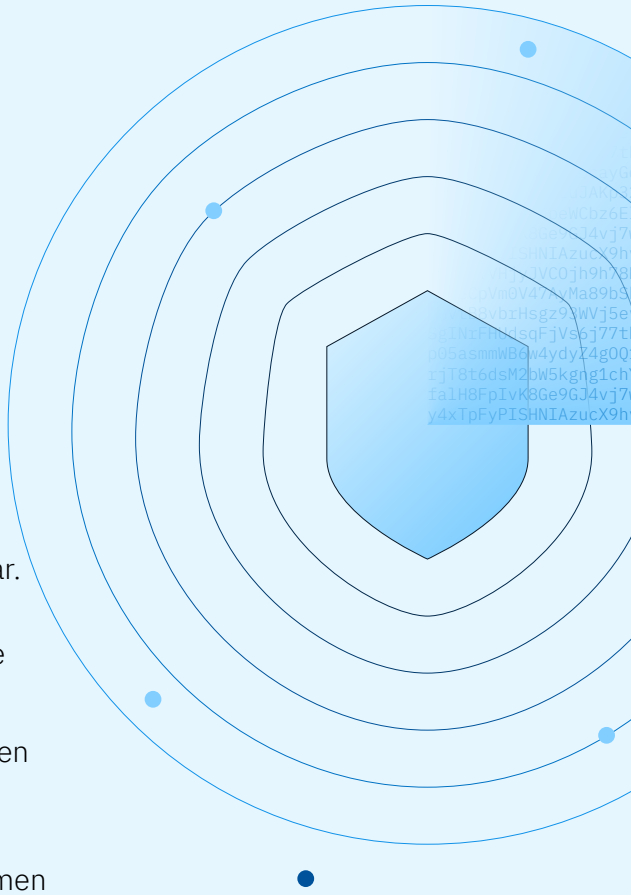
Wenn es um Cybersicherheit geht, müssen Angriffe mit Gegenangriffen abgewehrt werden



Generative KI ist mit keiner bisherigen Technologie vergleichbar. Sie bewirkt radikale und rasante Änderungen in Wirtschaft und Gesellschaft und zwingt Führungskräfte, ihre Annahmen, Pläne und Strategien innerhalb kürzester Zeit zu überdenken.

Um CEOs dabei zu unterstützen, den Überblick über die rasanten Entwicklungen zu behalten, veröffentlicht das IBM Institute for Business Value (IBM IBV) eine Reihe maßgeschneiderter, forschungsbasierter Leitfäden zu generativer KI, in denen Themen wie Cyberdatensicherheit, Strategien für Technologieinvestitionen und Kundenerfahrungen behandelt werden.

Dies ist Teil sieben: Cybersicherheit.

Generative KI erhöht Risiko – und Widerstandsfähigkeit

Generative KI hat eine neue Generation von Cyber-Bedrohungen hervorgebracht. Hacker haben mehr Möglichkeiten, Schwachstellen auszunutzen – und mehr Wege, ihre bösartigen Kampagnen durchzuführen.

Zum Glück ist auch das Gegenteil der Fall: Generative KI kann auch zum Schutz des Unternehmens beitragen. In naher Zukunft wird generative KI die Beschleunigung von Sicherheitsprozessen ermöglichen, die in der Vergangenheit eine Herausforderung waren. Indem sie riesige Datenmengen analysiert und Muster – und Anomalien – erkennt, kann die generative KI Bedrohungen so schnell erkennen, wie sie entstehen.

Je mehr neue Tricks die Cyberkriminellen in ihr Repertoire aufnehmen, desto schneller müssen die Cybersicherheitsteams reagieren, um Schritt halten zu können. Der Schlüssel zum Umgang mit Schwachstellen in diesem Katz-und-Maus-Spiel ist Wachsamkeit – und immer einen Schritt voraus zu sein.

Aus den Forschungsergebnissen des IBM Institute for Business Value lassen sich drei Erkenntnisse ableiten, die Führungskräfte berücksichtigen müssen, damit die Transformation die erhofften Erfolge bringt:

1. Mit der generativen KI eröffnet sich eine Welt von neuen Risiken und Bedrohungen.

2. Eine zuverlässige generative KI ist ohne eine sichere Datenbasis nicht möglich.

3. Generative KI für die Cybersicherheit zu nutzen, kann viele Vorteile bringen.

Und drei weitere Dinge, die man als Führungskraft tun sollte:

1. Behandeln Sie generative KI wie eine tickende Zeitbombe und sichern Sie sie sofort.

2. Machen Sie zuverlässige Daten zum Rückgrat Ihres Unternehmens.

3. Richten Sie Ihre Investitionen in die Cybersicherheit auf Geschwindigkeit und Skalierbarkeit aus.

1. Cyberrisiko + generative KI

Das sollten Sie wissen

Mit der generativen KI eröffnet sich eine Welt von neuen Risiken und Bedrohungen

Die generative KI gibt Cyberangreifern ein völlig neues Arsenal an die Hand. Hacker imitieren heutzutage nicht mehr nur E-Mails – sie können auch Stimmen, Gesichter und sogar Persönlichkeiten nachahmen, um Opfer in ihre Fallen zu locken.

Und das ist erst der Anfang.

Mit der zunehmenden Verbreitung von generativer KI in den nächsten sechs bis zwölf Monaten erwarten Experten, dass neue Angriffsattacken an Umfang, Geschwindigkeit, Raffinesse und Präzision zunehmen werden, wobei ständig neue Bedrohungen am Horizont auftauchen. Sowohl in Bezug auf die Wahrscheinlichkeit als auch auf die potenziellen Auswirkungen stellen autonome, massenhaft durchgeführte Angriffe das größte Risiko dar. Führungskräfte gehen jedoch davon aus, dass Hacker, die sich als vertrauenswürdige Benutzer ausgeben, den größten Schaden für das Unternehmen anrichten können, dicht gefolgt von der Erstellung bösartigen Codes.

Auch die Art und Weise, wie Unternehmen generative KI einsetzen, könnte neue Risiken mit sich bringen. So befürchten 47 % der Führungskräfte, dass der Einsatz generativer KI im Betrieb zu neuartigen Angriffen auf ihre eigenen KI-Modelle, Daten oder Dienste führen könnte. Und fast alle Führungskräfte (96 %) sind der Ansicht, dass die Einführung generativer KI innerhalb der nächsten drei Jahre in ihrem Unternehmen zu einem Sicherheitsverstoß führen wird.

Angesichts der Tatsache, dass sich die durchschnittlichen Kosten einer Datenschutzverletzung weltweit auf 4,45 Mio. US-Dollar belaufen – in den USA sind es 9,48 Mio. US-Dollar – investieren Unternehmen massiv in die Bewältigung neuer Cybersicherheitsrisiken. Führungskräfte geben an, dass ihre Budgets für KI-Cybersicherheit im Jahr 2023 um 51 % höher sind als im Jahr 2021. Und sie gehen davon aus, dass diese Budgets bis 2025 um weitere 43 % steigen werden.

Executives say their 2023 AI cybersecurity budgets are **51% greater** than they were in 2021.

And they expect those budgets to climb an **additional 43%** by 2025.

1. Cyberrisiko + generative KI

Das sollten Sie tun

Behandeln Sie generative KI wie eine tickende Zeitbombe und sichern Sie sie sofort

Üben Sie Druck auf die Verantwortlichen für Cybersicherheit aus, damit diese dringend handeln und auf generative KI-Risiken als unmittelbare und nicht als wachsende Risiken reagieren.

Verstehen Sie Ihre KI-Risiken. Bringen Sie Führungskräfte aus den Bereichen Cybersicherheit, Technologie, Daten und Betrieb zu einer Diskussion auf Vorstandsebene über die sich entwickelnden Risiken zusammen, einschließlich der Frage, wie generative KI ausgenutzt werden kann, um sensible Daten offenzulegen und unbefugten Zugriff auf Systeme zu ermöglichen. Bringen Sie alle auf den neuesten Stand in Bezug auf die aufkommende „feindliche" KI – fast unmerkliche Änderungen an einem Kerndatensatz, die bösartige Auswirkungen haben.

Sichern Sie die gesamte KI-Pipeline. Konzentrieren Sie sich auf die Sicherung und Verschlüsselung von Daten, die zum Trainieren und Anpassen von KI-Modellen verwendet werden. Scannen Sie während der Modellentwicklung kontinuierlich auf Schwachstellen, Malware und Schäden und überwachen Sie KI-spezifische Angriffe (z. B. Datenkorruption und Modelldiebstahl), nachdem das Modell bereitgestellt wurde.

Investieren Sie in neue Abwehrmaßnahmen, die speziell auf den Schutz von KI ausgerichtet sind. Bestehende Sicherheitskontrollen und Fachkenntnisse können zwar erweitert werden, um die Infrastruktur und die Daten, die KI-Systeme unterstützen, zu schützen, doch sind neue Methoden erforderlich, um Angriffe auf KI-Modelle zu erkennen und abzuwehren.

2. Daten + generative KI

Das sollten Sie wissen

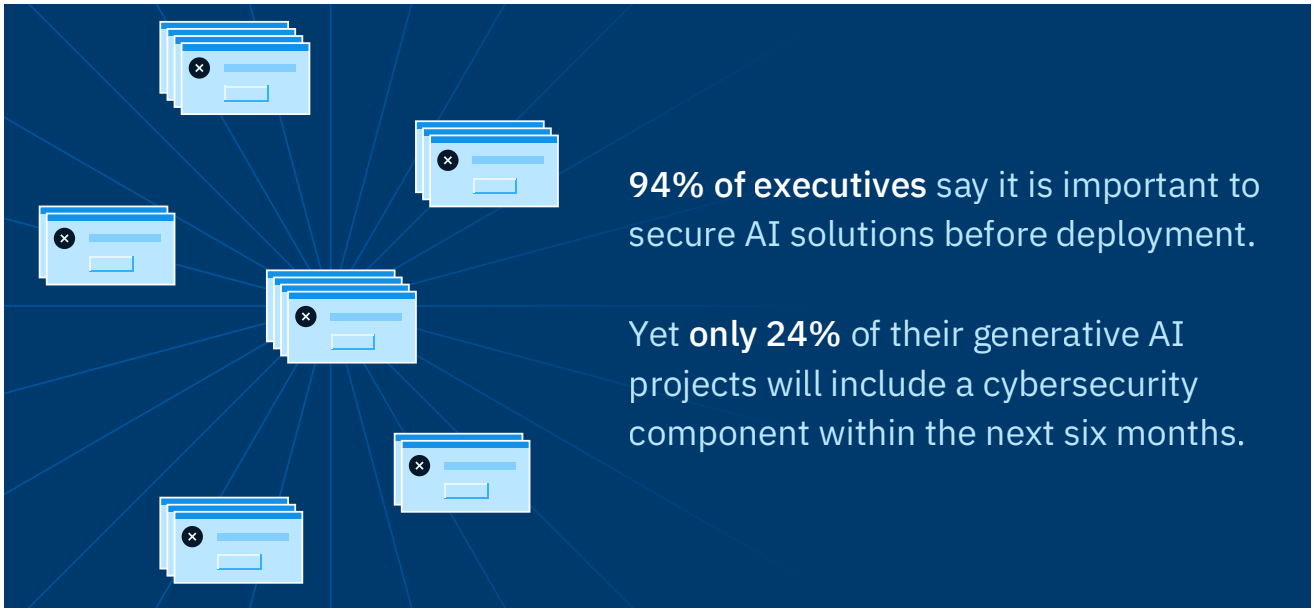
Eine zuverlässige generative KI ist ohne eine sichere Datenbasis nicht möglich

Daten sind das Herzstück der generativen KI. Alle Modelle stützen sich auf Daten, um Abfragen zu beantworten und Erkenntnisse zu gewinnen, weshalb Trainingsdaten zum Ziel von Cyberangriffen geworden sind. Während Hacker nach wie vor versuchen, Daten zu stehlen, um sie an den Meistbietenden zu verkaufen, bietet die Dateninfiltration einen neuen Weg zu unrechtmäßigem Gewinn. Wenn sie in der Lage sind, die Daten zu verändern, die das generative KI-Modell eines Unternehmens steuern, können sie Geschäftsentscheidungen durch gezielte Manipulation oder Fehlinformationen beeinflussen. Diese sich entwickelnde Bedrohung wirft eine Reihe neuer rechtlicher, sicherheitsbezogener und datenschutzrechtlicher Fragen auf, mit denen sich CEOs unternehmensweit auseinandersetzen müssen.

Die Verantwortlichen erkennen die Zeichen der Zeit. Bei der Einführung generativer KI rechnen sie mit einer Vielzahl von Risiken. 84 % befürchten weit verbreitete oder katastrophale Angriffe auf die Cybersicherheit, die neue Schwachstellen schaffen könnten. Jede dritte Führungskraft gibt an, dass diese Risiken ohne grundlegend neue Formen der Unternehmensführung, wie z. B. umfassende regulatorische Frameworks und unabhängige Audits durch Dritte, nicht in den Griff zu bekommen sind.

Insgesamt halten es 94 % der Führungskräfte für wichtig, KI-Lösungen vor dem Einsatz abzusichern. Dennoch werden nur 24 % ihrer generativen KI-Projekte in den nächsten sechs Monaten eine Cybersicherheitskomponente enthalten – und 69 % sagen, dass Innovation bei generativer KI Vorrang vor Cybersicherheit hat.

Dies zeigt eine eklatante Diskrepanz zwischen dem Verständnis der Anforderungen an die Cybersicherheit generativer KI und der Umsetzung von Cybersicherheitsmaßnahmen. Um kostspielige und unnötige Konsequenzen zu vermeiden, müssen CEOs die Probleme der Cybersicherheit und der Datenherkunft direkt angehen, indem sie in Datenschutzmaßnahmen wie Verschlüsselung und Anonymisierung, sowie in Datenverfolgungs- und Herkunftssysteme, die die Integrität der in generativen KI-Modellen verwendeten Daten besser schützen können.



2. Daten + generative KI

Das sollten Sie tun

Machen Sie zuverlässige Daten zum Rückgrat Ihres Unternehmens

Entwickeln Sie Ihre Cybersicherheitspraktiken weiter, um den Anforderungen verschiedener generativer KI-Modelle und Datendienste gerecht zu werden.

Schaffen Sie Vertrauen und Sicherheit bei der Nutzung von KI. Priorisieren Sie Datenrichtlinien und -kontrollen, die auf Sicherheit, Datenschutz, Governance und Compliance ausgerichtet sind. Kommunizieren Sie, wie wichtig Transparenz und Rechenschaftspflicht sind, um Voreingenommenheit, die Angst vor Halluzinationen und andere Bedenken beim Risikomanagement zu vermeiden.

Schützen Sie die Daten, die KI antreiben. Beauftragen Sie Ihren CISO mit der Identifizierung und Klassifizierung sensibler Daten, die für das Training oder die Feinabstimmung verwendet werden, und implementieren Sie Techniken zum Schutz vor Datenverlust, um Datenlecks durch Prompts zu verhindern. Setzen Sie Zugriffsrichtlinien und -kontrollen für Datensätze, die für maschinelles Lernen verwendet werden, durch. Erweitern Sie die Bedrohungsmodellierung, um generative KI-spezifische Bedrohungen wie Datenkorruption und die Ausgabe sensibler Daten oder unangemessener Inhalte abzudecken.

Behandeln Sie Cybersicherheit wie ein Produkt, und Stakeholder wie Kunden. Cybersicherheit spielt eine entscheidende Rolle bei der Sicherung der KI-Initiativen, die den Umsatz steigern werden. Um die KI, die Sie in Ihren Produkten einsetzen, zu sichern, sollten Sie Ihre Teams über die Cybersecurity-Bedrohungen aufklären, die mit generativer KI einhergehen. Weisen Sie auf die Bedeutung von Verhaltensänderungen zur Verbesserung der Daten- und Sicherheitshygiene hin. Fördern Sie die Akzeptanz, indem Sie die Ergebnisse der Cybersicherheit an den Geschäftsergebnissen ausrichten.

3. Cyber-Resilienz + generative KI

Das sollten Sie wissen

Generative KI für die Cybersicherheit zu nutzen, kann viele Vorteile bringen

Im Bereich der Cybersicherheit kann die generative KI den Betrieb beschleunigen. Sie kann sich wiederholende und zeitaufwändige Aufgaben automatisieren, so dass sich die Teams auf die komplexeren und strategischen Aspekte der Sicherheit konzentrieren können. Sie kann außerdem Bedrohungen erkennen und untersuchen und aus vergangenen Vorfällen lernen, um die Reaktionsstrategie des Unternehmens in Echtzeit anzupassen.

Da so viel auf dem Spiel steht, stehen die CEOs unter dem Druck, generative KI schnell und auf weitreichender Ebene einzuführen. Um jedoch zu verhindern, dass ein durch Wachstum getriebenes Kartenhaus einstürzt, ist es unerlässlich, dass die Unternehmensführung die Technologie auch zur Stärkung ihrer Widerstandsfähigkeit einsetzt. Auf diese Weise vermeiden Führungskräfte nicht nur die Risiken generativer KI, sondern nutzen sie auch, um ihr Unternehmen zu stärken.

Mehr als die Hälfte der Führungskräfte (52 %) geben an, dass die generative KI ihnen helfen wird, Ressourcen, Kapazitäten, Talente oder Fähigkeiten besser zuzuordnen, und 92 % sagen, dass sie ihr Cybersicherheitspersonal eher erweitern oder aufstocken als ersetzen werden, wenn sie generative KI einführen.

Diese neuen technischen Tools können Teams dabei helfen, die Komplexität zu reduzieren und sich auf das Wesentliche zu konzentrieren. Dies könnte der Grund sein, warum 84 % der Führungskräfte Cybersicherheitslösungen mit generativer KI gegenüber herkömmlichen Cybersicherheitslösungen bevorzugen.

Der Einsatz von generativer KI in der Cybersicherheit kann einen Multiplikatoreffekt auf das gesamte Ökosystem des Unternehmens haben. 84 % der Führungskräfte geben an, dass offene Innovation und Ökosysteme für ihre künftige Wachstumsstrategie wichtig sind. Da diese Führungskräfte bestrebt sind, Beziehungen aufzubauen, die Innovation und Wachstum unterstützen, gehen die meisten davon aus, dass generative KI-Funktionen in den nächsten zwei Jahren ihre Auswahl an Ökosystem-Partnern in der Cloud (59 %) und im gesamten Unternehmen (62 %) beeinflussen werden.

Mit zunehmender Reife der generativen KI wird ihr Potenzial zur Wertschöpfung bei gleichzeitiger Risikominderung weiter wachsen. Unternehmen, die umfassende Risiko- und Widerstandsfähigkeiten entwickelt haben, werden nicht nur in der Lage sein, diese neue Technologie schneller zu nutzen, sondern auch besser positioniert sein, um künftiges Wachstum zu verteidigen.

84% of executives plan to prioritize generative AI cybersecurity solutions over conventional cybersecurity solutions.

3. Cyber-Resilienz + generative KI

Das sollten Sie tun

Richten Sie Ihre Investitionen in Cybersicherheit auf Geschwindigkeit und Skalierbarkeit aus

Machen Sie KI zu einem unverzichtbaren Instrument zur Stärkung der Sicherheit. Ermutigen Sie die Verantwortlichen für Cybersicherheit, generative KI und Automatisierung in ihre Toolkits einzubinden, um Sicherheitsrisiken und -vorfälle schnell und im großen Maßstab zu beheben. Dies wird zu erheblichen Produktivitätssteigerungen führen und die Cybersicherheit als Faktor für das Unternehmenswachstum nutzen.

Nutzen Sie KI zur Beschleunigung von Sicherheitsergebnissen. Automatisieren Sie Routineaufgaben, die kein menschliches Fachwissen und kein menschliches Urteilsvermögen erfordern. Nutzen Sie generative KI, um Aufgaben zu rationalisieren, die auf der Zusammenarbeit von Menschen und Technologie beruhen, wie z. B. die Erstellung von Sicherheitsrichtlinien, die Bedrohungsjagd und die Reaktion auf Vorfälle.

Setzen Sie KI ein, um neue Bedrohungen zu erkennen. Aktualisieren Sie Tools und Verfahren, um Ihre Teams mit derselben Geschwindigkeit, Größe, Präzision und Raffinesse auszustatten wie Ihre Angreifer. Nutzen Sie generative KI, um Muster und Anomalien schneller zu erkennen, damit Teams neue Bedrohungsvektoren erkennen können, bevor sie das Geschäft beeinträchtigen.

Finden Sie Stärke in der Zusammenarbeit. Arbeiten Sie mit vertrauenswürdigen Partnern zusammen, um den Reifegrad Ihrer KI-Sicherheit zu definieren und eine umfassende Strategie für generative KI zu implementieren, von der Ihr gesamtes Unternehmen profitiert.

IBM Institute for Business Value

Leitfaden für CEOs zu generativer KI

Cybersicherheit

Die Statistiken, auf denen diese Erkenntnisse beruhen, stammen aus vier proprietären Umfragen, die vom IBM Institute for Business Value in Zusammenarbeit mit Oxford Economics durchgeführt wurden, sowie aus einer Referenz aus dem IBM-Bericht *„Cost of a data breach"* (2023) und einer aus *„Open the door to open innovation"* (2022). Die erste Umfrage wurde im September-Oktober 2023 unter 200 in den USA ansässigen Führungskräften zum Einfluss der generativen KI auf die Cybersicherheit durchgeführt. De zweite Umfrage wurde im Mai-Juni 2023 unter 414 Führungskräften in den USA zu den Auswirkungen generativer KI auf die Hybrid-Cloud durchgeführt. Die dritte Umfrage wurde im August-September 2023 unter 200 Führungskräften in den USA zum Thema generative KI und KI-Ethik durchgeführt. In der vierten Umfrage wurden im Mai 2023 300 in den USA ansässige Führungskräfte zu den Auswirkungen generativer KI auf die Arbeitswelt befragt.

ibm.co/de-de/ceo-generative-ai-cybersecurity

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de
IBM Corporation
New Orchard Road
Armonk, NY 10504

Hergestellt in den Vereinigten Staaten von Amerika | Oktober 2023

DBMQB8RE-DEDE-00