Investitionen in Chaos Engineering als strategische Notwendigkeit

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Investitionen in Chaos Engineering als strategische Notwendigkeit

Table of Contents

Investition in Chaos Engineering als strategische Notwendigkeit

Adrian Hornsby, Amazon Web Services

Januar 2025 (Geschichte der Dokumente)

Chaos Engineering nutzt kontrollierte Störungen, um Systemprobleme und Möglichkeiten zur Vermeidung von Ausfällen und anderen Vorfällen zu identifizieren. Chaos Engineering ist für die Verbesserung widerstandsfähiger Systeme unverzichtbar geworden, aber eine breite Akzeptanz stößt auf Hürden, die sich aus Missverständnissen, kulturellen Widerständen, Ressourcen und der Quantifizierung des Geschäftswerts ergeben. Die Festlegung anfänglicher Ziele trägt dazu bei, die Bemühungen um Chaos Engineering in Gang zu setzen, während die Quantifizierung der Kapitalrendite (ROI) weitere Investitionen rechtfertigt — insbesondere angesichts des wirtschaftlichen Drucks.

In diesem Strategiedokument wird ein ganzheitlicher Ansatz zur Erfassung sowohl quantitativer betrieblicher Verbesserungen als auch qualitativer organisatorischer Vorteile beschrieben. Das ultimative Ziel besteht darin, Chaos Engineering als strategische Notwendigkeit zu behandeln, die mit Cybersicherheit vergleichbar ist, und nicht als ständige Maßnahme zur Kostenrechtfertigung.

Ausfallkosten und das Aufkommen von Chaos Engineering

Das Information Technology Intelligence Consulting (ITIC) schätzt, dass 90 Prozent der Unternehmen mit Kosten von über 300.000$ pro Stunde Ausfallzeit konfrontiert sind, wobei 41 Prozent über 1—5 Millionen $ pro Stunde liegen. Neben unmittelbaren Umsatzeinbußen können Ausfallzeiten auch zu längerfristigen Problemen wie Compliance-Verstößen, gesunkenen Aktienkursen, erheblichen Minderungskosten und sogar zu Markenschäden führen.

Ausfallzeiten werden zwar häufig mit umsatzgenerierenden Online-Systemen in Verbindung gebracht, die negativen Auswirkungen gehen jedoch weit darüber hinaus. Alle großen Unternehmen und Organisationen verlassen sich unabhängig von ihrem primären Umsatzmodell entscheidend auf die Verfügbarkeit ihrer internen Systeme wie Personalwesen und Gehaltsabrechnung.

Ausfallzeiten, die sich auf diese zentralen internen Dienste auswirken, können die Funktionsfähigkeit eines Unternehmens beeinträchtigen und zu erheblichen Betriebsstörungen und finanziellen Auswirkungen führen. Die daraus resultierenden Probleme können Folgendes umfassen:

- Verzögerungen bei der Bezahlung von Mitarbeitern und Lieferanten
- Unfähigkeit, Kundenbestellungen oder Transaktionen zu bearbeiten
- Verstöße gegen sensible Daten, die durch kompromittierte Sicherheitssysteme ermöglicht wurden
- Verlust von Produktivität und Umsatzmöglichkeiten
- Gesetzliche Sanktionen bei Nichteinhaltung
- Schädigung des Rufs der Marke

Chaos Engineering führt bewusst zu kontrollierten Störungen. Der Einsatz von Chaos Engineering, um die Reaktion des Systems auf Beeinträchtigungen zu verstehen oder zu überprüfen, ist zu einer wichtigen Praxis für die Verbesserung der Widerstandsfähigkeit von Systemen geworden. Chaos Engineering ermöglicht es Ihrem Unternehmen, proaktiv Probleme aufzudecken, Resilienzmechanismen zu validieren und letztendlich das Risiko ungeplanter Ausfallzeiten und der damit verbundenen Kosten zu reduzieren. Zu den Vorteilen von Chaos Engineering gehören:

- Aufdeckung technischer Schulden
- Training einsatzfähiger Muskeln
- Vertrauen in Systeme aufbauen
- Identifizierung von Fehlerquellen

- Verbesserung der Überwachung und Beobachtbarkeit
- Unterstützung des experimentellen Lernens
- Bereitstellung verbesserter Widerstandsfähigkeit zur Reduzierung von Ausfallzeiten

Da Systeme immer komplexer werden und die Kundenerwartungen steigen, gewinnt Chaos Engineering zunehmend an Bedeutung. Gartner empfiehlt Chaos Engineering als wichtige Methode für Unternehmen, um ungeplante Ausfallzeiten zu reduzieren und die Widerstandsfähigkeit zu verbessern.

Die Herausforderungen bei der Einführung von Chaos Engineering

Obwohl Chaos Engineering eine immer wichtigere Methode zur Verbesserung der Widerstandsfähigkeit von Systemen darstellt, kann ihre Einführung auf die folgenden Hindernisse stoßen:

- Fehleinschätzungen in Bezug auf Risiken – Eine weit verbreitete Fehleinschätzung ist, dass Chaos Engineering nur in Produktionsumgebungen angewendet wird, was zu Bedenken hinsichtlich übermäßiger Risiken führt. Diese Auffassung ist auf mangelndes Verständnis für den systematischen und kontrollierten Charakter von Chaos-Engineering-Praktiken zurückzuführen. Wie im AWS Well-Architected Framework erwähnt, führen Sie die Fehlersimulation zunächst in einer Nicht-Produktionsumgebung durch.
- Langfristiger Geschäftswert – Die Vorteile von Chaos Engineering stellen sich allmählich ein, sodass es schwierig ist, den Geschäftswert zu quantifizieren und die Anfangsinvestition zu rechtfertigen. Der langsamere ROI macht es für Unternehmen schwierig, Prioritäten zu setzen und sich an Chaos Engineering zu halten.
- Qualifikations- und Fachkräftemangel – Chaos Engineering erfordert einzigartige Fähigkeiten und Fachkenntnisse, die in Ihrem Unternehmen möglicherweise nicht ohne Weiteres verfügbar sind. Der Aufbau oder Erwerb dieses Fachwissens kann ein erhebliches Hindernis sein, insbesondere für Organisationen, die mit der Praxis noch nicht vertraut sind und über begrenzte Ressourcen verfügen.

Der Rest dieses Strategiedokuments wird sich hauptsächlich auf die zweite Herausforderung konzentrieren, die darin besteht, den geschäftlichen Nutzen von Chaos Engineering aufzuzeigen.

Die sich häufenden Auswirkungen von Chaos Engineering

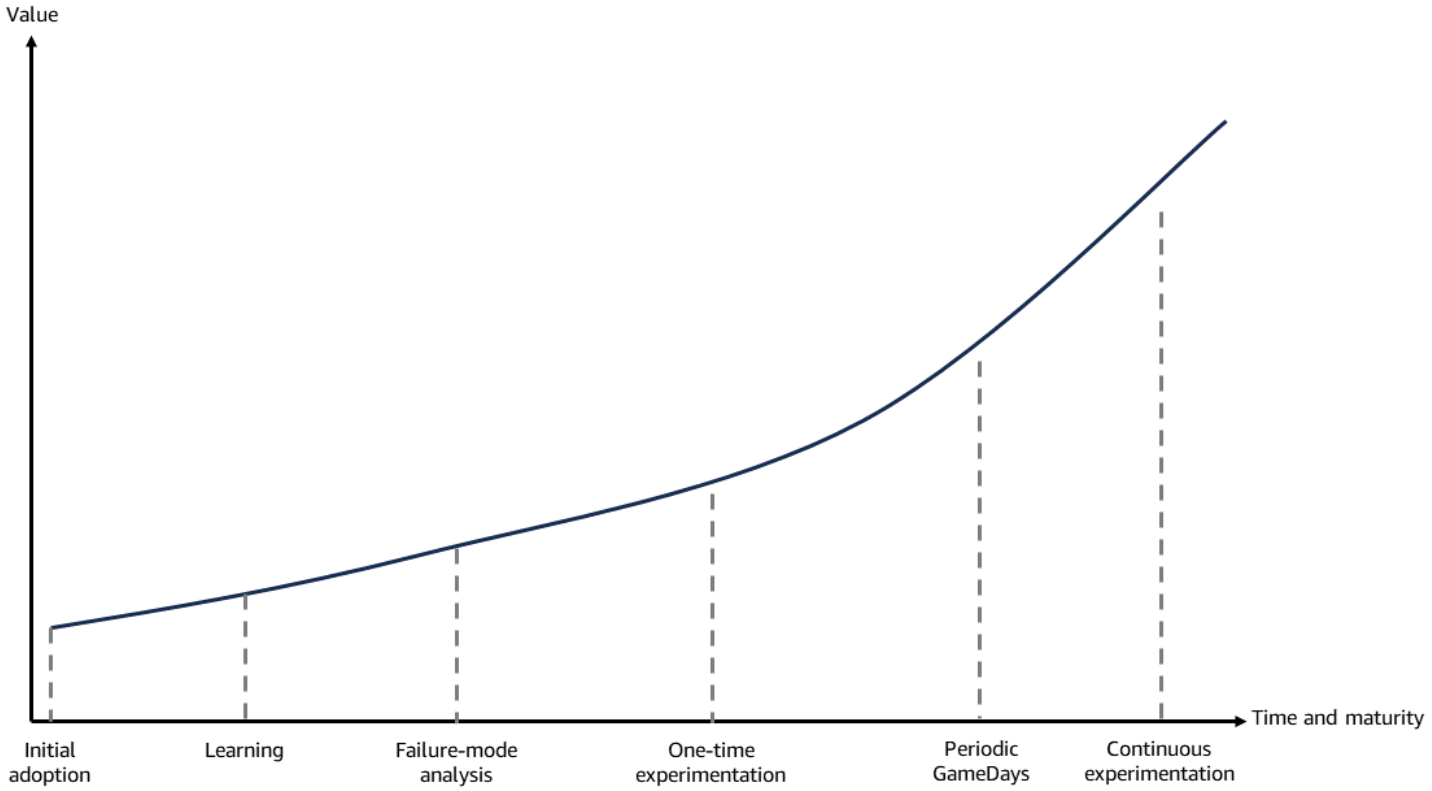
Im Gegensatz zu herkömmlichen Technologieprojekten mit klar definierten Start- und Enddaten ist Chaos Engineering eine kontinuierliche Praxis des kontinuierlichen Lernens und der kontinuierlichen Verbesserung der Systemresistenz. Die Vorteile von Chaos Engineering nehmen im Laufe der Zeit zu.

In dem Maße, wie sich Systeme weiterentwickeln und immer komplexer werden, entstehen neue Ausfallarten. Es sind mehr Chaos-Experimente erforderlich, um potenzielle Probleme zu identifizieren. Die Behebung eines Problems kann Monate dauern, insbesondere in großen Unternehmen mit komplizierten Systemen und Prozessen oder wenn Fehler externen Dienstleistern zuzuschreiben sind.

Der kulturelle Wandel hin zur Nutzung von Misserfolgen als Chance zum Lernen und Verbessern nimmt im Laufe der Jahre zu und ist in der Organisation tief verwurzelt. Investitionen in die Automatisierung von Chaos-Engineering-Experimenten und die Entwicklung unterstützender Tools tragen weiterhin zur Rationalisierung und Verbesserung der Chaos-Engineering-Praxis bei. Der Aufbau dieses institutionellen Wissens und Verständnisses von Systemresistenz ist ein schrittweiser Prozess, der sich im Laufe der Zeit ansammelt. Das Wissen, die Prozesse und die Werkzeuge, die durch Chaos Engineering entwickelt wurden, gewinnen an Wert, wenn die Praxis mit den sich ständig weiterentwickelnden Systemen reift.

Das folgende Diagramm zeigt, wie der Wert im Laufe der Zeit steigt, wenn die Einführung von Chaos die folgenden Phasen durchläuft:

- Erste Annahme
- Lernen
- Analyse des Fehlermodus
- Einmalige Experimente
- Periodisch GameDays
- Kontinuierliches Experimentieren



Wie in der Abbildung dargestellt, setzen die Vorteile von Chaos Engineering häufig ein, bevor ein Fehler in das System eindringt. Der Prozess der Planung und Gestaltung von Chaosexperimenten selbst bietet unmittelbaren Nutzen. Die Identifizierung potenzieller Ausfallszenarien, einzelner Fehlerquellen und unsicherer Bereiche im System führt zu Verbesserungen.

Beispielsweise hilft das Aufschreiben von Ausfallszenarien und die Erörterung der möglichen kaskadierenden Auswirkungen, ein Prozess, der als Fehlermodus- und Einflussanalyse (FMEA) bezeichnet wird, dabei, offensichtliche Schwächen oder Lücken aufzudecken, die möglicherweise übersehen wurden. Ihr Unternehmen kann diese Probleme proaktiv angehen, noch bevor das System vorsätzlichen Störungen ausgesetzt wird. Weitere Informationen finden Sie im Framework für die Resilienzanalyse.

Darüber hinaus bringt der verstärkte Fokus auf Systembeobachtbarkeit und -überwachung, der häufig mit Chaos-Engineering-Initiativen einhergeht, sofort Vorteile. Ein besserer Einblick in das Systemverhalten und die Ausfallarten hilft dem Team, die normalen Betriebsbedingungen des Systems besser zu verstehen. Ein besserer Einblick hilft dem Team auch zu verstehen, wie sich die Betriebsbedingungen verschlechtern, anpassen und versagen, wenn sie an ihre Grenzen stoßen.

Sowohl der Modus für einmaliges Experiment als auch der GameDay Modus für regelmäßige Experimente sind eher manuelle Ansätze als der Modus für kontinuierliche Experimente. Sie

erfordern einen eher praxisnahen und explorativen Prozess, bei dem Ingenieure anhand ihrer Beobachtungen und Experimente aktiv Hypothesen formulieren und verfeinern.

Der Modus des kontinuierlichen Experimentierens ist dagegen stärker automatisiert. Dieser Modus konzentriert sich auf die kontrollierte und iterative Ausführung genehmigter und validierter Hypothesen. Er nutzt Automatisierung und Integration in den Entwicklungsprozess durch eine spezielle Chaos-Pipeline, um konsistente und wiederholbare Experimente zu gewährleisten.

Initiativen zur Chaostechnik an der Basis

Die Reise zur Chaos-Technik beginnt oft an der Basis, wo Entwicklungsteams Bedürfnisse ermitteln und selbstständig mit Chaos Engineering experimentieren.

Bei diesem Basisansatz experimentieren, lernen und verfeinern Teams ihre Chaos-Engineering-Praktiken. Der Wert von Chaos Engineering kann anhand der folgenden konkreten Ergebnisse demonstriert werden:

- Weniger Vorfälle
- Bessere Beobachtbarkeit
- Schnellere Wiederherstellungszeiten
- Verbesserte und kontinuierliche Systemausfallsicherheit

Chaos-Engineering-Initiativen an der Basis entstehen in der Regel unter bestimmten organisatorischen Bedingungen. Sie erfordern ein Umfeld mit einem hohen Maß an technischer Autonomie, in dem Teams die Freiheit haben, ohne übermäßige bürokratische Hindernisse zu experimentieren und Innovationen zu entwickeln. Lokales Fachwissen in den Bereichen Resilienztechnik oder verteilte Systeme ist von entscheidender Bedeutung, da es die technische Grundlage für das Verständnis und die Durchführung von Chaosexperimenten bildet. Am wichtigsten ist, dass sich diese Initiativen oft auf Chaos-Champions stützen — leidenschaftliche Menschen, die den Wert von Chaos Engineering verstehen. Chaos-Champions sind bereit, sich für die Einführung von Chaos Engineering einzusetzen, ihre Kollegen weiterzubilden und erste Experimente voranzutreiben. Ohne organisatorische Freiheit, technisches Fachwissen und motivierte Champions schlagen die Bemühungen der Chaos-Technik an der Basis selten Fuß, unabhängig von ihren potenziellen Vorteilen.

Die Rolle von Zielen bei der Einführung von Chaos Engineering

Es ist üblich, dass die ursprünglichen Ziele organisch aus den Bemühungen eines Unternehmens zur Chaosingenieurierung an der Basis hervorgehen. Aus dem Bedürfnis heraus, ihre eigenen wiederkehrenden Probleme zu lösen, setzen sich diese Teams oder Gruppen häufig mit Methoden der Chaosingenieurtechnik auseinander, ohne dass dies ausdrücklich genehmigt oder von höheren Ebenen priorisiert wird.

Teams können diese Ergebnisse nutzen, um überzeugende Argumente für eine breitere Einführung in der Organisation vorzubringen und so effektiv zu einem Testgelände für andere Teams zu werden.

Wenn die Vorteile der Bemühungen an der Basis zu groß geworden sind, um sie zu ignorieren, können diese Teams ihre Anstrengungen und ihr Wissen auf die Führung ausweiten und sich Ziele setzen. Diese erhöhte Transparenz kann die Verabschiedung unternehmensweiter Resilienzziele erleichtern und zu der Unterstützung und den Ressourcen führen, die für die Implementierung von Chaos Engineering erforderlich sind.

Ziele, insbesondere solche, die von der Unternehmensleitung vorangetrieben und als Reaktion auf erhebliche Ausfälle festgelegt wurden, spielen eine entscheidende Rolle, wenn es darum geht, die Einführung von Chaos-Engineering-Praktiken voranzutreiben. Zu den gängigen Arten von Zielen gehören die folgenden:

- Verfügbarkeitsziele zur Identifizierung und Reduzierung von Single Points of Failure (SPOF)
- Ziele zur Wiederherstellung von Diensten zur Verbesserung der Fähigkeit zur Wiederherstellung nach Störungen oder Ausfällen
- Ziele im Hinblick auf das Nutzererlebnis zur Erreichung bestimmter Service-Level-Ziele () SLOs
- Metrikorientierte Ziele zur Erfassung der Fortschritte bei der Minderung bekannter Verfügbarkeitsrisiken und der Umsetzung empfohlener Resilienzmaßnahmen
- Regulatorische und Compliance-Ziele zum Nachweis der betrieblichen Belastbarkeit

Weitere Informationen zu einigen dieser Zieltypen und dazu, wie Amazon und andere Organisationen Ziele bei der Einführung von Chaos Engineering verwendet haben, finden Sie in Anhang A.

Diese Ziele dienen als überzeugende Begründung und bieten einen gezielten, umsetzbaren Ansatz, um die Einführung von Chaos Engineering voranzutreiben. Zu Beginn dienen Ziele als

Näherungswerte für herkömmliche ROI-Metriken. Die Ziele bieten eine überzeugende Begründung, wenn es schwierig sein könnte, quantifizierbare Berechnungen des ROI für Resilienz zu erhalten. Ohne solche Ziele zu Beginn der Einführung besteht die Gefahr, dass die Chaos-Engineering-Praxis ihre Wirksamkeit nicht unter Beweis stellt und die Zustimmung einer breiteren Organisation nicht findet.

Der Übergang von Zielen zur Messung des ROI

Wenn die Verfahren ausgereift sind und die ursprünglichen Ziele erreicht sind, verlagert sich der Schwerpunkt schließlich von der Festlegung von Zielen hin zur Quantifizierung der konkreten finanziellen Vorteile von Chaos Engineering — der Kapitalrendite (ROI). Dieser Wandel ist hauptsächlich auf zwei Gründe zurückzuführen:

- Wirtschaftliche Überlegungen
- Wahrung des Kundenerlebnisses und des Kundenvertrauens

Wirtschaftliche Überlegungen

In Zeiten von Wirtschaftswachstum und gesunden Finanzen benötigen Unternehmen oft keine umfassende Begründung, um konkrete Ziele für Chaos-Engineering-Strategien festzulegen. Veränderungen in der Finanzlandschaft haben jedoch viele Unternehmen dazu veranlasst, ihre Investitionen neu zu bewerten, und Chaos-Engineering-Implementierungen müssen einen quantifizierten ROI bieten.

Diese Unternehmen haben nun die Aufgabe, klare, traditionelle ROI-Metriken festzulegen, um den Wert und die Auswirkungen von Chaos-Engineering-Praktiken aufzuzeigen. Diese Herausforderung wird durch das Präventionsparadoxon noch komplizierter. Das Präventionsparadoxon tritt auf, wenn eine erfolgreiche Verhütung von Zwischenfällen es schwieriger macht, die Investition zu rechtfertigen, weil die Beteiligten dazu neigen, vermiedene Katastrophen zu unterschätzen. Selbst Unternehmen mit einer tief verwurzelten Kultur betrieblicher Exzellenz stehen unter dem Druck, ROI-Kennzahlen zu verwenden, um die fortgesetzte Einführung von Chaos Engineering zu rechtfertigen.

Wahrung des Kundenerlebnisses und des Kundenvertrauens

Die Aufrechterhaltung einer zielorientierten Widerstandsfähigkeit kann auf lange Sicht eine Herausforderung sein. Sobald ein anfängliches Ziel wie das Erreichen eines Ziels für die Wiederherstellungszeit erreicht ist, wird es schwierig, kontinuierliche Investitionen in Chaos-Engineering bis zum nächsten größeren Ausfall zu rechtfertigen. Das Auf und Ab der Investitionen führt zu einem reaktiven Sägezahnzyklus. Bei jedem neuen Ausfall steigen die Investitionen in Resilienz, wobei ein neues Ziel verfolgt wird, die Grundursache zu bekämpfen. Sobald das neue Ziel erreicht ist, sinken die Investitionen bis zum nächsten Vorfall, wodurch der reaktive Kreislauf wieder in Gang kommt.

Die Ausfälle, die diesen reaktiven Ansatz vorantreiben, wirken sich negativ auf die Kunden aus. Die zentrale Frage: Wie viele größere Ausfälle werden Kunden tolerieren, bevor sie einen Dienstleister zugunsten eines widerstandsfähigeren Wettbewerbers verlassen?

Quantifizierung des ROI von Chaos Engineering

Derzeit bieten nur sehr wenige veröffentlichte Ressourcen umfassende Methoden oder reale Daten zur Quantifizierung der langfristigen Kapitalrendite (ROI) von Chaos Engineering.

In dem paper The Business Case for Chaos Engineering bietet Netflix eine wertvolle Gleichung zur Berechnung des ROI für Chaos Engineering. Diese Gleichung bietet einen Ausgangspunkt für Unternehmen, die sich auf ihre Reise nach Chaos Engineering begeben.

Die Gleichung erfordert, dass Sie die Kosten für Folgendes genau schätzen:

- Vermeidbare und nicht vermeidbare Ausfälle
- Kosten für die Implementierung des Chaos Engineering-Programms
- Kosten für Schäden, die durch Chaos verursacht werden

Als durch Chaos verursachter Schaden werden negative Auswirkungen oder Störungen bezeichnet, die dadurch entstehen, dass im Rahmen von Chaos-Engineering-Experimenten bewusst Fehler oder turbulente Bedingungen in ein System eingebracht werden. Die Gleichung erfordert eine Schätzung der Kosten vermeidbarer und nicht vermeidbarer Ausfälle, der Kosten für die Implementierung von Chaos-Engineering-Programmen und der durch Chaos verursachten Schäden.

Es ist eine schwierige Aufgabe, mit Sicherheit festzustellen, welche Probleme durch ein Chaos-Engineering-Programm hätten vermieden werden können. Es erfordert eine hypothetische Analyse, bei der die Grundursachen von Problemen untersucht und darüber spekuliert wird, wie Experimente im Bereich Chaos-Engineering zu ihrer Identifizierung beigetragen haben könnten. Diese Analyse ist schwierig, da moderne Systeme hochkomplex sind und zahlreiche Interdependenzen und Interaktionen zwischen verschiedenen Komponenten, Diensten und Bibliotheken von Drittanbietern aufweisen. Darüber hinaus sind Fehler in Systemen oft nicht deterministisch, und es kann schwierig sein, die Bedingungen, die Fehler verursachen, im Nachhinein vollständig zu verstehen.

Obwohl der von Netflix vorgeschlagene Ansatz einige Einschränkungen aufweist, bietet er eine gute Grundlage für Unternehmen, die beginnen, sich mit Chaos Engineering zu beschäftigen. Die Gleichung kann Ihnen bei der Schätzung der Kosten und des potenziellen Nutzens helfen, was Ihnen hilft, Entscheidungen über die Implementierung eines solchen Programms zu treffen. Da Unternehmen auf ihrem Weg zum Chaos Engineering jedoch immer weiter voranschreiten, ist es wichtig, die ROI-Bewertung um eine ganzheitlichere Perspektive zu erweitern.

Dieser ganzheitliche Ansatz wird nicht nur die direkten Vorteile reduzierter Ausfälle und Engineering-Kosten nutzen, sondern auch die langfristigen, transformativen Auswirkungen auf die allgemeine Widerstandsfähigkeit des Unternehmens hervorheben. Er erfasst die Vorteile und umfassenderen Auswirkungen von Chaos Engineering auf die Organisation, um den wahren Wert und die Auswirkungen von Chaos Engineering genauer darzustellen.

Ein ganzheitlicher Ansatz zur ROI-Quantifizierung

Bei einer ganzheitlichen ROI-Bewertung müssen nicht nur quantitative Maßnahmen, sondern auch qualitative Faktoren berücksichtigt werden. Der ganzheitliche Ansatz erfordert reale Daten von Organisationen, die Chaos Engineering in großem Umfang über längere Zeiträume anwenden. Sie können Daten von Basisprojekten und Zielen bis hin zu beliebigen ROI-Daten für Gleichungsansätze verwenden, die Sie gesammelt haben.

Quantitative Maßnahmen konzentrieren sich auf Mengen oder Häufigkeiten. Die Messungen sind objektiv und können statistisch analysiert werden. Beispiele hierfür sind Umfragen, Experimente und Datenanalysen. Quantitative Maßnahmen können Folgendes umfassen:

- Kennzahlen zu Vorfällen
- Kosten
- Verbesserungen
- Compliance
- Adoptionsraten
- Kundenzufriedenheit

Durch die Verfolgung quantitativer Maßnahmen können die direkten betrieblichen Vorteile von Chaos Engineering aufgezeigt werden.

Qualitative Maßnahmen sind beschreibend und konzentrieren sich auf das Verständnis von Erfahrungen und Meinungen. Sie sind oft subjektiv und können nicht einfach numerisch gemessen werden. Beim Chaos Engineering erfassen qualitative Maßnahmen die umfassenderen Auswirkungen auf die Organisation. Qualitative Maßnahmen können Folgendes umfassen:

- Vertrauen der Mitarbeiter
- Kultureller Wandel
- Zusammenarbeit

- Effektivität des Trainings
- Bindung von Talenten
- Ruf der Marke
- Wettbewerbsvorteil

Wenn Sie sowohl die quantitativen finanziellen Auswirkungen als auch die qualitativen organisatorischen Vorteile berücksichtigen, können Sie fundiertere Entscheidungen über weitere Investitionen im Bereich Chaos Engineering treffen und gleichzeitig eine Resilienzkultur fördern.

Weitere Informationen zu diesen Maßnahmen und dem damit verbundenen Rahmen zur Klassifizierung von Vorfällen finden Sie in Anhang B und Anhang C.

Der Übergang von ROI zu Chaos Engineering als strategische Notwendigkeit

Obwohl es verlockend ist, den ROI zu überwachen, führen die Herausforderungen bei der Messung des Nutzens von Chaos Engineering häufig dazu, dass Unternehmen unmittelbaren, kurzfristigen Effizienzsteigerungen Vorrang vor strategischen Investitionen in Resilienz einräumen. Bei diesem Ansatz wird Chaos Engineering als Hauptfaktor für Resilienz und die Wettbewerbsvorteile, die sich aus der Vermeidung von Ausfällen ergeben, übersehen. Der wahre Wert von Chaos Engineering besteht darin, future Ausfälle zu verhindern. Chaos Engineering unterstützt die langfristige Geschäftskontinuität.

Anstatt sich auf den ROI zu konzentrieren, sollten Sie Chaos Engineering wie Cybersicherheit behandeln. Wie im Forbes-Artikel Cybersicherheit als strategische Investition: Wie die ROI-Optimierung zu einer sichereren Zukunft führen kann, erklärt, sollte Cybersicherheit nicht als Kostenstelle oder obligatorische Ausgabe für Unternehmen betrachtet werden, da diese Denkweise den strategischen Wert nicht berücksichtigt, den robuste Cybersicherheitsmaßnahmen im Laufe der Zeit bieten können. Stattdessen argumentiert der Autor, dass Unternehmen neue Wege für Innovation, betriebliche Effizienz und Differenzierung innerhalb ihrer jeweiligen Märkte erschließen können, indem sie ihre Sichtweisen ändern und Cybersicherheit als langfristige Investition betrachten, die Wettbewerbsvorteile schafft. Durch diesen Ansatz kommt der Autor zu dem Schluss, dass Chief Information Security Officers (CISOs) die Zustimmung und Finanzierung der Führung besser sicherstellen können. Sie können ihre Unternehmen dann so positionieren, dass sie Wettbewerber in einer zunehmend riskanten Cyberlandschaft hinter sich lassen. Diese langfristige, strategische Wertschöpfung durch Cybersicherheit entspricht den kontinuierlichen Verbesserungen, die den Chaos-Engineering-Praktiken innewohnen.

Während die Sicherheit die Fähigkeit eines Unternehmens schützt, Anlagen zu betreiben und zu schützen, trägt Chaos Engineering dazu bei, die Verfügbarkeit, Zuverlässigkeit und Wiederherstellbarkeit von Kernsystemen und -diensten sicherzustellen. Um langfristigen Nutzen und Wettbewerbsvorteile zu erzielen, sollten Sie Chaos Engineering als Kernkompetenz und strategische Notwendigkeit betrachten und nicht als eine Initiative, die ständig begründet werden muss.

Das folgende Diagramm zeigt die Entwicklung von Chaos Engineering von der Basis über Ziele und ROI bis hin zur Strategie.

An der Basis experimentieren einzelne Teams in der Regel unabhängig voneinander und orientieren sich dabei an den lokalen Bedürfnissen. Diese Experimente werden von engagierten Ingenieuren unterstützt, die ihren Nutzen durch weniger Zwischenfälle und eine verbesserte Beobachtbarkeit unter Beweis stellen.

Wenn sich diese Bemühungen als erfolgreich erweisen, können Teams ihr Lernen in Führungspositionen umwandeln. Mit dieser Transparenz gehen die Bemühungen in eine zielorientierte Phase über. Die Organisation legt formelle Ziele für Resilienz und Erholung fest, die durch Ressourcen und Unterstützung für eine umfassendere Umsetzung unterstützt werden.

Und schließlich reift Chaos Engineering über die ständige Begründung des ROI hinaus, um als strategische Notwendigkeit anerkannt zu werden, ähnlich wie bei der Cybersicherheit. In dieser Phase wird Chaos Engineering vollständig in die organisatorischen Prozesse integriert. Die Umsetzung konzentriert sich eher auf die langfristige Widerstandsfähigkeit als auf kurzfristige Kennzahlen. Chaos Engineering wird als eine Kernkompetenz betrachtet, die für die Aufrechterhaltung eines Wettbewerbsvorteils und des Kundenvertrauens unerlässlich ist.

Integrieren Sie Chaos Engineering in Ihr Unternehmen

Beachten Sie die folgenden Vorschläge, um der Chaos-Technik die gleiche Bedeutung wie der Sicherheit einzuräumen:

- Chaos-Engineering als unverhandelbare Praxis etablieren – So wie Cybersicherheit als grundlegende Anforderung für Unternehmen angesehen wird, sollten Sie Chaos Engineering als obligatorische Praxis zur Gewährleistung der Widerstandsfähigkeit und Zuverlässigkeit von Systemen betrachten. Integrieren Sie Chaos Engineering in die Prozesse, Tools und Kultur Ihres Unternehmens, anstatt es als optionale oder diskretionäre Aktivität zu betrachten. Weitere Informationen finden Sie im Leitfaden zum Resilience Lifecycle Framework.
- Sicherstellung der Zustimmung und Unterstützung auf Führungsebene – Wie bei Sicherheitsinitiativen müssen die Bemühungen um Chaos Engineering auf Zustimmung und aktive Unterstützung durch die Geschäftsleitung angewiesen sein. Dazu gehört die Zuweisung spezieller

Ressourcen, Budgets und Mitarbeiter für die Implementierung und Aufrechterhaltung von Chaos Engineering-Praktiken im gesamten Unternehmen.

- Implementierung von Steuerung und Aufsicht – Ähnlich wie bei einem CISO- und Sicherheits-Governance-Framework sollten Sie ein eigenes Chaos Engineering-Team oder einen Chief Resilience Officer einrichten. Dieses Team oder diese Rolle ist für die Überwachung und Koordination der Chaos-Engineering-Maßnahmen in verschiedenen Teams und Geschäftsbereichen verantwortlich.
- Integrieren Sie Chaos Engineering in Entwicklungs- und Betriebszyklen – So wie Sicherheitspraktiken in die Softwareentwicklungs- und -bereitstellungsprozesse integriert sind, machen Sie Chaos Engineering zu einem nahtlosen Bestandteil des Softwareentwicklungs- und -bereitstellungszyklus.
- Führen Sie regelmäßig Chaos-Engineering-Übungen und -Simulationen durch – Ähnlich wie bei Simulationen zu Sicherheitsverletzungen und Incident-Response-Übungen sollten Sie regelmäßig Experimente zur Chaos-Technik durchführen, um die Fähigkeiten zur Reaktion auf Vorfälle zu validieren und potenzielle blinde Flecken proaktiv zu identifizieren.
- Verwenden Sie Chaos Engineering zur Verwaltung von Runbooks – Wie bei der Durchführung von Sicherheitsüberprüfungen sollten Sie auch Chaos Engineering-Experimente verwenden, um die Effektivität und Genauigkeit von Runbooks für die Reaktion auf Vorfälle und die Wiederherstellung zu überprüfen. Darüber hinaus können Chaos-Engineering-Experimente als realistische Simulationen für Techniker auf Abruf dienen, um die Ausführung von Runbook-Verfahren zu üben. Simulationen helfen Ingenieuren dabei, ihr funktionstüchtiges Muskelgedächtnis aufrechtzuerhalten und für den Umgang mit realen Ereignissen gewappnet zu sein.
- Förderung einer Kultur der Resilienz – Wie bei Schulungen zum Sicherheitsbewusstsein sollten Sie auch hier in die Ausbildung zur Chaosmechanik und in Initiativen zum Wissensaustausch investieren, um eine Kultur der Resilienz zu fördern. Dazu gehören Schulungsprogramme, funktionsübergreifende Zusammenarbeit und Anreize für Teams, die Chaos-Engineering-Praktiken anwenden.
- Messung und Berichterstattung über Resilienzkennzahlen – Überwachen Sie die Resilienzkennzahlen regelmäßig und melden Sie sie den Stakeholdern. Verwenden Sie die in diesem Dokument erörterten quantitativen und qualitativen Kennzahlen als Ausgangspunkt.
- Resilienz als Wettbewerbsvorteil betrachten – Cybersicherheitsmaßnahmen können einen Wettbewerbsvorteil bieten. Betrachten Sie auch Ihre Fähigkeiten im Bereich Chaos Engineering und Resilienz als Alleinstellungsmerkmal, das Ihnen hilft, Ihren Kunden zuverlässigere und vertrauenswürdigere Dienste anzubieten.

Unterstützung durch die Geschäftsleitung gewinnen

Bei Chaos Engineering fehlt es oft an einem klaren Eigentümer innerhalb der traditionellen Verantwortlichkeiten der C-Suite. Der CEO kümmert sich um Wachstum, Rentabilität und Marktführerschaft. Der CFO konzentriert sich auf finanzielle Leistung, Kostenkontrolle und Risikomanagement. Der CTO priorisiert Technologiestrategie, Produkt-Roadmaps und technische Exzellenz. Der CISO überwacht Sicherheit und Compliance.

Da keine einzelne Führungskraft wirklich über Resilienz verfügt, ist es oft schwierig, Zustimmung und Unterstützung zu gewinnen. Systemausfälle wirken sich jedoch auf den Umsatz, die Kundenzufriedenheit und den Ruf der Marke aus, was für den CEO und den CFO ein Problem darstellt. Der CTO und der CISO sind mit der Umsetzung von Resilienzmaßnahmen beauftragt, aber ihnen fehlt möglicherweise ein organisatorisches Mandat. Diese Unklarheit kann strategische Investitionen und die Ausrichtung der Organisation auf eine gemeinsame Resilienzstrategie behindern.

Diese Unklarheit macht es auch schwierig, die Zustimmung der Geschäftsleitung für Resilienzinitiativen wie Chaos Engineering zu gewinnen. Schließlich jonglieren Führungskräfte auf C-Level mit einer Vielzahl strategischer Prioritäten: Wachstum, Innovation, Kundenerlebnis, Compliance und mehr.

Um Führungskräften auf C-Ebene den Wert von Chaos Engineering effektiv zu vermitteln, sollten Sie die folgenden Ansätze in Betracht ziehen:

- Ermitteln Sie die wichtigsten Anliegen und Entscheidungsträger Ihrer Führungskräfte.

  Sorgen sich die Führungskräfte der C-Suite beispielsweise um Kundenabwanderung, Einhaltung gesetzlicher Vorschriften, Kostensenkung oder Wettbewerbsdruck? Positionieren Sie Chaos Engineering als Multiplikator, der sich an den individuellen Herausforderungen und Zielen des Unternehmens orientiert.
- Identifizieren Sie gemeinsame Ziele und strategische Ergebnisse.

  Wie unterstützt Ihre Chaos-Engineering-Strategie die Wachstumsstrategie, das Kundenerlebnis, die Marktchancen und die betriebliche Effizienz des gesamten Unternehmens? Priorisieren Sie Initiativen auf der Grundlage von Zielen, Geschäftsauswirkungen, ROI und dem Risiko, die Initiativen nicht umzusetzen.
- Kommunizieren Sie die Effektivität Ihrer Chaos-Engineering-Strategie anhand von wichtigen Resilienzindikatoren in quantifizierbarer Form.

Beginnen Sie mit diesen vier wichtigen Resilienzindikatoren: Verfügbarkeit, Erkennungszeit, Reaktionszeit und Wiederherstellungszeit. Verknüpfen Sie diese direkt mit Geschäftsergebnissen wie Umsatz, Kosteneinsparungen und dem Ruf der Marke.

- Verlieren Sie sich nicht in den technischen Details.

  Konzentrieren Sie sich auf die allgemeine Stimmung und die messbaren Auswirkungen auf das Geschäft. Der Unternehmensleitung sind die Ergebnisse wichtig, die das Wachstum vorantreiben, das Kundenvertrauen stärken und Innovationen fördern.

Das Präventionsparadoxon

Wenn Fehler erfolgreich behoben werden, bevor sie auftreten, wird es schwierig, die Beteiligten vom Wert und der Notwendigkeit der getroffenen Präventivmaßnahmen zu überzeugen. Dieses Phänomen wird als Präventionsparadoxon bezeichnet. Das Präventionsparadoxon ist das größte Hindernis für die Integration von Chaos Engineering als strategische Notwendigkeit, und es ist auf die inhärenten Vorurteile der menschlichen Kognition zurückzuführen.

Der Y2K-Bug ist ein gutes Beispiel für dieses Paradoxon. Jahrelange Vorbereitung und Milliarden von Dollar wurden in die Aktualisierung von Computersystemen weltweit investiert. Der reibungslose Übergang ins Jahr 2000 wurde jedoch von vielen als Beleg für den überzogenen Charakter der Y2K-Bedenken gewertet. Der Erfolg der unternommenen Präventivmaßnahmen wurde selten anerkannt.

Dieses Präventionsparadoxon stellt Unternehmen, die heute in Chaos Engineering investieren, weiterhin vor Herausforderungen. Wenn potenzielle Ausfälle durch proaktive Maßnahmen erfolgreich abgewendet werden können, kann das bloße Ausbleiben einer Katastrophe es paradoxerweise schwierig machen, die für die Prävention aufgewendeten Ressourcen zu rechtfertigen.

Die Hauptursache für dieses Phänomen liegt in der Art und Weise, wie unser Verstand darauf ausgelegt ist, Informationen zu verarbeiten. Die kognitiven Prozesse des Menschen sind darauf ausgerichtet, auf tatsächliche Ereignisse und sichtbare Ergebnisse zu reagieren und sich daran zu erinnern. Wenn eine Katastrophe verhindert wird, gibt es kein dramatisches Narrativ, an dem man festhalten oder teilen könnte. Ein weiterer Aspekt des Präventionsparadoxons ist die Voreingenommenheit im Nachhinein. Nach einem Nichtereignis neigen Menschen dazu, zu dem Schluss zu kommen, dass nichts passiert ist, es also kein wirkliches Problem war. Die Möglichkeit, dass durch geeignete Vorsichtsmaßnahmen ein echtes Problem verhindert wurde, wird nicht anerkannt. Dieser psychologische blinde Fleck stellt Unternehmen vor eine ständige

Herausforderung. Je erfolgreicher Sie bei Prävention und Resilienz sind, desto mehr erscheinen Ihre Bemühungen im Nachhinein unnötig.

Um das Präventionsparadoxon zu lösen, kann Ihre Organisation spezifische Maßnahmen ergreifen, um die unsichtbare Arbeit der Prävention sichtbar, messbar und wertgeschätzt zu machen. Zu den möglichen Schritten gehören die folgenden:

- Dokumentieren und simulieren Sie, was ohne Präventivmaßnahmen hätte passieren können.
- Erzählen Sie Geschichten von Ereignissen, bei denen präventive Maßnahmen potenzielle Katastrophen abgewendet haben.
- Nennen Sie vergleichbare Organisationen, die sich nicht vorbereitet haben und die dadurch Konsequenzen erlitten haben.
- Gegenwärtige Präventionskosten im Zusammenhang mit den potenziellen Auswirkungen, die sie verhindern.
- Unterteilen Sie die Präventionsmaßnahmen in sichtbare Meilensteine und Erfolge.
- Verschaffen Sie sich ein institutionelles Gedächtnis darüber, warum Präventionsmaßnahmen existieren und welche historische Bedeutung sie haben.
- Informieren Sie die Interessengruppen regelmäßig über den Wert von Resilienz- und Chaos-Engineering-Praktiken.

Schlussfolgerung

Chaos Engineering ist für Unternehmen ein strategischer Imperativ. Auf Ihrem Weg zur Einführung können Herausforderungen wie Missverständnisse, kulturelle Widerstände und Ressourcenknappheit auftreten, aber die Festlegung klarer, von der Führung getriebener Ziele kann den Prozess katalysieren. Wenn die Praktiken immer ausgereifter werden, sollten Sie die Kapitalrendite anhand eines ganzheitlichen Ansatzes quantifizieren, der sowohl quantitative betriebliche Verbesserungen als auch qualitative organisatorische Vorteile berücksichtigt. Der ganzheitliche Ansatz ist angesichts des wirtschaftlichen Drucks besonders wichtig.

Um diese strategische Notwendigkeit in die Realität umzusetzen, bewerten Sie zunächst den aktuellen Reifegrad Ihres Unternehmens. Befindet sich Ihre Organisation in der Phase der Experimente an der Basis, in der zielorientierten Phase oder irgendwo dazwischen? Erstellen Sie auf der Grundlage dieser Bewertung eine maßgeschneiderte Roadmap, um Folgendes zu erreichen:

- Richten Sie die Steuerung im Bereich Chaos Engineering ein (ernennen Sie beispielsweise einen Chief Resilience Officer).
- Integrieren Sie Chaos-Praktiken in Entwicklungsabläufe.
- Implementieren Sie regelmäßige Schulungsprogramme.
- Entwickeln Sie umfassende Kennzahlen zur Widerstandsfähigkeit.

Diese Transformation wird nicht über Nacht geschehen. Diese konkreten Schritte bei gleichzeitiger Sicherstellung der kontinuierlichen Unterstützung durch die Geschäftsleitung werden jedoch dazu beitragen, Chaos Engineering auf das gleiche strategische Niveau wie Cybersicherheit zu heben. Ähnlich wie Cybersicherheit kann Chaos Engineering zu einem integralen Bestandteil der betrieblichen DNA und der Prozesse Ihres Unternehmens werden.

Ressourcen

- Ergebnisse der weltweiten ITIC-Umfrage zur Zuverlässigkeit von Serverhardware und Serverbetriebssystemen 2021
- Das Geschäftsszenario für Chaos Engineering
- Cybersicherheit als strategische Investition: Wie eine ROI-Optimierung zu einer sichereren Zukunft führen kann
- Der Leitfaden für I&O-Führungskräfte zum Thema Chaos Engineering
- Wie benutzt man den AWS Resilience Hub Score
- Implementierung empfohlener Experimente mit der AWS Resilience Hub-Konsole

Anhang A – Zieltypen für Chaos Engineering

Die folgenden Beschreibungen der Zieltypen enthalten reale Beispiele dafür, wie Amazon und andere Organisationen Ziele für Chaos Engineering entworfen haben.

Ziele einer belastbaren Architektur

Einer der ersten Gründe für die Einführung von Chaos Engineering ist die Identifizierung und Reduzierung von Single Points of Failure (SPOF) in allen Systemen und Infrastrukturen. Ziel ist es, die Widerstandsfähigkeit kritischer Systeme und Architekturen zu validieren, insbesondere für neue Dienste oder Anwendungen.

Zu den Zielen einer ausfallsicheren Architektur gehört die Durchführung von Chaosexperimenten, bei denen Fehler in Dienstabhängigkeiten simuliert werden. Die Experimente bestätigen, ob Timeouts, Wiederholungsversuche, Caching-Verhalten und Circuit-Breaker-Konfigurationen korrekt funktionieren. Diese Experimente helfen dabei, Probleme aufzudecken, die behoben werden müssen, und so Vorfälle zu verhindern, die sich auf Kunden auswirken. Ein Beispiel finden Sie unter Aufbau robuster Dienste bei Prime Video mit Chaos Engineering.

Ziele der Servicewiederherstellung

Im Mittelpunkt der Servicewiederherstellungsziele steht die Verbesserung der Fähigkeit zur Wiederherstellung nach Betriebsunterbrechungen oder Infrastrukturausfällen. Beispielsweise könnte Ihr Unternehmen bestrebt sein, im Falle eines Ausfalls ein bestimmtes Recovery Time Objective (RTO) für Ihre Kerndienste zu erreichen. Teams können Chaosexperimente entwerfen, um Evakuierungsstrategien, Failover-Mechanismen und automatisierte Wiederherstellungsprozesse zu validieren und zu optimieren. Die Optimierungen reduzieren letztendlich den Zeitaufwand für die Wiederherstellung des Dienstes. Ein Beispiel finden Sie unter AWS Lambda under-the-hoodResilienz.

Ziele im Hinblick auf das Nutzererlebnis

Die Aufrechterhaltung eines konsistenten und zuverlässigen Benutzererlebnisses ist von größter Bedeutung, insbesondere in Zeiten mit hohem Besucheraufkommen oder kritischen Ereignissen. Setzen Sie sich in solchen Fällen Ziele, in deren Mittelpunkt die Erfüllung bestimmter Service-Level-Ziele steht ()SLOs. Dieser kundenorientierte Ansatz stellt sicher, dass die Bemühungen um Resilienz

direkt auf die Bereitstellung eines erstklassigen Benutzererlebnisses ausgerichtet sind, selbst bei Ausfällen oder verschlechterten Bedingungen. Ein Beispiel finden Sie unter Engineering Resilience: Lessons from Amazon Search's Chaos Engineering Journey.

Metrikorientierte Ziele

Sie können Ziele auf der Grundlage quantitativer Kennzahlen festlegen, z. B. eines Resilienz-Scores, der berechnet wird, indem Services, die bewährte Best Practices für Resilienz anwenden, Punkte vergeben werden. Anschließend können Sie anhand bestimmter Chaosexperimente den Resilienzwert ermitteln. Dieser Wert kann Teams als Maßstab dienen, um ihre Fortschritte bei der Minderung bekannter Verfügbarkeitsrisiken und der Umsetzung empfohlener Resilienzmaßnahmen zu verfolgen. Es ist jedoch wichtig, solche Werte vorsichtig zu interpretieren und zu vermeiden, dass eine einzelne Kennzahl auf Kosten umfassenderer Resilienzziele überbewertet wird. Ein Beispiel finden Sie unter Grundlegendes zu Resilienzwerten.

Ziele zur Einhaltung gesetzlicher Vorschriften

Die Finanzdienstleistungsbranche hat sich als Vorreiter bei der Umsetzung von Chaos Engineering herausgestellt, was in erster Linie auf strenge regulatorische Anforderungen zurückzuführen ist, die robuste Widerstandsfähigkeit erfordern. Die Vorschriften werden von Finanzinstituten verlangen, dass sie Sicherheitslücken in ihren kritischen Systemen und Prozessen proaktiv identifizieren, testen und beheben. Diese Vorschriften beinhalten Folgendes:

- Das behördenübergreifende Papier über solide Praktiken zur Stärkung der betrieblichen Widerstandsfähigkeit, herausgegeben von US-Bundesbehörden
- Die Leitlinien der Europäischen Zentralbank zur operativen Resilienz
- Der Vorschlag der Europäischen Kommission für einen Digital Operational Resilience Act (DORA)

Wenn es sich bei Ihrer Organisation um ein Finanzinstitut handelt, halten Sie sich an diese Vorschriften, indem Sie explizite Ziele für den Nachweis der betrieblichen Belastbarkeit durch umfassende Test- und Validierungsstrategien festlegen. Ein Beispiel finden Sie unter London Stock Exchange Group setzt Chaos Engineering ein AWS , um die Widerstandsfähigkeit zu verbessern.

Anhang B – Quantitative und qualitative Maßnahmen

In diesem Abschnitt werden quantitative Kennzahlen zur Erfassung betrieblicher Verbesserungen und qualitative Maßnahmen zur Bewertung allgemeiner organisatorischer Ergebnisse von Chaos-Engineering-Praktiken beschrieben.

Quantitative Maßnahmen

Die folgenden quantitativen Kennzahlen bieten einen Rahmen für die Erfassung wichtiger Kennzahlen, anhand derer sich die direkten Verbesserungen bei Zwischenfällen und Betriebsabläufen nachweisen lassen, die durch Chaos-Engineering-Praktiken erzielt wurden:

- Vorfälle:
  - Häufigkeit von Vorfällen – Verfolgen Sie die Anzahl der Vorfälle innerhalb eines Rahmens zur Klassifizierung von Vorfällen und klassifizieren Sie sie nach ihrer Kritikalität (kritisch, schwerwiegend, geringfügig) über einen bestimmten Zeitraum. Weitere Informationen zum Rahmen zur Klassifizierung von Vorfällen finden Sie in Anhang C.
  - Ausfallzeit und Verschlechterung – Messen Sie die Gesamtdauer von Ausfallzeiten oder Leistungseinbußen für jede Klassifizierung von Vorfällen.
  - Kennzahlen zur Reaktion auf Vorfälle – Um Vorfälle zu verstehen, messen Sie die Zeit bis zur Erkennung, die Zeit bis zur Identifizierung, die Zeit bis zur Minderung, die Zeit bis zur Wiederherstellung, die Zeit bis zur Eskalation und andere verwandte Kennzahlen für jede Vorfallklassifizierung.
  - Kundenbelastende Vorfälle – Verfolgen Sie die Anzahl der Vorfälle, die sich auf Kunden auswirken, oder den Prozentsatz der Vorfälle, die vor den Auswirkungen auf den Kunden eingedämmt wurden.
  - Runbook-Änderungen – Verfolgen Sie die Anzahl der Runbook-Updates oder -Überarbeitungen, die sich aus Erkenntnissen ergeben, die durch Chaosexperimente gewonnen wurden. Ein Runbook enthält detaillierte Anweisungen für die Durchführung eines bestimmten Vorgangs oder Verfahrens zur Wiederherstellung nach einer bestimmten Art von Vorfall.
- Kosten:
  - Infrastrukturkosten – Sammeln Sie Daten zu den Infrastrukturkosten, einschließlich Cloud-Computing-Ressourcen und Redundanzmaßnahmen, die für die Maßnahmen zur Verbesserung der Widerstandsfähigkeit erforderlich sind.

    - Auswirkungen auf die Kunden – Messen Sie die Auswirkungen auf das Kundenerlebnis, die Abwanderungsraten und Umsatzverluste aufgrund von Systemausfällen oder Ausfallzeiten.
    - Mitarbeiterproduktivität – Verfolgen Sie die Zeit, die die Ingenieur- und Betriebsteams mit der Reaktion auf Vorfälle, der Brandbekämpfung, der Erstellung von Nachbesprechungen und anderen reaktiven Aufgaben im Zusammenhang mit Systemausfällen verbringen.
- Kontinuierliche Systemverbesserungen – Zählen Sie die Anzahl der Prozessverbesserungen, Architekturänderungen oder automatisierten Wiederherstellungsmechanismen, die als direktes Ergebnis von Erkenntnissen aus Chaosexperimenten implementiert wurden.
- Einhaltung gesetzlicher Vorschriften – Behalten Sie die Kosten im Blick und arbeiten Sie daran, regulatorische Anforderungen oder Industriestandards in Bezug auf die betriebliche Belastbarkeit zu erfüllen.
- Einführung – Verfolgen Sie die Akzeptanz von Chaos-Praktiken im gesamten Unternehmen.
- Kundenzufriedenheit – Messen Sie Veränderungen der Kundenzufriedenheitskennzahlen, um zu beurteilen, wie sich eine verbesserte Systemzuverlässigkeit auf das Geschäft auswirkt.

Qualitative Maßnahmen

Die folgenden qualitativen Maßnahmen bieten einen Rahmen für die Erfassung der allgemeinen organisatorischen Ergebnisse, die durch Chaos-Engineering-Praktiken erzielt wurden:

- Selbstvertrauen und Bereitschaft der Mitarbeiter:
    - Befragen Sie die Teams regelmäßig, um ihr Selbstvertrauen im Umgang mit realen Vorfällen und ihre wahrgenommene Bereitschaft zu Bereitschaftswechseln zu messen.
    - Erfassen Sie den Prozentsatz der Bereitschaftsingenieure, die im Rahmen ihrer Ausbildung an Chaosexperimenten teilgenommen haben.
- Kultureller Wandel:
    - Beurteilen Sie anhand von Umfragen, Feedbacksitzungen oder Audits, inwieweit die Denkweise der Resilienz das Unternehmen durchdrungen hat.
    - Verfolgen Sie die Anzahl der Teams, die sich aktiv für Chaos-Engineering-Praktiken einsetzen und diese befürworten.
- Funktionsübergreifende Zusammenarbeit und Wissensaustausch:
    - Verfolgen Sie die Häufigkeit und Teilnahme an teamübergreifenden Sitzungen oder Workshops zum Wissensaustausch im Zusammenhang mit dem Lernen im Bereich Chaos Engineering.

    - Verfolgen Sie die Anzahl der gemeinsamen Initiativen im Bereich Chaos Engineering, an denen mehrere Teams oder Abteilungen beteiligt sind.
- Effektivität der Schulungen:
    - Bewerten Sie die Effektivität von Schulungsprogrammen für Chaos Engineering, indem Sie nach der Schulung Umfragen oder Bewertungen durchführen.
    - Verfolgen Sie die Anzahl der Techniker, die an Schulungsprogrammen zur Chaos-Technik teilnehmen, und lesen Sie die Postmortems.
- Gewinnung und Bindung von Talenten:
    - Prüfen Sie, ob das Chaos Engineering-Programm dazu beiträgt, die besten Techniker zu gewinnen und zu halten, indem es den Zeit- und Arbeitsaufwand für die Behebung von Ausfällen reduziert.
- Ruf der Marke:
    - Verfolgen Sie alle Veränderungen der Markenwahrnehmung oder des Rufs im Zusammenhang mit dem nachgewiesenen Engagement des Unternehmens für betriebliche Widerstandsfähigkeit.
- Wettbewerbsvorteil:
    - Verfolgen Sie den Wettbewerbsvorteil gegenüber Branchenkollegen in Bezug auf die Systemverfügbarkeit.

Anhang C – Klassifizierung von Vorfällen

Die Verfolgung von Vorfällen innerhalb eines Klassifizierungsrahmens ist von entscheidender Bedeutung, da das Framework einen ganzheitlichen Überblick über die Fehlertypen und Probleme bietet, die sich auf das System auswirken. Wenn Ihr Unternehmen Vorfälle nur innerhalb einer einzigen Klasse verfolgt, z. B. Infrastrukturfehler, entgehen Ihnen möglicherweise Erkenntnisse und Verbesserungsmöglichkeiten in anderen Bereichen. Indem Sie Vorfälle über mehrere Klassen hinweg verfolgen, gewinnen Sie ein besseres Verständnis für die vielfältigen Chaosexperimente, die Sie durchführen müssen. Diese Perspektive hilft bei der Identifizierung potenzieller blinder Flecken und unterstützt die Erweiterung des technischen Umfangs, was zu einem robusteren und fehlertoleranteren System führt.

Der vorgeschlagene Rahmen zur Klassifizierung von Vorfällen soll dazu beitragen, Vorfälle anhand ihrer Art und ihrer potenziellen Auswirkungen zu kategorisieren. Es verwendet eine allgemeine Klassifizierung, bei der Vorfälle in acht Hauptkategorien eingeteilt werden:

- Probleme bei der Bereitstellung:
  - Fehlgeschlagene Bereitstellungen
  - Rollback-Fehler
  - Konfigurationsprobleme bei der Bereitstellung
- Softwarefehler und Regressionen:
  - Funktionelle Fehler
  - Probleme mit der Integration
  - Probleme mit der Leistung
  - Probleme mit der Quote
  - Probleme mit dem Resilienzmechanismus (Wiederholungsversuche, Timeouts)
  - Probleme mit der Datenintegrität
- Probleme beim Testen:
  - Fehlende Tests
  - Ineffektive Tests
  - Flockige Tests
- Fehler in der Infrastruktur:
  - Hardwarefehler (Server, Netzwerkgeräte, Speicher)

    - Probleme mit der Skalierung
    - Abhängigkeitsfehler (Dienste von Drittanbietern, APIs)
    - Probleme mit der Netzwerkkonnektivität
- Probleme mit dem Betrieb:
    - Menschliche Fehler (Fehlkonfiguration, versehentliche Änderungen)
    - Überwachung und Alarmierung von Ausfällen
    - Probleme bei der Kapazitätsplanung
    - Fehler bei der Backup und Wiederherstellung
- Sicherheitsvorfälle:
    - Unbefugte Zugriffsversuche
    - Datenschutzverletzungen
    - Denial-of-Service-Angriffe (DoS)
- Ausfälle von Diensten von Drittanbietern:
    - Ausfälle von Cloud-Anbietern
    - DNS-Fehler
    - Externe API- und Dienstunterbrechungen
- Umweltfaktoren:
    - Naturkatastrophen (Erdbeben, Brände, Überschwemmungen, Stromausfälle)
    - Probleme im Zusammenhang mit dem Wetter

Dies ist ein nicht aussagekräftiges Beispiel für einen Klassifizierungsrahmen, den Sie an Ihre spezifischen Bedürfnisse und Ihr Unternehmen anpassen können. Wir empfehlen, den Klassifizierungsrahmen regelmäßig zu überprüfen und zu aktualisieren, wenn sich Ihr System weiterentwickelt oder neue Arten von Vorfällen auftreten.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	28. Januar 2025

AWS Glossar zu präskriptiven Leitlinien

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern von AWS Prescriptive Guidance verwendet. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora PostgreSQL-kompatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der. AWS Cloud
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr CRM-System (Customer Relationship Management) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2 Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.

- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Weitere Informationen finden Sie unter Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen im Bereich künstliche Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung in der AWS Migrationsstrategie finden Sie im Operations Integration Guide. AIOps

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den

öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Cloud-Einführung (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue

Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, sogenannte bösartige Bots, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er in der Regel keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter Framework für die AWS Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Exzellenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen bei der Migration in der Regel durchlaufen AWS Cloud:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament — Tätigen Sie grundlegende Investitionen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer landing zone, Definition eines CCo E, Einrichtung eines Betriebsmodells)

- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oderBitbucket Cloud. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. Amazon SageMaker AI bietet beispielsweise Bildverarbeitungsalgorithmen für CV.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD is commonly described as a pipeline. CI/CDkann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil

der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Variation zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, die sicherstellen, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen historischer Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

defense-in-depth

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein defense-in-depth Ansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In AWS Organizations kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren, um die Konten der Organisation und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto

wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Bereitstellung

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, die Sie verwenden, um Ausfallzeiten und Datenverluste aufgrund einer Katastrophe zu minimieren. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domaingesteuertes Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration. Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung des Wertstroms in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

elektronischer Datenaustausch (EDI)

Der automatisierte Austausch von Geschäftsdokumenten zwischen Organisationen. Weitere Informationen finden Sie unter Was ist elektronischer Datenaustausch.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-Endian-Systeme speichern das höchstwertige Byte zuerst. Little-Endian-Systeme speichern das niedrigwertigste Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen

Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.
- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD-Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit,

Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS - Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

Eingabeaufforderung mit wenigen Klicks

Bereitstellung einer kleinen Anzahl von Beispielen, die die Aufgabe und das gewünschte Ergebnis veranschaulichen, bevor das LLM aufgefordert wird, eine ähnliche Aufgabe auszuführen. Bei dieser Technik handelt es sich um eine Anwendung des kontextbezogenen Lernens, bei der Modelle anhand von Beispielen (Aufnahmen) lernen, die in Eingabeaufforderungen eingebettet sind. Bei Aufgaben, die spezifische Formatierungs-, Argumentations- oder Fachkenntnisse erfordern, kann die Eingabeaufforderung mit wenigen Handgriffen effektiv sein. Siehe auch Zero-Shot Prompting.

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

Ein großes neuronales Deep-Learning-Netzwerk, das mit riesigen Datensätzen generalisierter und unbeschrifteter Daten trainiert wurde. FMs sind in der Lage, eine Vielzahl allgemeiner Aufgaben zu erfüllen, z. B. Sprache zu verstehen, Text und Bilder zu generieren und Konversationen in natürlicher Sprache zu führen. Weitere Informationen finden Sie unter Was sind Foundation-Modelle.

G

generative KI

Eine Untergruppe von KI-Modellen, die mit großen Datenmengen trainiert wurden und mit einer einfachen Textaufforderung neue Inhalte und Artefakte wie Bilder, Videos, Text und Audio erstellen können. Weitere Informationen finden Sie unter Was ist Generative KI.

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

goldenes Bild

Ein Snapshot eines Systems oder einer Software, der als Vorlage für die Bereitstellung neuer Instanzen dieses Systems oder dieser Software verwendet wird. In der Fertigung kann ein Golden Image beispielsweise zur Bereitstellung von Software auf mehreren Geräten verwendet werden und trägt zur Verbesserung der Geschwindigkeit, Skalierbarkeit und Produktivität bei der Geräteherstellung bei.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dazu beiträgt, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Unternehmenseinheiten zu regeln (OUs). Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Holdout-Daten

Ein Teil historischer, beschrifteter Daten, der aus einem Datensatz zurückgehalten wird, der zum Trainieren eines Modells für maschinelles Lernen verwendet wird. Sie können Holdout-Daten verwenden, um die Modellleistung zu bewerten, indem Sie die Modellvorhersagen mit den Holdout-Daten vergleichen.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im AWS Well-Architected Framework.

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS Security Reference Architecture empfiehlt, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr und Inspektion einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer

schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und KI/ML bezieht.

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

industrielles Internet der Dinge (T) IIo

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Weitere Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in demselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. In der AWS Security Reference Architecture wird empfohlen, Ihr Netzwerkkonto mit eingehendem und ausgehendem Datenverkehr sowie Inspektionen einzurichten, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit. AWS

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Weitere Informationen finden Sie in der IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten

und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

großes Sprachmodell (LLM)

Ein Deep-Learning-KI-Modell, das anhand einer riesigen Datenmenge vorab trainiert wurde. Ein LLM kann mehrere Aufgaben ausführen, z. B. Fragen beantworten, Dokumente zusammenfassen, Text in andere Sprachen übersetzen und Sätze vervollständigen. Weitere Informationen finden Sie unter Was sind. LLMs

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Weitere Informationen finden Sie unter Label-basierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der

Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind. AWS Organizations Ein Konto kann jeweils nur einer Organisation angehören.

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

Microservice

Ein kleiner, unabhängiger Dienst, der über genau definierte Kanäle kommuniziert APIs und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren mithilfe von Lightweight über eine klar definierte Schnittstelle. APIs Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementierung von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wurde, um einen Workload auf den AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um umfangreiche Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Evaluierung der Modernisierungsbereitschaft von Anwendungen in der AWS Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Siehe Origin Access Control.

OAI

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während

der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Einen Trail für eine Organisation erstellen.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS Security Reference Architecture empfiehlt die Einrichtung Ihres Netzwerkkontos mit eingehendem und ausgehendem Datenverkehr sowie Inspektion, VPCs um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet im weiteren Sinne zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe

Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz von Natur aus

Ein systemtechnischer Ansatz, der den Datenschutz während des gesamten Entwicklungsprozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und deren Subdomains innerhalb einer oder mehrerer VPCs Domains antworten

soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Diese Steuerelemente scannen Ressourcen, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

schnelle Verkettung

Verwendung der Ausgabe einer LLM-Eingabeaufforderung als Eingabe für die nächste Aufforderung, um bessere Antworten zu generieren. Diese Technik wird verwendet, um eine komplexe Aufgabe in Unteraufgaben zu unterteilen oder um eine vorläufige Antwort iterativ zu verfeinern oder zu erweitern. Sie trägt dazu bei, die Genauigkeit und Relevanz der Antworten eines Modells zu verbessern und ermöglicht detailliertere, personalisierte Ergebnisse.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

publish/subscribe (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen,

den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

LAPPEN

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

Wiederherstellungszeitziel (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten aller an Migrationsaktivitäten und Cloud-Operationen beteiligten Parteien definiert. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

Eine generative KI-Technologie, bei der ein LLM auf eine maßgebliche Datenquelle verweist, die sich außerhalb seiner Trainingsdatenquellen befindet, bevor eine Antwort generiert wird. Ein RAG-Modell könnte beispielsweise eine semantische Suche in der Wissensdatenbank oder in benutzerdefinierten Daten einer Organisation durchführen. Weitere Informationen finden Sie unter Was ist RAG.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS Management Console oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldedaten, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheit durch Design

Ein systemtechnischer Ansatz, der die Sicherheit während des gesamten Entwicklungsprozesses berücksichtigt.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als

detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer EC2 Amazon-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Steuerung der Berechtigungen für alle Konten in einer Organisation in ermöglicht AWS Organizations. SCPs Definieren Sie Leitplanken oder legen Sie Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können sie SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Dienste oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, während Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der AWS Cloud.

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb

genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

Systemaufforderung

Eine Technik, mit der einem LLM Kontext, Anweisungen oder Richtlinien zur Verfügung gestellt werden, um sein Verhalten zu steuern. Systemaufforderungen helfen dabei, den Kontext festzulegen und Regeln für Interaktionen mit Benutzern festzulegen.

T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

Transit-Gateway

Ein Netzwerk-Transit-Hub, über den Sie Ihre Netzwerke VPCs und Ihre lokalen Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der Dokumentation unter Was ist ein Transit-Gateway. AWS Transit Gateway

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen

finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs , die es Ihnen ermöglicht, den Verkehr mithilfe privater IP-Adressen weiterzuleiten. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems beeinträchtigt.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Sehen Sie einmal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur gilt als unveränderlich.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Zero-Shot-Aufforderung

Bereitstellung von Anweisungen für die Ausführung einer Aufgabe an einen LLM, jedoch ohne Beispiele (Schnappschüsse), die ihm als Orientierungshilfe dienen könnten. Der LLM muss sein

vortrainiertes Wissen einsetzen, um die Aufgabe zu bewältigen. Die Effektivität von Zero-Shot Prompting hängt von der Komplexität der Aufgabe und der Qualität der Aufforderung ab. Siehe auch Few-Shot-Prompting.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.