Antworten auf Ihre 4 wichtigsten Fragen zur Sicherheit generativer KI

Schnelle Einführung von generativer KI bei gleichzeitiger Gewährleistung von Sicherheit, Datenschutz und Compliance

Dieses E-Book richtet sich an Führungskräfte in Unternehmen, insbesondere an IT-Entscheidungsträger und Leiter von Sicherheitsteams, die planen oder darüber nachdenken, wie sie generative KI sicher in ihr Unternehmen integrieren können.

Inhalt

EINFÜHRUNG

Auf die Plätze, fertig, generieren: generative KI schnell und sicher einführen

Das Rennen um generative KI ist eröffnet. Aufgrund massiver Verbesserungsmöglichkeiten in den Bereichen Produktivität und Erlebnis drängen Unternehmen darauf, Kundenerlebnisse und Anwendungen neu zu erfinden.

Obwohl die Ära der generativen künstlichen Intelligenz (KI) gerade erst begonnen hat, erzielen Unternehmen bereits jetzt greifbare Vorteile in praktisch allen Geschäftsbereichen. Sicherheitsexperten raten jedoch zur Vorsicht. Als Gründe für die Vorsicht bei der Einführung der generativen KI geben sie den Datenschutz, Verzerrungen bei Modellen, die Erstellung schädlicher Inhalte (z. B. Deepfakes) und das Risiko böswilliger Eingaben in Modelle an.

Es ist unerlässlich, dass sich Unternehmen der generativen KI mit einer klaren Strategie nähern. Diese muss Daten, Benutzer und auch den Ruf des Unternehmens schützen, aber dennoch eine schnelle Einführung und eine Optimierung des Kundenerlebnisses ermöglichen.

Zweifelsohne eine vielschichtige Herausforderung. Dabei sollten Unternehmen berücksichtigen, dass die standardmäßigen bewährten Methoden für KI, Machine Learning (ML), Datenschutz und Cloud-Workload-Sicherheit nach wie vor gelten. Es ist durchaus möglich, dass Ihr Unternehmen besser auf eine sichere generative KI vorbereitet ist, als Sie denken.

Wenn Sie jetzt angemessene Schutzmaßnahmen für generative KI-Workloads einrichten, können Sie Innovationen in Ihrem Unternehmen vorantreiben. So erhalten Ihre Teams das Selbstvertrauen, großartige Ideen zu verfolgen, und die Freiheit, sich auf das Wachstum Ihres Unternehmens konzentrieren zu können.

In diesem E-Book befassen wir uns mit 4 wichtigen Fragen, die Sie sich stellen sollten, wenn Sie beginnen, Ihre generativen KI-Workloads sicherer zu machen.

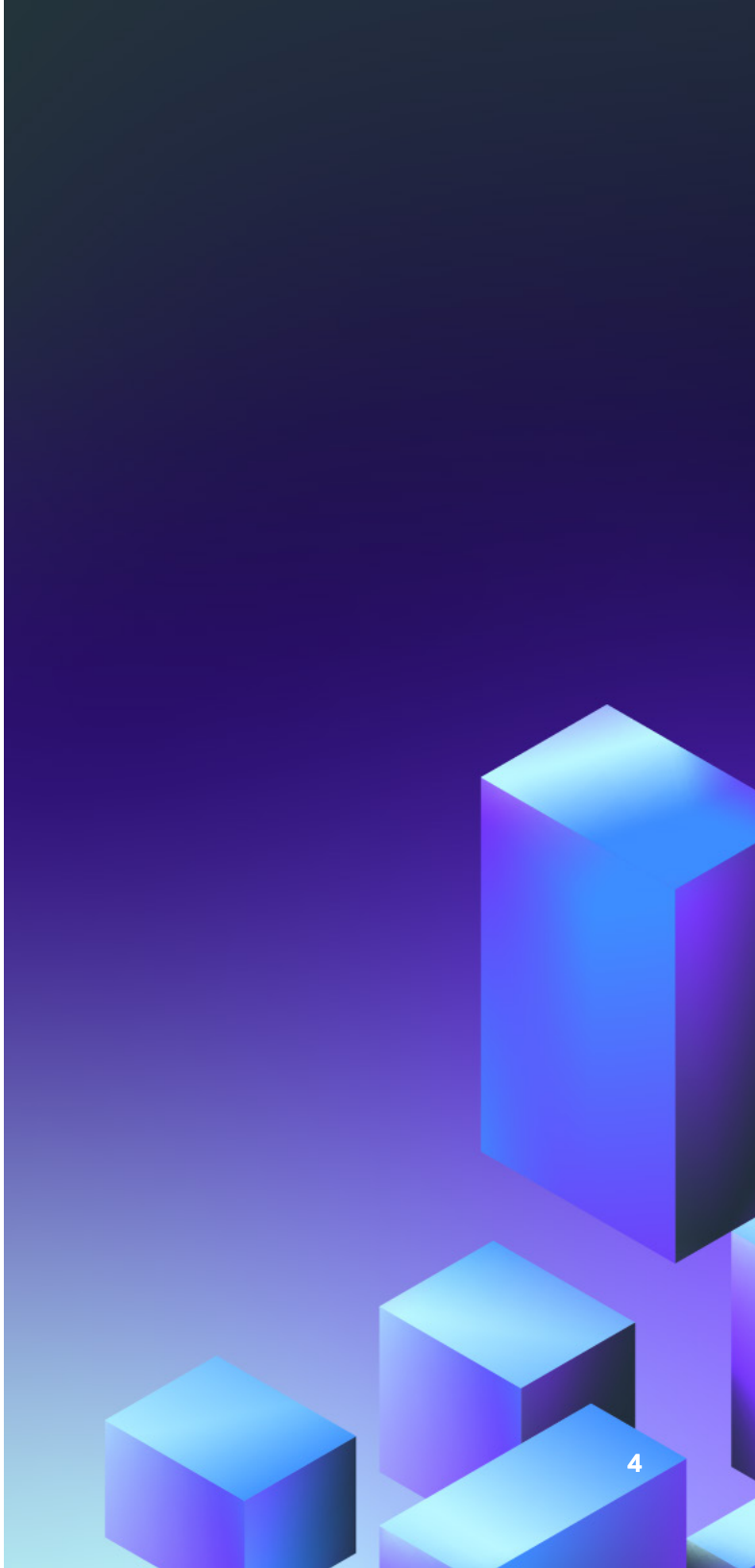
1. **Was muss geschützt werden?**
2. **Wie können Sie Bedenken zur Compliance ausräumen?**
3. **Wie können Sie sicherstellen, dass die Modelle wie beabsichtigt funktionieren?**
4. **Wo sollten Sie anfangen?**

Frage 1:

Was muss geschützt werden?

Bevor Sie generative KI-Anwendungen sicher entwickeln und einsetzen können, müssen Sie wissen, was genau geschützt werden muss. Es kann von Vorteil sein, hier eine Unterteilung in drei Kategorien vorzunehmen:

- **Schutz Ihrer Cloud-Workloads**
- **Schutz Ihrer Daten**
- **Schutz Ihrer generativen KI-Anwendungen**



Schutz Ihrer Cloud-Workloads

Der Einsatz generativer KI bei gleichzeitiger Erfüllung Ihrer Sicherheits- und Datenschutzziele beginnt mit dem Schutz Ihrer gesamten Cloud-Infrastruktur, Services und Konfigurationen. Dazu müssen Sie zunächst zwischen Ihren Sicherheitsaufgaben und denen Ihres Cloud-Anbieters differenzieren.

Kunden von Amazon Web Services (AWS) können sich dazu am **Modell der geteilten Verantwortung** orientieren. Es besagt, dass AWS im Großen und Ganzen für den Betrieb, die Verwaltung und die Kontrolle der Infrastruktur verantwortlich ist, auf der alle in der AWS Cloud angebotenen Services ausgeführt werden – dies wird auch als „Sicherheit *der* Cloud“ bezeichnet.

Die AWS-Kunden dagegen sind verantwortlich für die Verwaltung des Gastbetriebssystems (einschließlich Updates und Sicherheits-Patches) und andere damit verbundene Anwendungssoftware sowie für die Konfiguration der von AWS bereitgestellten Firewall für die Sicherheitsgruppe. Der Umfang und die spezifischen Aufgaben, die Kunden erfüllen müssen, hängen von den AWS-Services ab, für die sie sich entscheiden. Dies wird als „Sicherheit *in* der Cloud“ bezeichnet.

Die Beliebtheit generativer KI mag zwar neu sein, aber traditionelle bewährte Sicherheitsverfahren sind und bleiben ein hilfreicher Ausgangspunkt. Zu diesen zählen grundlegende Verfahren zur Sicherheitshygiene für Folgendes:

- Identity and Access Management (IAM)
- Erkennung und Reaktion
- Schutz der Infrastruktur
- Datenschutz
- Anwendungssicherheit

Schutz Ihrer Daten

Als Nächstes müssen Sie dazu beitragen, die Sicherheit und den Datenschutz der von Ihren generativen KI-Anwendungen verwendeten Daten zu gewährleisten. Dies kann geschützte Informationen, wertvolles geistiges Eigentum (IP) und persönlich identifizierbare Informationen (PII) beinhalten.

Generative KI-Anwendungen basieren auf Basismodellen (FMs), die mit riesigen Datenmengen trainiert werden. FMs analysieren diese Daten, um Muster zu erkennen und zu lernen, wie neue, ähnliche Inhalte generiert werden können. Zum Entwickeln generativer KI-Anwendungen, die Ihren spezifischen Geschäftsanforderungen entsprechen, müssen Sie in der Regel ein vorhandenes FM anpassen, indem Sie es mit den Daten Ihres Unternehmens trainieren.

Damit diese Daten geschützt sind, müssen Datenschutzkontrollen und bewährte Methoden der IAM-Richtlinie berücksichtigt werden.

Stellen Sie beim Anpassen von FMs sicher, dass Ihre Teams mit einer Modellversion arbeiten, die sicher gespeichert ist und nicht dazu verwendet wird, das FM selbst zu verbessern. Durch die Festlegung einer dedizierten Single-Tenant-Kapazität in **Amazon Bedrock** kann der Service seine Inferenz-Instances an Ihre **Amazon Virtual Private Cloud** (Amazon VPC) anhängen, um in **Amazon Simple Storage Service** (Amazon S3) zu schreiben und aus diesem Service zu lesen.

Effektives IAM sorgt dafür, dass die richtigen Personen und Maschinen unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Das **AWS-Well-Architected-Framework** beschreibt Designprinzipien und bewährte architektonische Verfahren zur Identitätsverwaltung. Diese Ressource ist ein nützliches Tool für die Entwicklung von IAM-Richtlinien und die Lösung anderer Sicherheitsprobleme wie Bedrohungserkennung und Netzwerksicherheit.

Schutz Ihrer generativen KI-Anwendungen

Zum Schützen generativer KI auf Anwendungsebene müssen Sie Risiken kontinuierlich identifizieren, klassifizieren, beheben und mindern. Ein erster Schritt ist hierbei die Umsetzung vorhandener bewährter Methoden zum Schutz von Daten und Umgebungen.

Ausgehend von diesem Punkt sollten Sie überlegen, wie Sie den Sicherheitsaspekt zu einem früheren Zeitpunkt im Entwicklungsprozess verschieben können. Dies kann Ihre Bestrebungen rationalisieren und dafür sorgen, dass Entwicklungsteams schneller und freier innovativ sein können, ohne dass eben dieser Sicherheitsaspekt zu einem Nadelöhr wird.

Als Nächstes sollten Sie überlegen, wie Sie die drei kritischen Komponenten einer KI-Anwendung schützen können: Eingaben, Ausgaben und das Modell selbst.

Eingaben schützen

Überprüfen Sie zunächst die Daten, die in Ihr KI-System eingehen. Benutzer sollten ohne Eingabefilterung keinen direkten Zugriff auf das FM haben, um das Risiko von Integritätsangriffen wie Manipulation, Spoofing oder Prompt Injection zu verringern. Diese Angriffstechniken umgehen Kontrollen oder missbrauchen das Modell. Andere Strategien, die zum Schutz von Eingaben in Betracht gezogen werden sollten, sind die Automatisierung der Datenqualität, die kontinuierliche Überwachung und die Bedrohungsmodellierung.

Ausgaben schützen

Zu den Risiken für generative KI-Anwendungen gehören die Offenlegung von Informationen, IP-Vorfälle und der Missbrauch des Modells, wodurch der Ruf des Unternehmens Schaden nehmen könnte. Berücksichtigen Sie bei der Entwicklung Ihres Bedrohungsmodells den Informationsfußabdruck und den Nutzungskontext und sorgen Sie für eine komplexe Erkennung und Überwachung von Verhaltensweisen.

Das Modell selbst schützen

Überlegen Sie sich zu guter Letzt, wie böswillige Personen versuchen könnten, Daten aus dem Modell selbst oder den zugehörigen Komponenten zu entfernen. Zu den Risiken gehören falsche Darstellungen der realen Welt oder der Daten im Modell sowie Schäden an der Integrität oder Verfügbarkeit des Modells. Modellieren Sie Bedrohungen für Ihre Geschäftsziele und implementieren Sie eine Überwachung dieser Bedrohungsszenarien.

COMPLIANCE-ANFORDERUNGEN

Frage 2:

Wie können Sie Bedenken zur Compliance ausräumen?

Indem Sie die Risiken minimieren, die mit dem Entwurf und der Entwicklung generativer KI-Anwendungen verbunden sind, kann Ihr Unternehmen Vertrauen bei Partnern und Kunden aufbauen, den Ruf der Marke aufrechterhalten und die Compliance-Anforderungen weiterhin erfüllen.

Die gesetzliche Regulierung generativer KI-Anwendungen steckt noch in den Kinderschuhen. Derzeit gibt es noch keinen Konsens hinsichtlich bewährter Methoden. Sich im Labyrinth der widersprüchlichen Standards zurechtzufinden und einen Überblick über die verschiedenen Rechtsprechungen und Zuständigkeiten zu behalten, stellt eine komplexe und anhaltende Herausforderung dar.

Arbeiten Sie mit Ihren Rechtsberatern und Datenschutzexperten zusammen, um die Anforderungen und Auswirkungen der Entwicklung Ihrer generativen KI-Anwendung einschätzen zu können. Dies kann die Überprüfung Ihrer Rechtsansprüche hinsichtlich der Verwendung bestimmter Daten und Modelle sowie die Feststellung der Anwendbarkeit von Gesetzen in den Bereichen Datenschutz, Biometrie, Antidiskriminierung und andere anwendungsfallspezifische Vorschriften umfassen.

Beachten Sie die unterschiedlichen gesetzlichen Anforderungen in den einzelnen Bundesstaaten, Regionen und Ländern sowie die neuen KI-Vorschriften, die weltweit vorgeschlagen werden. Greifen Sie diese Überlegungen bei zukünftigen Bereitstellungs- und Betriebsphasen wieder auf.

Die Zusammenarbeit mit Kollegen, KI-Experten und Regierungsorganisationen hilft außerdem bei der Einhaltung von Vorschriften und macht Kunden deutlich, dass Sie rechtliche und ethische KI-Standards ernst nehmen. Vor Kurzem hat sich Amazon gemeinsam mit dem Weißen Haus und 6 führenden KI-Unternehmen **freiwillig zu einer verantwortungsvollen und sicheren KI-Entwicklung verpflichtet**. Dies stellt den Wert solcher Engagements unter Beweis und legt zugleich den Grundstein für eine zukünftige Zusammenarbeit.

Mit künstlicher Intelligenz verbundene Risiken

Wie bei jeder Lösung, bei der ML zum Einsatz kommt, bergen generative KI-Anwendungen Risiken, die über die herkömmlicher Software hinausgehen. Damit Anwendungen mit generativer KI sicher erstellt und bereitgestellt werden können, müssen Sie sich mit diesen Risiken befassen und Strategien zu deren Minderung entwickeln. Dazu zählen:

- Ausgaben, die voreingenommen, unwahr, irreführend, schädlich oder anstößig sind
- Komplexität und Kosten in großem Umfang
- Datensätze, die zu groß werden, zunehmend veraltet sind oder aus dem vorgesehenen Kontext herausgelöst wurden
- Bedenken hinsichtlich erhöhter Opazität und Reproduzierbarkeit
- Teststandards und -verfahren, die unzureichend entwickelt sind

Im nächsten Abschnitt befassen wir uns mit umfangreichen Strategien zur Reduzierung einiger dieser Risiken und mit bewährten Methoden zum Definieren der fachlichen, organisatorischen und gesellschaftlichen Auswirkungen Ihrer generativen KI-Anwendungen.

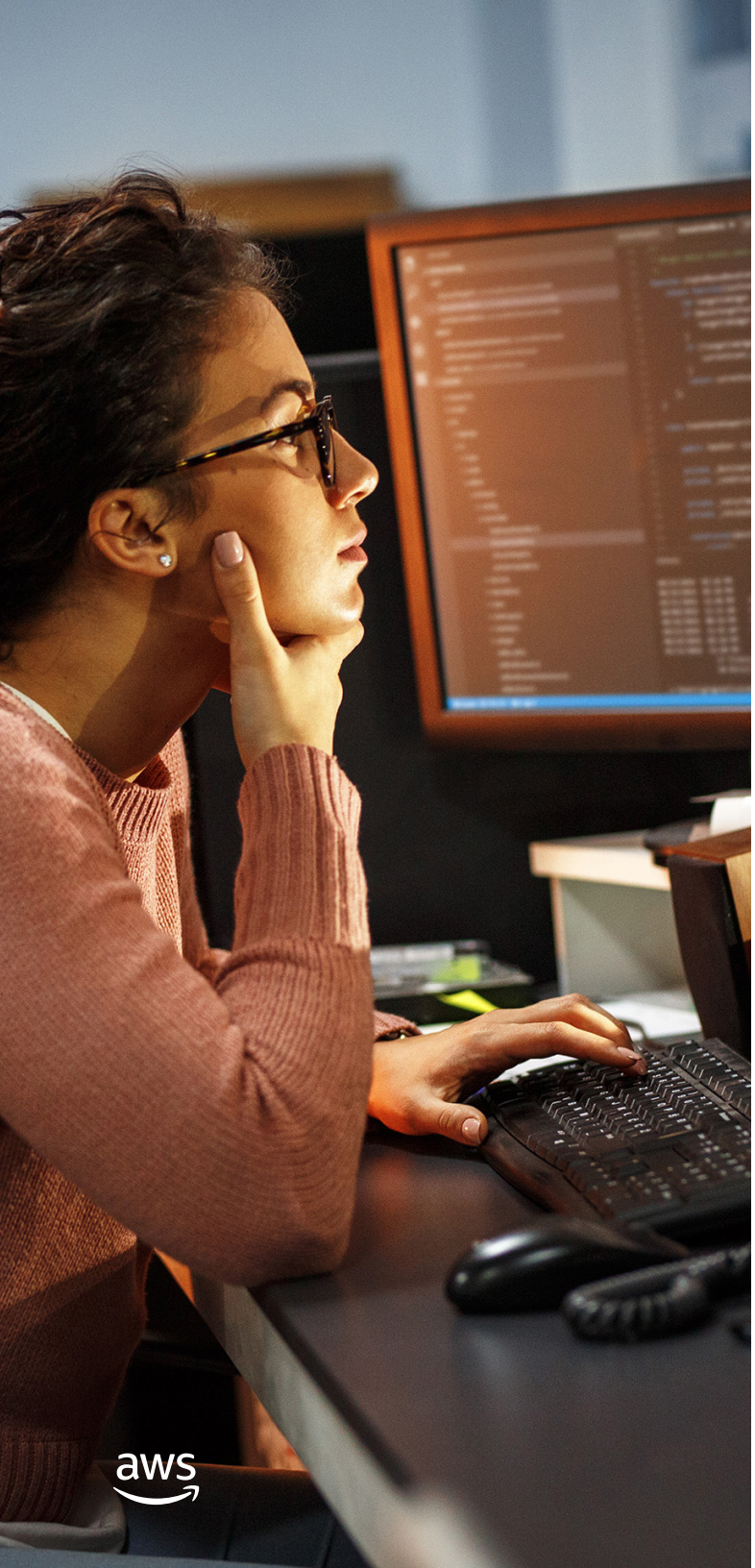
Frage 3:

Wie können Sie sicherstellen, dass die Modelle wie beabsichtigt funktionieren?

Die Sicherstellung einer verantwortungsvollen Verwendung generativer KI hat sich zu einer wesentlichen Geschäftsaufgabe entwickelt – und zu einer wichtigen Voraussetzung für kontinuierliche Innovation.

FMs werden mit riesigen Datensätzen trainiert und führen komplexe Analysen durch, um zu verstehen, wie ähnliche Inhalte generiert werden. Obwohl viele FMs bemerkenswerte Ergebnisse liefern, gilt nach wie vor das alte Diktum „Garbage in, Garbage out“ (GIGO, Müll rein, Müll raus). Wenn ein FM mit ungenauen, unvollständigen oder verzerrten Daten gespeist wird, weisen dessen Ausgaben möglicherweise ähnliche Schwächen auf.

Fehlerhafte Daten eröffnen Möglichkeiten für Missbrauch und böswillige Aktionen und bergen weitere Risiken. Mit der Erweiterung Ihrer generativen KI-Anwendung in Bezug auf Benutzer, Umfang und Funktionalität nehmen die potenziellen Auswirkungen dieser Probleme zu.



Eine verantwortungsvolle KI fördern

Mit einer verantwortungsvollen KI-Strategie können Sie diese Risiken besser bewältigen. Zu den Dimensionen einer verantwortungsvollen KI gehören Erklärbarkeit, Fairness, Governance, Datenschutz, Sicherheit, Robustheit und Transparenz. Dazu gehört außerdem, zu verstehen, wie verschiedene Kulturen und demografische Gruppen von der Anwendung betrachtet, behandelt und beeinflusst werden.

Denken Sie am besten bereits schon bei Ihrem Einstieg in die generative KI über einen verantwortungsvollen Umgang mit dieser nach und behalten Sie dieses Bestreben als wichtigen Teil Ihrer Vision während des Anwendungslebenszyklus bei. Beginnen Sie mit relativ kleinen und einfachen Aktionen. Skalieren Sie als Nächstes, wie sich verantwortungsvolle KI im Laufe der Zeit auf Ihr Design, Ihre Entwicklung und Ihren Betrieb auswirkt.

Machen Sie sich bei der Ausarbeitung verantwortungsvoller KI- und Governance-Richtlinien Gedanken darüber, wie sich Ihre generative KI-Anwendung auf Ihre Benutzer, Kunden, Mitarbeiter und die Gesellschaft auswirken wird. Achten Sie zudem auf algorithmische Fairness, eine diverse und inklusive Repräsentation und das Erkennen von Verzerrungen.

Toxizität bekämpfen

Der Begriff Toxizität bezieht sich bei großen Sprachmodellen (LLMs) auf die Generierung von unhöflichem, respektlosem oder unangemessenem Text. Es gibt viele Strategien, um einer Toxizität vorzubeugen und Fairness in Ihren generativen KI-Anwendungen zu gewährleisten. Sie können beispielsweise anstößige Ausdrücke oder voreingenommene Phrasen identifizieren und aus den Trainingsdaten entfernen. Sie können auch enger gefasste Fairness-Tests durchführen, die sich auf den spezifischen Anwendungsfall Ihrer Anwendung, die Zielgruppen oder die am ehesten zu erwartenden Aufforderungen und Abfragen konzentrieren.

Sie können zudem Modelle zum Integritätsschutz mit kommentierten Datensätzen trainieren, die die verschiedenen Arten und das Ausmaß der Toxizität identifizieren. Auf diese Weise lernt das FM, unerwünschte Inhalte in Trainingsdaten, Eingabeaufforderungen und generierten Ausgaben automatisch zu erkennen und zu filtern.

Datenschutz

Sie haben mehrere Möglichkeiten, um zu verhindern, dass sensible Informationen, Geschäftsgeheimnisse und geistiges Eigentum ungewollt offengelegt werden, wenn Sie mit generativen KI-Anwendungen arbeiten.

Das Löschen von Modellen ist eine Methode, um Datenschutzbedenken auszuräumen. Dies beinhaltet das Entfernen missbräuchlich verwendeter Daten nach deren Identifizierung, um die Auswirkungen dieser Daten auf alle FM-Komponenten zu beseitigen.

Ein weiterer Ansatz ist das Sharding, bei dem die Trainingsdaten in kleinere Teile aufgeteilt werden, mit denen dann Teilmodelle trainiert werden, die schließlich zusammen das FM bilden. Diese Vorgehensweise kann die Behebung von Problemen mit FMs vereinfachen, bei denen das Risiko besteht, dass private Informationen offengelegt werden. Anstatt das gesamte Modell neu zu trainieren, müssen Sie nur die unerwünschten oder unsachgemäß verwendeten Daten aus dem Shard entfernen und dann das Teilmodell neu trainieren.

Auch Filtern und Blockieren können effektive Ansätze sein. Diese Methoden vergleichen explizit geschützte Informationen mit generierten Inhalten, bevor der Benutzer diese sieht. Bei einer hohen Übereinstimmung wird der Inhalt unterdrückt oder ersetzt, um eine Offenlegung zu vermeiden. Auch die Begrenzung der Häufigkeit, mit der ein bestimmter Inhalt in den Trainingsdaten vorkommt, kann hilfreich sein.

Erklärbarkeit und Überprüfbarkeit verbessern

Zur weiteren Unterstützung einer verantwortungsvollen KI können Sie die Methoden und wichtigsten Faktoren erläutern, die die Ausgaben Ihrer Anwendung beeinflussen. Die Überprüfbarkeit ist ein weiterer wesentlicher Bestandteil verantwortungsvoller KI. Implementieren Sie Mechanismen, mit denen Sie die Entwicklung und den Einsatz Ihrer generativen KI-Anwendung nachverfolgen und überprüfen können. So können Sie die Ursachen von Problemen ermitteln und dazu beitragen, die Governance-Anforderungen zu erfüllen.

Erwägen Sie, relevante Designentscheidungen und Eingaben während des gesamten Entwicklungslebenszyklus zu dokumentieren. Die Erstellung eines nachverfolgbaren Datensatzes kann internen oder externen Teams helfen, die Entwicklung und Funktionsweise Ihrer generativen KI-Anwendung zu bewerten.

Verantwortungsbewusst sein und bleiben

Denken Sie abschließend darüber nach, was Sie tun können, damit Ihre Richtlinien für verantwortungsvolle KI auch zukünftig eingehalten werden. Stellen Sie sicher, dass Sie Gelerntes anwenden und Erfahrungen, die Sie machen, berücksichtigen, um Ihre Sicherheits- und Datenschutzverfahren weiterzuentwickeln. Informieren Sie regelmäßig alle Mitarbeiter in Ihrem Unternehmen über ihre Verpflichtungen zu sicheren generativen KI-Verfahren. Fördern Sie eine Kultur der verantwortungsvollen KI, verwenden Sie die richtigen Tools, um die Modellleistung zu überwachen und über Risiken zu informieren, und geben Sie Ihren Teams die Möglichkeit, das Modell und seine Komponenten bei Bedarf zu überprüfen. Testen, testen und – im Zweifelsfall – erneut testen.

Frage 4:

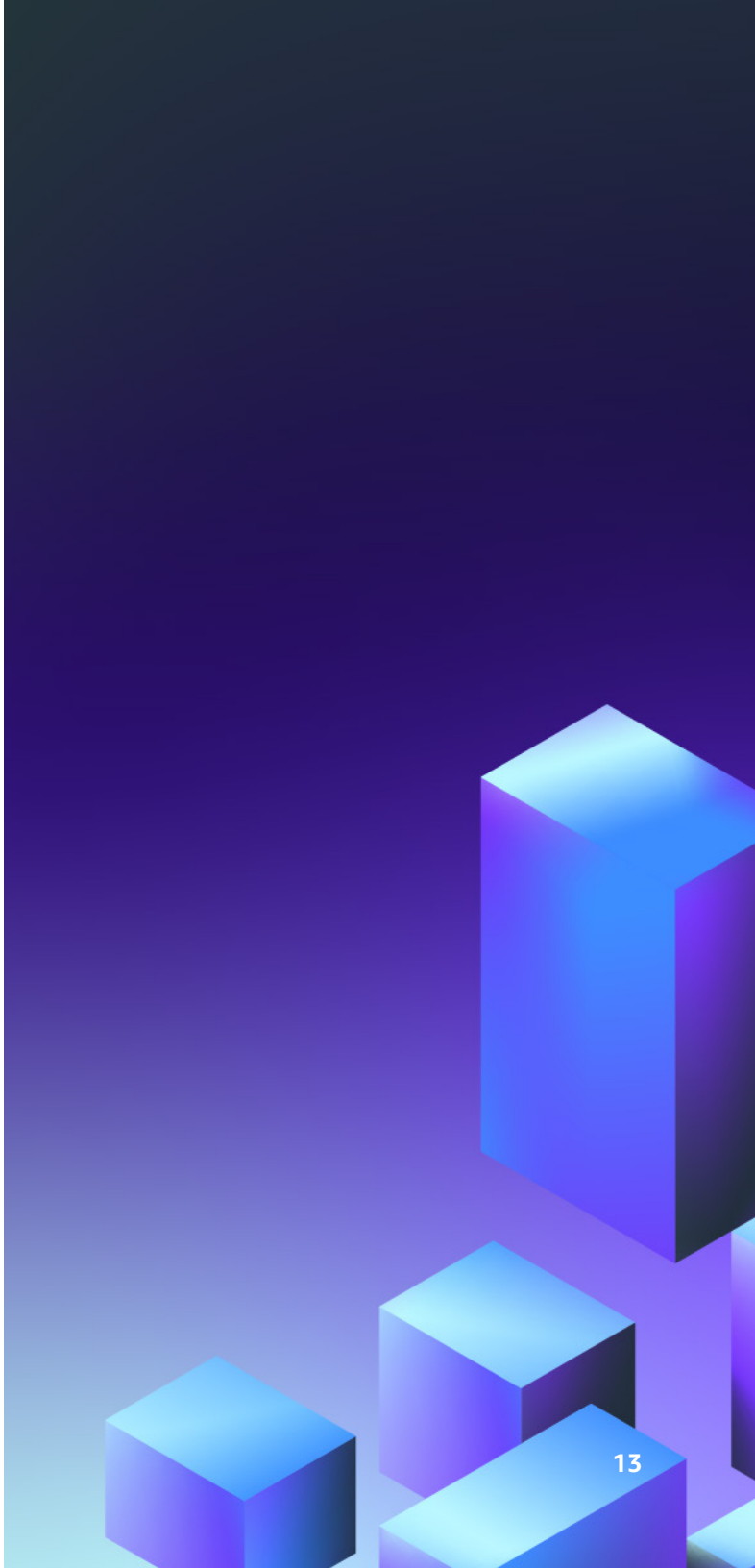
Wo sollten Sie anfangen?

Das Sichern generativer KI-Anwendungen ist kein einfaches Unterfangen und es gibt keine allgemein gültigen Maßnahmen, mit denen Sie dies erreichen können. Wenn Sie jedoch mit dem richtigen Anbieter zusammenarbeiten und die richtigen Tools einsetzen, wird der Weg zum Erfolg viel weniger steinig.

Mit **Amazon Bedrock** lässt sich beispielsweise die Entwicklung sicherer generativer KI-Anwendungen drastisch vereinfachen und beschleunigen. Amazon Bedrock ist ein vollständig verwalteter Service, der FMs von Amazon und führenden KI-Startups über eine API verfügbar macht.

Wenn Sie ein Modell mit Amazon Bedrock anpassen, kann der Service dieses für eine bestimmte Aufgabe optimieren, ohne dass große Datenvolumen kommentiert werden müssen. Amazon Bedrock erstellt dann eine separate Kopie des zugrunde liegenden FM, auf die nur Sie Zugriff haben. Diese private Kopie des Modells wird dann trainiert. Kein Teil Ihrer Daten wird verwendet, um das ursprüngliche Basismodell zu trainieren, so dass Ihre Unternehmensdaten vertraulich und sicher bleiben.

Sie können Ihre **Amazon-VPC**-Einstellungen auch so konfigurieren, dass auf Amazon-Bedrock-APIs zugegriffen und Ihr Modell mit Daten zur Feinabstimmung versorgt wird. Ihre Daten werden sowohl während der Übertragung als auch im Ruhezustand über vom Service verwaltete Schlüssel verschlüsselt. Außerdem können Sie **AWS PrivateLink** nutzen, um Ihre AWS-Cloud-Daten ausschließlich über das AWS-Netzwerk zu Amazon Bedrock zu übertragen, so dass sie nicht dem öffentlichen Internet ausgesetzt sind.



Besserer Datenschutz mit AWS

Ganz gleich, ob Sie generative KI-Anwendungen mit Amazon Bedrock, einem anderen Service (beispielsweise **Amazon SageMaker**) oder Ihren eigenen Tools erstellen, wenn Sie Ihre Anwendungen in AWS ausführen und verwalten, profitieren Sie automatisch von branchenführenden Datenschutzmaßnahmen und -kontrollen.

AWS unterstützt 143 Sicherheitsstandards und Compliance-Zertifizierungen und trägt so dazu bei, die Anforderungen unserer Kunden weltweit zu erfüllen. Ihre gesamten Daten können im Ruhezustand mit Ihren eigenen **AWS Key Management Service** (Amazon KMS)-Schlüsseln verschlüsselt werden, sodass Sie die volle Kontrolle und Transparenz darüber haben, wie Ihre Daten und FMs gespeichert werden und wie auf diese zugegriffen wird.

FAZIT

Nächste Schritte

AWS hat es sich zur Aufgabe gemacht, Sie bei der Entwicklung generativer KI-Anwendungen zu unterstützen, die Ihr Unternehmen voranbringen und Ihnen helfen, Ihre Sicherheits-, Datenschutz- und Compliance-Ziele zu erreichen.

Wir sind fest davon überzeugt, dass generative KI-Anwendungen sicher entworfen, entwickelt und eingesetzt werden können. Uns ist bewusst, dass die Sicherheits- und Datenschutzbedenken in Bezug auf diese Technologien Ihre Berechtigung haben. **Generative KI bringt neue Herausforderungen** bei der Definition, Einschätzung und Entschärfung von Problemen im Zusammenhang mit Datenschutz, geistigem Eigentum, gesetzlicher Kontrolle, Gleichheit und Transparenz mit sich.

Die Einführung neuer Produkte, die zunehmende Komplexität und der zunehmende Umfang von Lösungen, neue Trainingsparameter und ständig größer werdende Datensätze sorgen dafür, dass die Sicherheit generativer KI in Zukunft noch wichtiger sein wird. Indem Sie bereits jetzt eine effektive und umfassende Sicherheitsstrategie für generative KI-Workloads entwickeln, können Sie Ihren Wettbewerbsvorteil ausbauen und sind für die sich schnell nähernde Zukunft gerüstet.

Die gute Nachricht: Die grundlegenden Kontrollen, die für das sichere Entwerfen, Entwickeln und Ausführen generativer KI-Anwendungen erforderlich sind, gibt es bereits seit Jahren – und sie entsprechen bewährten Prinzipien der Cloud-Sicherheit, wie sie beispielsweise beim **AWS-Well-Architected-Framework** zu finden sind.

Indem Sie sich mit den in diesem E-Book beschriebenen Verfahren vertraut gemacht haben, haben Sie bereits den ersten Schritt zum Sichern Ihrer generativen KI-Workloads getan.

Machen Sie jetzt den nächsten Schritt mit AWS. Wir sorgen für detaillierte Einblicke und spezifische Anleitungen, die Sie benötigen, um über neue Themen auf dem Laufenden zu bleiben, Ihre einzigartigen Herausforderungen zu durchdenken und die Vorteile generativer KI voll auszuschöpfen – und das alles bei gleichzeitigem Schutz Ihrer Daten, Ihrer Kunden und Ihres Unternehmens.

Weitere Informationen über generative KI in AWS ›

Schneller Einstieg mit Amazon Bedrock ›

FMs mit Amazon SageMaker erstellen und anpassen ›

Mit AWS Ihre Sicherheit in der Cloud erhöhen ›

Transformieren Sie verantwortungsvolle KI von der Theorie in die Praxis ›