
linkedin.com/in/smuppidi
muppidi@us.ibm.com

Sridhar ist ein IBM Fellow und CTO für IBM Security. Seine Aufgabe ist die Entwicklung der technischen Strategie, der Architektur und der Forschung für das IBM Security-Portfolio von Produkten und Services, die Kunden bei der Abwehr von Bedrohungen und dem Schutz digitaler Ressourcen unterstützen. Er ist ein ergebnisorientierter technischer Vordenker mit 25 Jahren Erfahrung in der Entwicklung von Sicherheitsprodukten, der Bereitstellung von Lösungsarchitekturen für Kunden, der Förderung offener Standards und der Leitung von Technikteams.

Lisa Fisher

Global Benchmark Research Leader für den Bereich IT, Sicherheit und Cloud
IBM Institute for Business Value Leader, Naher Osten und Afrika
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

Lisas Aufgabe ist die Erstellung von Benchmarking-Studien für alle Branchen und Regionen, die die Auswirkungen von Technologien auf Unternehmen unter dem Gesichtspunkt von Cyberrisiken und Cybersicherheit untersuchen und darstellen. Lisa lebt in Südafrika.

Gerald Parham

Global Research Leader für die Bereiche Sicherheit und CIO
IBM Institute for Business Value
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald leitet die Forschungsbereiche Sicherheit und CIO innerhalb des IBM Institute for Business Value. Er konzentriert sich auf Cyberstrategie, Vorstandsberatung und Sicherheit auf Ökosystemebene, insbesondere auf die Beziehung zwischen Strategie, Risiko, offene Sicherheit, Vertrauen und Geschäftswert. Er verfügt über mehr als 20 Jahre Erfahrung in den Bereichen Unternehmensführung, Innovation und Entwicklung geistigen Eigentums.

Über Benchmark Insights

Benchmark Insights bieten Führungskräften Erkenntnisse über wichtige geschäftliche und verwandte Technologiethemen. Sie beruhen auf der Analyse von Leistungsdaten und anderen Benchmarking-Maßnahmen. Weitere Informationen erhalten Sie beim IBM Institute for Business Value unter global.benchmarking@us.ibm.com.

IBM Institute for Business Value

Seit zwei Jahrzehnten dient das IBM Institute for Business Value als innovative Ideenschmiede für IBM. Uns inspiriert die Gewinnung forschungsgestützter, technologiebasierter, strategischer Erkenntnisse, mit der Führungskräfte intelligentere Geschäftsentscheidungen treffen können.

Aus unserer einzigartigen Position heraus – genau an der Schnittstelle von Wirtschaft, Technologie und Gesellschaft – befragen wir jedes Jahr Tausende von Führungskräften, Verbrauchern und Experten und fassen ihre Perspektiven zu glaubwürdigen, inspirierenden und umsetzbaren Erkenntnissen zusammen.

Wenn Sie in Verbindung bleiben wollen, melden Sie sich beim E-Mail-Newsletter von IBM an unter ibm.com/de-de/ibv. Sie können uns auch über @IBMIBV auf Twitter folgen oder auf LinkedIn unter https://ibm.co/ibv-linkedin finden

Der richtige Partner für eine Welt im Wandel

Bei IBM arbeiten wir eng mit Kunden zusammen, um ihnen durch geschäftliche Erkenntnisse, zukunftsweisende Forschung und Technologie in einer von schnellem Wandel geprägten Zeit einen deutlichen Vorteil zu verschaffen.

Zugehörige Berichte

Getting started with zero trust security

McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher und Gerald Parham. „Getting started with zero trust security.“ IBM Institute for Business Value. Juli 2021. ibm.co/zero-trust-security

The new era of cloud security

Thompson, Shue-Jane, Shamla Naidoo, Shawn Dsouza und Gerald Parham. „The new era of cloud security: Use trust networks to strengthen cyber resilience.“ IBM Institute for Business Value. April 2021. ibm.co/cloud-security-cyber-resilience

KI-Ethik in der Anwendung

„KI-Ethik in der Anwendung: Ein Unternehmensleitfaden für die Entwicklung einer vertrauenswürdigen KI.“ IBM Institute for Business Value. April 2022. ibm.co/ai-ethics-action

Studien- und Forschungsmethodik

Das IBM Institute for Business Value hat in Zusammenarbeit mit dem APQC (American Productivity and Quality Center) 1.000 Führungskräfte befragt, die die Gesamtverantwortung für die Cybersicherheit in den Bereichen IT und Betriebstechnologie (OT) ihres Unternehmens tragen. Die Befragten repräsentieren 16 Branchen, darunter Banken und Finanzmärkte, Elektronik und Software, Behörden, Versicherungen, Medien und Unterhaltung, Einzelhandel und Dienstleistungen. Sie sind auf 5 globale Regionen verteilt: Afrika und Naher Osten, Asien/Pazifik, Zentral- und Südamerika, Europa sowie USA und Kanada. Auch Unternehmen, die keine KI in ihren Sicherheitsfunktionen verwenden, wurden berücksichtigt.

Die Befragten wurden gebeten, Angaben über den aktuellen und geplanten Einsatz von KI in ihren Cyberrisiko- und Cybersicherheitsprozessen sowie über die Leistung ihrer Sicherheitsfunktionen zu machen. Da viele Faktoren die Leistung beeinflussen, haben wir die KI-Adopter – 637 Unternehmen, die KI in mindestens einem Sicherheitsprozess erproben, implementieren, betreiben oder optimieren – gebeten, die eigene Einschätzung darüber abzugeben, wie KI die Leistung bezüglich gängiger Leistungskennzahlen (KPIs) zu Cyberrisiko- und Sicherheitsfunktionen beeinflusst hat. So ermittelten wir die Leistungsspanne für jeden KPI sowie die Bandbreite der Auswirkungen der KI auf jeden KPI.

Die KPIs in diesem Bericht sind wie folgt definiert:

Haltezeit ist die Zeit zwischen erfolgreichem Eindringen und Erkennung.

Durchschnittliche Zeit (in Kalendertagen) zur Reaktion auf Cybersicherheitsvorfälle und die Erholung vom betreffenden Vorfall. Diese Zeitspanne beginnt, wenn ein Vorfall erkannt und sein Ausmaß bestimmt wurde. Sie umfasst Aktivitäten zur Bedrohungsbeseitigung und zur Wiederherstellung der betroffenen Systeme in ihren Ausgangszustand, das Testen, Überwachen und Validieren der betroffenen Systeme und die Wiederherstellung des Betriebs.

Durchschnittliche Zeit (in Stunden) zur Untersuchung von Cybersicherheitsvorfällen. Diese Zeitspanne beginnt mit dem Zeitpunkt, an dem eine Sicherheitswarnung zur Untersuchung eskaliert wird, und endet mit dem Abschluss der Untersuchung.

Cybersicherheitskosten als Prozentsatz der IT-Kosten umfassen IT-Kosten im Zusammenhang mit Anwendungs-, Cloud- und Datensicherheit, Identitätszugriffsverwaltung, Infrastrukturschutz, integriertem Risikomanagement, Netzwerksicherheitsgeräten, anderer Informationssicherheitssoftware, Sicherheitsservices und Sicherheitssoftware für den Verbraucher. Sie umfassen alle Kosten für Prozesse zur Unterstützung des Unternehmensbetriebs und schließen Abschreibungen/Amortisierungen (auf der Grundlage des Cashflows) und „weiterverkaufte IT“ aus.

Sicherheitsrendite wird als Prozentsatz ausgedrückt und entspricht {[dem geschätzten Gesamtverlust in USD x Gesamtkosten der Cybersicherheit (die prozentuale Minderung durch Cybersicherheitslösungen oder -bemühungen)] – Gesamtkosten der Cybersicherheit (die Gesamtkosten der Cybersicherheitslösung oder -bemühungen)} / Gesamtkosten der Cybersicherheit (die Gesamtkosten der Cybersicherheitslösungen oder -bemühungen)

Kosten von Datenschutzverletzungen umfassen direkte und indirekte Kosten, die bei Erkennung, Eskalation, Benachrichtigung und Maßnahmen zur Reaktion auf Datenschutzverletzungen anfallen. Die durchschnittlichen Kosten einer Datenschutzverletzung werden folgendermaßen berechnet: (jährliche Anzahl der Verstöße multipliziert mit allen Kostenfaktoren) / (jährliche Anzahl der Verstöße).

Die in diesem Bericht verwendeten Leistungsbereiche sind wie folgt definiert:

Top-Performer sind KI-Adopter, die bei der jeweiligen Metrik im 75. bzw. im 25. Perzentil abschneiden, je nachdem, ob ein höherer oder niedrigerer Wert für eine bestimmte Kennzahl günstiger ist. Ist ein höherer Werte für eine bestimmte Metrik besser, sind die Top-Performer – die oberen 25 % der KI-Adopter – Unternehmen, die im 75. Perzentil abschneiden. 75 % der Befragten schneiden unter und 25 % auf oder über diesem Niveau ab. Ist ein niedrigerer Wert besser, sind die Top-Performer KI-Adopter, die im 25. Perzentil abschneiden. 25 % der Befragten liegen auf oder unter diesem Niveau und 75 % darüber. Der Mittelwert bezieht sich auf die Verteilung der Antworten. Die Hälfte der Befragten liegt unter diesem Niveau, die andere Hälfte darüber.

Danksagungen

Das IBV möchte sich beim ausgezeichneten Team von Sicherheitsforschern von IBM Research bedanken, die die Auswirkungen neuer Technologien und angewandter Innovationen während eines Sicherheitsvorfalls untersuchen. Zu diesem Team gehören J. R. Rao, Marc Stoecklin und Ian Molloy. Wir möchten uns auch bei Srini Tummalapenta und Charles Henderson bedanken, die uns freundlicherweise ihre Expertise zur Formulierung von Schlüsselthemen zur Verfügung gestellt haben. Dieser Bericht wäre ohne die großzügigen Beiträge dieser Kolleginnen und Kollegen nicht möglich gewesen.

Wir möchten Mary O'Brien und Chris McCurdy, die ein großartiges Team von Sicherheitsexperten bei IBM Security leiten, unsere Anerkennung aussprechen. Unsere Kolleginnen und Kollegen bei IBM Security haben wertvolle, praxisnahe Ratschläge gegeben, die auf der Zusammenarbeit mit Hunderten internationaler Kunden basieren. Ihre Arbeit bildet eine wesentliche Grundlage für einen Großteil unserer Forschung.

Abschließend möchten wir uns bei unseren Kolleginnen und Kollegen von IBV bedanken, die uns bei der Erstellung dieser Materialien unterstützt haben. Dazu gehören Dave Zaharchuk, Kirsten Palmer, Heba Nashaat, Sherihan Sherif, Joanna Wilkins, Angela Finley und Kathy Cloyd. Jede Woche veröffentlicht das IBV neue Thought-Leadership-Berichte, die auf Primärforschung basieren. Jeder Bericht wird von einem breit aufgestellten Team aus Forschungs-, Analyse- und Kreativexperten unterstützt, die gemeinsam die Aussagekraft dieser Materialien herausarbeiten.

Hinweise und Quellenangaben

1 Turton, William, and Kartikay Mehrota. “Hackers Breached Colonial Pipeline Using Compromised Password.” Bloomberg. June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password; Holmes, Aaron; “Ransomeware gangs targeted 3 different US water treatment plants this year in previously unreported attacks, according to federal agencies.” Insider. October 16, 2021. https://www.businessinsider.com/3-us-water-treatment-plants-attacked-by-ransomware-gangs-report-2021-10

2 Vigliarolo, Brandon. “Report: Pretty much every type of cyberattack increased in 2021.” TechRepublic. February 17, 2022. https://www.techrepublic.com/article/report-pretty-much-every-type-of-cyberattack-increased-in-2021/; 2022 IBM X-Force Threat Intelligence Index.” IBM Security. February 2022. ibm.com/de-de/security/data-breach/threat-intelligence/

3 “SolarWinds hack was ‘largest and most sophisticated attack’ ever: Microsoft president.” Reuters. February 14, 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R; Robertson, Paul. “Best of 2021—Worldwide Hack: Microsoft Exchange Server Zero-Day Exploits.” Security Boulevard. December 27, 2021. https://securityboulevard.com/2021/12/worldwide-hack-microsoft-exchange-server-zero-day-exploits/; Torres-Arias, Santiago. “What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what’s at stake.” The Conversation. https://theconversation.com/what-is-log4j-a-cybersecurity-expert- explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896

4 “The 2021 CIO Study. The CIO Revolution: Breaking barriers, creating value.” IBM Institute for Business Value. November 2021. ibm.co/c-suite-study-cio

5 Schneier, Bruce. “The Coming AI Hackers.” Harvard Kennedy School, Belfer Center for Science and International Affairs. April 2021. https://www.belfercenter.org/publication/coming-ai-hackers

6 “AI & Cybersecurity: Balancing Innovation, Execution & Risk.” Pillsbury Law and The Economist Intelligence Unit. September 9, 2021. https://www.pillsburylaw.com/en/news-and-insights/ai-and-cybersecurity-balancing-innovation-execution-and-risk.html

7 Morgan, Steve. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” Cybercrime Magazine. November 13, 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

8 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.co/security/data-breach. “Identity Theft Resource Center’s 2021 Annual Data Breach Report Sets New Record for Number of Compromises.” Identity Theft Resource Center. January 24, 2002. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021- annual-data-breach-report-sets-new-record-for-number-of-compromises/

9 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.com/de-de/security/data-breach

10 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

11 “2022 IBM X-Force Threat Intelligence Index.” IBM Security. February 2022. ibm.com/de-de/security/data-breach/threat-intelligence/

12 Hatton, Tim. “The Cybersecurity Talent Shortage: An Urgent Threat.” EMSI. March 8, 2022. https://www.economicmodeling.com/2022/03/08/the-cybersecurity-talent-shortage/

13 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

14 Brandenburg, Rico and Paul Mee. “Cybersecurity for a Remote Workforce.” MIT Sloan Management Review. July 23, 2020. https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße
95 1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Hergestellt in den Vereinigten Staaten von Amerika | Juni 2022

Dieses Dokument wurde von einer zertifizierten Druckerei mit FSC-Zertifizierung (Forest Stewardship Council) auf chlorfreiem Recyclingpapier mit biogener Tinte gedruckt. Die zur Herstellung des Papiers und des Drucks verwendete Energie wurde durch erneuerbare, grüne Energiequellen erzeugt. Bitte der Wiederverwertung zuführen.

9NGZA7GK-DEDE-01

IBM