Sicherheit nach Maß: Governance in AWS

Analyse von AWS-Funktionen zur besseren Bewältigung lokaler Herausforderungen

November 2013

(Die aktuelle Version dieses Dokuments finden Sie unter http://aws.amazon.com/compliance.)

Inhaltsverzeichnis

Überblick

In AWS können Sie praktisch alles ausführen, was auch lokal ausgeführt werden kann: Websites, Anwendungen, Datenbanken, mobile Apps, E-Mail-Kampagnen, verteilte Datenanalysen, Medienspeicher und private Netzwerke. Die von AWS gebotenen Services sind auf Zusammenarbeit ausgelegt, sodass Sie Komplettlösungen entwickeln können. Ein Vorteil der Migration von Verarbeitungslasten zu AWS wird häufig übersehen: Es handelt sich dabei um die Möglichkeit, durch die Nutzung der vielen Governance ermöglichenden Funktionen einen höheren Grad an Sicherheit zu erreichen – und zwar maßgeschneidert für das eigene System. Aus denselben Gründen, aus denen die Bereitstellung von Infrastruktur in der Cloud Vorteile gegenüber der lokalen Bereitstellung hat, ermöglicht Cloud-basierte Governance niedrigere Einstiegskosten, einen einfacheren Betrieb und mehr Agilität, indem eine bessere Übersicht, Kontrolle der Sicherheit und zentrale Automatisierung geboten wird. In diesem Whitepaper wird beschrieben, wie Sie mithilfe von AWS ein hohes Maß an Governance für Ihre IT-Ressourcen erzielen. Zusammen mit dem Whitepaper Amazon Web Services – Risiko und Compliance und dem Whitepaper Checkliste zur Überprüfung der Sicherheit kann dieses Whitepaper Ihnen helfen, sich mit den in AWS-Services integrierten Governance-Funktionen vertraut zu machen, damit Sie beim Entwickeln Ihrer mit AWS integrierten Umgebung Sicherheitsempfehlungen und bewährte Methoden befolgen.

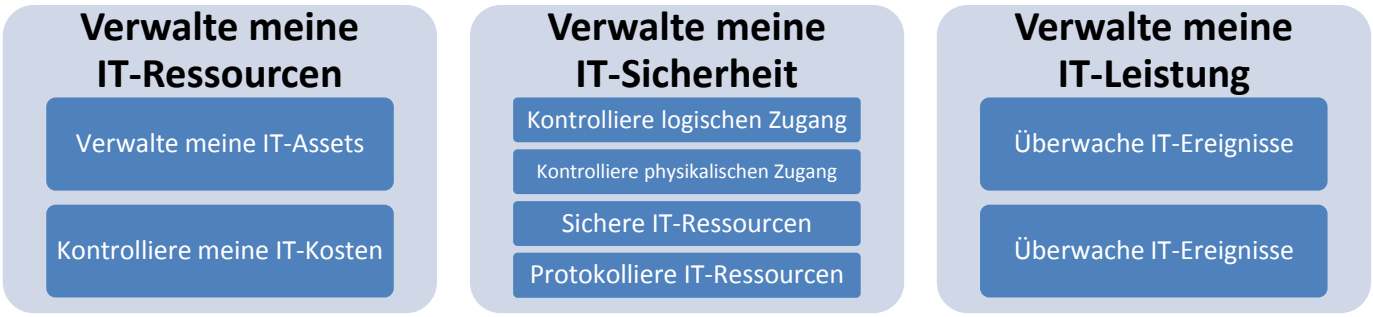
Einführung

Branchen- und Regulierungsgremien haben ein komplexes Geflecht an neuen und älteren Gesetzen und Vorschriften geschaffen, das eine breite Palette an Sicherheits- und Governance-Maßnahmen erforderlich macht. Marktforschungsunternehmen gehen deshalb davon aus, dass viele Unternehmen bis zu 75 % ihres IT-Budgets für die Verwaltung von Infrastruktur und nur 25 % für IT-Aspekte ausgeben, die in direktem Bezug zum Geschäft stehen, das die Unternehmen betreiben. Einer der Schlüssel zum Verbessern dieses Verhältnisses ist eine effizientere Bewältigung der IT-Governance-Anforderungen im Back-End. Eine einfache und wirksame Möglichkeit dazu bieten die standardmäßig verfügbaren Governance-Funktionen von AWS.

Da AWS eine Vielzahl von IT-Governance-Funktionen bietet, kann es schwierig sein zu entscheiden, wo begonnen und was implementiert werden sollte. In diesem Dokument werden die gängigen IT-Governance-Bereiche untersucht, indem der Anwendungsfall (bzw. die Herausforderung in lokalen Umgebungen), die von AWS gebotenen Funktionen und die dazugehörigen Nutzenversprechen für Governance durch die Verwendung dieser Funktionen vorgestellt werden. Dieses Dokument soll Ihnen helfen, die Ziele in jedem einzelnen IT-Governance-Bereich zu erreichen[1].

Dieses Dokument folgt in den wesentlichen Bereichen dem Ansatz weit verbreiteter IT-Governance-Frameworks (z. B. CoBIT, ITIL, COSO, CMMI, usw.). Doch die IT-Governance-Bereiche, gemäß denen das Dokument strukturiert ist, sind allgemein gehalten, damit Kunden es nutzen können, um die von AWS gebotenen Governance-Funktionen im Vergleich mit denen ihrer lokalen Ressourcen und Tools vergleichen zu können. Die folgenden IT-Governance-Bereiche werden mithilfe eines anwendungsfallorientierten Ansatzes behandelt:

Ich wünsche mir eine besseres...



[1] Wenngleich dieses Dokument mit einer umfassenden Liste der Governance ermöglichenden Funktionen aufwartet, sind, da ständige neue Funktionen entwickelt werden, nicht alle verfügbaren Funktionen enthalten. Weitere Tutorials, Entwickler-Tools und Dokumentation finden Sie unter http://aws.amazon.com/resources/.

Management von IT-Ressourcen

Management von IT-Komponenten

Die Bestimmung und das Management Ihrer IT-Komponenten ist der erste Schritt zu effektiver IT-Governance. IT-Komponenten reichen von Hochleistungs-Routern, Switches, Servern, Hosts und Firewalls zu Anwendungen, Services, Betriebssystemen und anderen in Ihrem Netzwerk bereitgestellten Softwarekomponenten. Ein aktualisierter Bestand von Hardware- und Softwarekomponenten ist für Entscheidungen zu Upgrades und Beschaffung, die Verfolgung des Garantiestatus sowie zum Zweck der Fehlerbehebung und aus Sicherheitsgründen wichtig. Eine fehlerfreie Aufstellung des Komponentenbestands wird zunehmend zu einer zwingenden Notwendigkeit, um Sichten und umfassende Berichte bedarfsabhängig bereitzustellen. Darüber hinaus sind umfassende Komponentenbestandslisten zur Erfüllung bestimmter Compliance-Vorgaben erforderlich. Beispielsweise sehen die Vorgaben von FISMA, SOX, PCI DSS und HIPAA allesamt fehlerfreie Komponentenbestandslisten vor. Doch da lokale Ressourcen häufig zusammengestückelt sind, kann das Pflegen einer solchen Liste bestenfalls mühselig und schlimmstenfalls unmöglich sein. Organisationen müssen häufig auf Lösungen anderer Anbieter zurückgreifen, um eine Automatisierung der Komponentenbestandsliste zu ermöglichen. Und selbst dann ist es nicht immer möglich, einen detaillierten Bestand aller Komponententypen in einer zentralen Konsole anzuzeigen.

Bei Verwenden von AWS stehen Ihnen mehrere Funktionen zur Verfügung, Ihren Bestand an IT-Ressourcen in AWS rasch und einfach zu erfassen. Diese Funktionen, dazugehörige Anleitungen und Links zu weiteren Informationen zu den Funktionen finden Sie nachstehend:

AWS-Funktion zur Ermöglichung von Governance	Sicherheit nach Maß
Seite "Account Activity"	Bietet eine zusammengefasste Auflistung von IT-Ressourcen mit detaillierten Angaben zur Nutzung aller Services nach Region. Weitere Informationen.
Amazon Glacier – Bestand von Archivdatenspeichern	Stellt den Glacier-Datenbestand bereit, indem alle IT-Ressourcen in Glacier angezeigt werden. Weitere Informationen.
AWS CloudHSM	Ermöglicht die virtuelle und physische Kontrolle über Verschlüsselungsschlüssel, indem zur Schlüsselspeicherung den Kunden fest zugeordnete Hardware-Sicherheitsmodule (HSMs) zur Verfügung gestellt werden. Weitere Informationen.
AWS Data Pipeline – Task Runner	Ermöglicht eine automatisierte Verarbeitung von Aufgaben durch Abfragen der AWS Data Pipeline nach Aufgaben, die anschließend ausgeführt werden und deren Status gemeldet wird.. Weitere Informationen.
AWS Management Console	Bietet eine Bestandsliste von Komponenten und Daten in Echtzeit, indem alle in AWS ausgeführten IT-Ressourcen sortiert nach Service angezeigt werden. Weitere Informationen.
AWS Storage Gateway-APIs	Bieten die Möglichkeit, den Bestand an Komponenten und Daten programmgesteuert zu erfassen, indem Schnittstellen, Tools und Skripts für die Verwaltung von Ressourcen programmiert werden. Weitere Informationen.

Kontrollieren der IT-Kosten

Sie können Ihre IT-Kosten besser kontrollieren, indem Sie Ressourcen auf die wirtschaftlichste Weise beschaffen und mit den Kosten Ihrer IT-Services vertraut sind. Doch das Management und die Nachverfolgung von Kosten und ROI im Zusammenhang mit Ausgaben für lokale IT-Umgebungen können schwierig und fehlerhaft sein, da die Berechnungen so komplex sind. Kapazitätsplanung, Nutzungsvorhersagen, Beschaffungskosten, Abschreibungen, Kapitalkosten und Anlagenkosten sind nur einige wenige Aspekte, die das Berechnen der Gesamtbetriebskosten erschweren.

AWS bietet mehrere Funktionen, mit denen Sie die Kosten Ihrer IT-Ressourcen einfach und präzise bestimmen und kontrollieren können. Durch die Nutzung von AWS können Sie sich im Vergleich zu gleichwertigen lokalen Bereitstellungen Kostenersparnisse von bis zu 80 % sichern[2]. Diese Funktionen, dazugehörige Anleitungen und Links zu weiteren Informationen zu den Funktionen finden Sie nachstehend:

AWS-Funktion zur Ermöglichung von Governance	Sicherheit nach Maß
Seite "Account Activity"	Bietet jederzeit nach Services sortiert eine Ansicht der Ausgaben für IT-Ressourcen. Weitere Informationen.
Amazon EC2 – Idempotenz beim Start von Instances	Hilft das irrtümliche Starten von Ressourcen und Anfallen zusätzlicher Kosten zu vermeiden, indem bei Timeouts oder Verbindungsfehlern keine zusätzlichen Instances gestartet werden. Weitere Informationen.
Amazon EC2 – Versehen von Ressourcen mit Tags	Ermöglicht eine Zuordnung zwischen Ressourcenausgaben und Geschäftsbereichen, indem IT-Ressourcen anpassbare Suchbezeichnungen zugewiesen werden. Weitere Informationen.
AWS-Fakturierung	Bietet benutzerfreundliche Funktionen zum Überwachen und Begleichen Ihrer Rechnung, indem die genutzten Ressourcen und die entsprechenden tatsächlich angefallenen IT-Kosten detailliert aufgeschlüsselt werden. Weitere Informationen.
AWS Management Console	Stellt eine zentrale Sicht auf die Kostentreiber bereit, indem alle in AWS ausgeführten IT-Ressourcen aufgeschlüsselt nach Service mit den tatsächlichen Kosten und der Ausführungsquote angezeigt werden. Weitere Informationen.
AWS-Services – Preise	Bietet aussagekräftige Informationen zu den AWS-Tarifen von IT-Ressourcen, Preisen der einzelnen AWS-Produkte und spezifische Preismerkmale. Weitere Informationen.
AWS Trusted Advisor	Hilft, die Kosten von IT-Ressourcen zu optimieren, indem nicht verwendete Ressourcen und Ressourcen im Leerlauf bestimmt werden. Weitere Informationen.
Fakturierungsbenachrichtigungen	Ermöglichen proaktive Warnungen zu dem Ausgabeaktivitäten für IT-Ressourcen. Weitere Informationen.

[2] Im Total Cost of Ownership Whitepaper finden Sie weitere Informationen zu den gesamten Kosteneinsparungen bei Nutzung von AWS.

Konsolidierte Fakturierung	Ermöglicht eine zentrale Kostenkontrolle und kontenübergreifende Kostentransparenz, indem mehrere AWS-Konten in einer Rechnung zusammengefasst werden. Weitere Informationen.
Nutzungsbasierte Preise	Bereitstellen von IT-Ressourcen und -Services, mit denen Sie Anwendungen binnen Minuten zu nutzungsbasierten Preisen ohne vorab anfallende Beschaffungskosten oder laufende Wartungskosten einrichten können, indem Sie automatisch eine Skalierung auf weitere Server vornehmen lassen, sobald die Nachfrage nach Ihrer Anwendung steigt. Weitere Informationen.

Management der IT-Sicherheit

Steuern des physischen Zugriffs auf IT-Ressourcen

Das Management des physischen Zugriffs ist ein wesentlicher Bestandteil von IT-Governance-Programmen. Zusätzlich zu Sperren, Sicherheitsalarmen, Zugangskontrollen und Überwachungsvideos, die die herkömmlichen Komponenten physischer Sicherheit darstellen, sind die elektronischen Kontrollen des physischen Zugangs für eine effektive physische Sicherheit ebenfalls von großer Bedeutung. Das herkömmliche Bewachungsgewerbe durchläuft einen raschen Wandel und Spezialisierungsbereiche bilden sich heraus, durch die physische Sicherheit immer komplexer wird. Da die Aspekte bei der lokalen physischen Sicherheit und den Kontrollen komplexer geworden sind, gibt es einen zunehmenden Bedarf an besonders qualifizierten und spezialisierten IT-Sicherheitsfachleuten. Ihre Aufgabe ist, den beträchtlichen Aufwand zu bewältigen, der anfällt, um eine wirksame Kontrolle der Zugangsanmeldeinformationen für Karten/Kartenleser, Controller und Systemserver für das Hosten von Daten im Umfeld der physischen Sicherheit zu erreichen.

Durch Nutzung von AWS können Sie Kontrollen der physischen Sicherheit Ihrer AWS-Infrastruktur einfach und effektiv AWS-Spezialisten überlassen, die über die Fertigkeiten und Ressourcen verfügen, die physische Umgebung abzusichern. AWS hat mehrere unabhängige Prüfer beauftragt, die die physische Sicherheit von Rechenzentren das ganze Jahr hindurch untersuchen. Sie zertifizieren die Konzeption und detaillierten Tests der Wirksamkeit unsere physischen Sicherheitskontrollen. Nachstehend finden Sie weitere Informationen zu den AWS-Prüfprogrammen und dazugehörigen physischen Sicherheitskontrollen:

AWS-Funktion zur Ermöglichung von Governance	Sicherheit nach Maß
Physische AWS-Zugangskontrollen gemäß SOC1	Transparenz bei den vorhandenen Kontrollen, die einen unbefugten Zugang zu Rechenzentren verhindern. Die Kontrollen wurden von einem unabhängigen Prüfunternehmen ordnungsgemäß konzipiert, getestet und geprüft. Weitere Informationen.
Physische AWS-Zugangskontrollen gemäß SOC 2	Transparenz bei den vorhandenen Kontrollen, die einen unbefugten Zugang zu Rechenzentren verhindern. Die Kontrollen wurden von einem unabhängigen Prüfunternehmen ordnungsgemäß konzipiert, getestet und geprüft. Weitere Informationen.

Physische AWS-Zugangskontrollen gemäß PCI DSS	Transparenz bei den vorhandenen Kontrollen, die einen unbefugten Zugang zu Rechenzentren verhindern, entsprechend dem Datensicherheitsstandard der Kreditkartenbranche (Payment Card Industry Data Security Standard, PCI DSS). Die Kontrollen wurden von einem unabhängigen Prüfunternehmen ordnungsgemäß konzipiert, getestet und geprüft. Weitere Informationen.
Physische AWS-Zugangskontrollen gemäß DIN ISO 27001	Transparenz bei den vorhandenen Kontrollen, die einen unbefugten Zugang zu Rechenzentren verhindern, entsprechend den bewährten Methoden des Sicherheitsstandards DIN ISO 27002. Die Kontrollen wurden von einem unabhängigen Prüfunternehmen ordnungsgemäß konzipiert, getestet und geprüft. Weitere Informationen.
Physische AWS -Zugangskontrollen gemäß FedRAMP	Transparenz bei den vorhandenen Kontrollen, die einen unbefugten Zugang zu Rechenzentren verhindern, entsprechend den bewährten Methoden des Standards NIST 800-53. Die Kontrollen wurden von durch US-Behörden zugelassenen Prüfunternehmen ordnungsgemäß konzipiert, getestet und geprüft. Weitere Informationen.

Steuern des logischen Zugriffs auf IT-Ressourcen

Eines der Hauptziele von IT-Governance ist eine wirksame Steuerung des logischen Zugriffs auf Computersysteme und -daten. Doch viele Organisationen kämpfen damit, ihre lokalen Lösungen an die zunehmende und sich ständig ändernde Anzahl komplexer Aspekte beim logischen Zugriff anzupassen. Dies schließt die Fähigkeit zum Definieren einer Regel nach dem Prinzip der geringsten Berechtigungen, die Berechtigungsverwaltung für Ressourcen, den Umgang mit sich sich ändernden Rollen und Informationsanforderungen sowie die Zunahme sensibler Daten ein. Wesentliche, hartnäckige Herausforderungen bei der Verwaltung des logischen Zugriffs in einer lokalen Umgebung ergeben sich, wenn Benutzern der Zugriff basierend auf den folgenden Kriterien gewährt wird:

- Rolle (d. h. interne Benutzer, Auftragnehmer, externe Mitarbeiter, Partner usw.)
- Datenklassifizierung (d. h. vertraulich, nur zur internen Verwendung, privat, öffentlich usw.)
- Datentyp (d. h. Anmeldeinformationen, persönliche Daten, Kontaktinformationen, aufgabenbezogene Daten, digitale Zertifikate, Kennworteingabe mit Beantwortung einer Frage usw.)

AWS bietet zahlreiche Kontrollfunktionen für eine effektive Verwaltung des logischen Zugriffs basierend auf einer Matrix von Anwendungsfällen gemäß den Prinzip der geringsten Rechte. Diese Funktionen, dazugehörige Anleitungen und Links zu weiteren Informationen zu den Funktionen finden Sie nachstehend:

AWS-Funktion zur Ermöglichung von Governance	Sicherheit nach Maß
Amazon S3 – Zugriffskontrolllisten (ACLs)	Ermöglichen zentrale Berechtigungen durch Hinzufügen spezifischer Bedingungen, die steuern, wie Benutzer AWS nutzen dürfen, z. B. Uhrzeit, ursprüngliche IP-Adresse, SSL-Verwendung oder ob die Authentifizierung mit einem Multifaktor-Authentifizierungsgerät erfolgt ist. Weitere Informationen finden Sie hier und hier.

Amazon S3 – Bucket-Richtlinien	Ermöglichen die Erstellung bedingter Regeln für die Verwaltung des Zugriffs auf Buckets und Objekte dadurch, dass Sie den Zugriff basierend auf dem Konto sowie anforderungsbasierten Attributen wie HTTP-Referrer und IP-Adresse einschränken können. Weitere Informationen.
Amazon S3 – Abfrage-String-Authentifizierung	Bietet die Möglichkeit, einen HTTP- oder Browserzugriff auf Ressourcen zu gewähren, für den normalerweise eine Authentifizierung erforderlich wäre, indem die Signatur in der Abfragezeichenfolge zum Absichern der Anforderung verwendet wird. Weitere Informationen.
AWS CloudTrail	Dient zum Protokollieren von API- oder Konsolenaktionen (z. B. bei Änderung einer Bucket-Richtlinie oder Beenden einer Instance) und bietet erweiterte Überwachungsfunktionen. Weitere Informationen.
AWS IAM – Multifaktor-Authentifizierung (MFA)	Ermöglicht das Erzwingen der Multifaktor-Authentifizierung für alle Ressourcen, indem für die Anmeldung und den Zugriff auf Ressourcen ein Token verlangt wird. Weitere Informationen.
AWS IAM – Kennwortrichtlinie	Ermöglicht die Verwaltung der Qualität und Kontrolle der Kennwörter Ihrer Benutzer, indem Sie eine Kennwortrichtlinie für IAM-Benutzer festlegen, die vorgibt, dass Kennwörter eine bestimmte Länge haben müssen, bestimmte Zeichen enthalten müssen usw. Weitere Informationen.
AWS IAM-Berechtigungen	Ermöglichen eine einfache Verwaltung von Berechtigungen, indem Sie angeben können, welche Benutzer Zugriff auf AWS-Ressourcen haben sollen und welche Aktionen sie auf diese Ressourcen anwenden dürfen. Weitere Informationen.
AWS IAM-Richtlinien	Ermöglichen eine detaillierte Zugriffsverwaltung nach dem Prinzip der geringsten Rechte, indem Sie mehrere Benutzer unter Ihrem AWS-Konto einrichten, denen Sie Anmeldeinformationen zuweisen und deren Berechtigungen Sie verwalten. Weitere Informationen.
AWS IAM-Rollen	Ermöglichen die vorübergehende Delegierung des Zugriffs an Benutzer oder Services, die üblicherweise keinen Zugriff auf Ihre AWS-Ressourcen haben, indem Sie eine Gruppe von Berechtigungen für den Zugriff auf Ressourcen definieren, die ein Benutzer oder Service benötigt. Weitere Informationen.
AWS Trusted Advisor	Bietet eine automatische Bewertung des Sicherheitsmanagements, indem mögliche Sicherheitsprobleme ausgemacht und eskaliert werden. Weitere Informationen.

Schützen von IT-Ressourcen

Der Schutz von IT-Ressourcen ist der Eckpfeiler von IT-Governance-Programmen. Doch bei lokalen Umgebungen ist eine ganze Reihe sicherheitsbezogener Schritte auszuführen, wenn ein neuer Server online geschaltet wird. Beispielsweise müssen Firewall- und Zugriffskontrollrichtlinien aktualisiert werden, das neu erstellte Serverabbild muss auf Übereinstimmung mit der Sicherheitsrichtlinie geprüft werden und alle Softwarepakete müssen auf dem neuesten Stand sein. Außer wenn diese Sicherheitsaufgaben automatisiert sind und in einer Weise erfolgen, die mit den überaus dynamischen Anforderungen der Geschäftsbereiche Schritt halten kann, werden in Organisationen, die ausschließlich mit herkömmlichen Governance-Ansätzen arbeiten, die Benutzer die Sicherheitskontrollen umgehen oder kostspielige Verzögerungen für die Geschäftsbereiche auftreten.

AWS bietet zahlreiche Sicherheitsfunktionen, mit deren Hilfe Sie Ihre IT-Ressourcen einfach und wirksam schützen können. Diese Funktionen, dazugehörige Anleitungen und Links zu weiteren Informationen zu den Funktionen finden Sie nachstehend:

AWS-Funktion zur Ermöglichung von Governance	Sicherheit nach Maß
Amazon Linux-AMIs (Amazon Machine Images, Computerabbilder)	Bieten die Möglichkeit der einheitlichen Bereitstellung eines "goldenen" (gehärteten) Abbilds, das bei allen Instance-Bereitstellungen verwendet wird. Weitere Informationen.
Amazon EC2 – Dedicated Instances	Stellen ein privates, isoliertes virtuelles Netzwerk bereit und sicher, dass Ihre Amazon EC2-Instances auf Hardware-Ebene isoliert sind und in einer VPC gestartet werden. Weitere Informationen.
Amazon EC2 – Assistent zum Starten von Instances	Ermöglicht einen einheitlichen Startprozess durch Einschränken der Computerabbilder, die beim Starten von Instances zur Verfügung stehen. Weitere Informationen.
Amazon EC2-Sicherheitsgruppen	Ermöglichen eine differenzierte Steuerung des ein- und ausgehenden Datenverkehrs, indem diese Gruppen als Firewall fungieren, die den Datenverkehr für eine oder mehrere Instances kontrollieren. Weitere Informationen.
Amazon Glacier-Archive	Bieten einen kostengünstigen langfristigen Speicherservice zum Schutz und zur beständigen Speicherung von Datenarchiven und -sicherungen unter standardmäßiger Verwendung einer 256-Bit-AES-Verschlüsselung. Weitere Informationen.
Amazon S3 – Verschlüsselung auf dem Client	Ermöglicht die Verschlüsselung Ihrer Daten vor dem Senden an Amazon S3, indem Sie eine eigene Bibliothek anlegen, die Ihre Daten auf Client-Seite verschlüsselt, bevor sie in Amazon S3 hochgeladen werden. Das AWS SDK für Java ermöglicht auch eine automatische Verschlüsselung Ihrer Daten, ehe sie in Amazon S3 hochgeladen werden. Weitere Informationen.

Amazon S3 – Verschlüsselung auf dem Server	Ermöglicht eine Verschlüsselung von in AWS gespeicherten Objekten und verwalteten Schlüsseln mithilfe einer 256-Bit-AES-Verschlüsselung für Amazon S3-Daten. Weitere Informationen.
Amazon VPC	Bietet ein virtuelles Netzwerks, das weitgehend einem herkömmlichen lokal betriebenen Netzwerk entspricht, jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen kann. Ermöglicht das Erstellen eines logisch isolierten Bereichs in AWS, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk ausführen können. Weitere Informationen.
Amazon VPC – Logische Isolierung	Ermöglicht eine virtuelle Isolierung von Ressourcen, indem Computerabbilder von anderen Netzwerkressourcen isoliert werden. Weitere Informationen.
Amazon VPC – Netzwerk-ACLs	Ermöglichen eine Firewall-ähnliche Isolierung für dazugehörige Subnetze, indem ein- und ausgehender Datenverkehr auf Subnetzebene kontrolliert wird. Weitere Informationen.
Amazon VPC – Private IP-Adressen	Schützen private IP-Adressen vor der Offenlegung im Internet, indem der dazugehörige Datenverkehr durch eine NAT-Instance (Network Address Translation, Netzwerkadressenübersetzung) in ein öffentliches Subnetz geleitet wird. Weitere Informationen.
Amazon VPC-Sicherheitsgruppen	Ermöglichen eine Firewall-ähnliche Isolierung für dazugehörige Amazon EC2-Instances, indem ein- und ausgehender Datenverkehr auf Instance-Ebene kontrolliert wird. Weitere Informationen.
AWS CloudFormation-Vorlagen	Ermöglichen die einheitliche Bereitstellung eines spezifischen Computerabbilds gemeinsam mit anderen Ressourcen und Konfigurationen mithilfe von Skripts. Weitere Informationen.
AWS Direct Connect	Beseitigt die Notwendigkeit einer öffentlichen Internetverbindung mit AWS durch die Inbetriebnahme einer Standleitung von Ihren Standort zum AWS-Rechenzentrum. Weitere Informationen.
Lokale hardware-/softwaregestützte VPN-Verbindungen	Bieten eine differenzierte Steuerung der Netzwerksicherheit, indem sichere Verbindungen zwischen vorhandenen Netzwerken und AWS zugelassen werden. Weitere Informationen.
Virtuell private Gateways	Ermöglichen eine differenzierte Steuerung der Netzwerksicherheit, indem eine Möglichkeit zum Einrichten einer hardwaregestützten VPN-Verbindung mit Ihrer VPC geboten wird. Weitere Informationen.

Management der Protokollierung von IT-Ressourcen

Ein entscheidender Faktor für den Schutz der IT ist die Protokollierung von IT-Ressourcen. Bei einer Vielzahl von Anwendungsfällen ist die Protokollierung für IT-Governance von entscheidender Bedeutung, so z. B. bei der Erkennung/Nachverfolgung verdächtigen Verhaltens, zur Unterstützung kriminaltechnischer Untersuchungen, Erfüllung von Compliance-Anforderungen, Unterstützung IT-/Netzwerkwartung und -betrieb, für die Kontrolle/Senkung von IT-Sicherheitskosten, zur Überwachung von Service Levels und Unterstützung interner Geschäftsprozesse. Organisationen sind zunehmend von einem effektiven Protokollmanagement abhängig, um wichtige Governance-Funktionen zu unterstützen, wie z. B. Kostenmanagement, Überwachung von Service Level und Line-of-Business-Anwendungen und andere Aktivitäten mit Schwerpunkt auf IT-Sicherheit und -Compliance. Der SANS Log Management Survey zeigt durchgängig, dass Organisationen stetig versuchen, ihre Protokolle noch sinnvoller zu nutzen. Doch sie haben Probleme zu erreichen, dass bei Anwendungsfällen mit Nutzung lokaler Ressourcen diese Protokolle erfasst und analysiert werden. Bei zunehmender Anzahl von Protokolltypen, die aus verschiedenen IT-Ressourcen erfasst und analysiert werden, stehen Organisationen vor der Herausforderung, den manuellen Aufwand für die Normalisierung von Protokolldaten in vielen verschiedenen Formaten sowie die Such-, Korrelations- und Berichtsfunktionen in den Griff zu bekommen. Das Protokollmanagement ist eine Schlüsselfunktion für die Sicherheitsüberwachung, Compliance und effektive Entscheidungsfindung für Zehn- oder Hunderttausende von Aktivitäten jeden Tag.

AWS bietet zahlreiche Protokollierungsfunktionen, mit denen Sie die Nutzung Ihrer IT-Ressourcen effektiv protokollieren und nachverfolgen können. Diese Funktionen, dazugehörige Anleitungen und Links zu weiteren Informationen zu den Funktionen finden Sie nachstehend:

AWS-Funktion zur Ermöglichung von Governance	Sicherheit nach Maß
Amazon CloudFront-Zugriffsprotokolle	Protokolldateien mit Informationen zum Endbenutzerzugriff auf Ihre Objekte. Protokolle können direkt in einem bestimmten Amazon S3-Bucket übertragen werden. Weitere Informationen.
Amazon RDS-Datenbankprotokolle	Bieten eine Möglichkeit zur Überwachung verschiedener Protokolldateien, die von Ihren Amazon RDS-Datenbank-Instances erzeugt werden. Diese dienen zur Diagnose, Fehlerbehebung und Korrektur von Problemen bei der Datenbankkonfiguration und -leistung. Weitere Informationen.
Amazon S3 – Ablauf von Objekten	Ermöglicht einen automatisierten Ablauf von Protokollen, in dem das Entfernen von Objekten nach einem festgelegten Zeitraum zeitlich geplant wird. Weitere Informationen.
Amazon S3-Serverzugriffsprotokolle	Protokolle von Zugriffsanforderungen mit Details zur Anforderung wie z. B. Anforderungstyp, Ressource, für die die Anforderung erfolgt ist, sowie Datum und Uhrzeit der Verarbeitung der Anforderung. Weitere Informationen.
AWS CloudTrail	Bietet über die AWS Management Console oder APIs Protokolle zu sicherheitsbezogenen Aktionen. Weitere Informationen.

Management der IT-Leistung

Überwachen von und Reagieren auf Ereignisse

Das Leistungsmanagement und die Überwachung der IT sind zu einem strategisch wichtigen Bestandteil von IT-Governance-Programmen geworden. Die IT-Überwachung ist ein wesentliches Element von Governance, welches das Verhindern, Erkennen und Korrigieren von IT-Problemen ermöglicht, die sich auf die Leistung und/oder Sicherheit auswirken können. Die wesentliche Herausforderung in lokalen Umgebungen beim IT-Leistungsmanagement ist, was Governance betrifft, dass Sie es bei der Verwaltung sämtlicher Ebenen Ihrer IT-Ressourcen mit mehreren Überwachungssystemen zu tun haben. Und die Kombination aus herstellereigenen Verwaltungs-Tools und IT-Prozessen führt zu einer systemischen Komplexität, die die Reaktionszeiten bestenfalls verlangsamt und sich schlimmstenfalls auf die Effektivität von IT-Leistungsmanagement und -Überwachung auswirkt. Darüber hinaus sorgen die steigende Komplexität und Ausgeklügeltheit von Sicherheitsbedrohungen dafür, dass sich die Funktionen für die Überwachung von Ereignissen und die entsprechenden Reaktionen rasch weiterentwickeln müssen, um aufkommende Bedrohungen im Griff zu behalten. Das lokale Leistungsmanagement sieht sich demzufolge weiter wachsenden Herausforderungen gegenüber, was die Beschaffung von Infrastruktur, Skalierbarkeit, die Fähigkeit zur Simulation von Testbedingungen in mehreren Regionen usw. angeht.

In AWS gibt es mehrere Überwachungsfunktionen, mit denen Sie Ihre IT-Ressourcen einfach und wirksam überwachen und verwalten können. Diese Funktionen, dazugehörige Anleitungen und Links zu weiteren Informationen zu den Funktionen finden Sie nachstehend:

AWS-Funktion zur Ermöglichung von Governance	Sicherheit nach Maß
Amazon CloudWatch	Stellt statistische Daten bereit, mit deren Hilfe Sie das Betriebsverhalten Ihrer Instances anzeigen, analysieren und Alarme festlegen können. Zu diesen Metriken zählen die CPU-Auslastung, der Netzwerkdatenverkehr, die E/A-Leistung und Latenz. Weitere Informationen.
Amazon CloudWatch-Alarme	Einheitliche Benachrichtigungen bei kritischen Ereignissen durch Angeben benutzerdefinierter Metriken, Alarme und Benachrichtigungen bei Ereignissen. Weitere Informationen.
Amazon EC2-Instance-Status	Überprüfungen des Instance-Status mit zusammengefassten Ergebnissen automatisierter Tests und Informationen zu bestimmten Aktivitäten, die für Ihre Instances geplant sind. Genutzt werden automatisierte Überprüfungen zum Erkennen, ob sich bestimmte Probleme auf Ihre Instances auswirken. Weitere Informationen.
Amazon Incident Management Team	Bietet eine laufende Erkennung, Überwachung und Verwaltung durch rund um die Uhr aktive Mitarbeiter, um das Ermitteln, Untersuchen und Beheben bestimmter sicherheitsrelevanter Ereignisse zu unterstützen. Weitere Informationen.
Amazon S3 – TCP Selective Acknowledgement	Ermöglicht das Verbessern der Wiederherstellungszeit nach einer großen Anzahl von Paketverlusten. Weitere Informationen.

Amazon Simple Notification Service	Bietet einheitliche Benachrichtigungen bei kritischen Ereignissen durch Übermittlung von Nachrichten an Abonnenten (Endpunkte oder Clients). Weitere Informationen.
AWS Elastic Beanstalk	Ermöglicht das Überwachen von Details zur Bereitstellung von Anwendungen wie Kapazitätsbereitstellung, Lastverteilung, automatische Skalierung und Statusüberwachung von Anwendungen. Weitere Informationen.
Elastic Load Balancing	Automatisches Verteilen des eingehenden Anwendungsdatenverkehrs auf mehrere Amazon EC2-Instances, indem überlastete Instances erkannt werden und der Datenverkehr zu nicht ausgelasteten Instances geleitet wird. Weitere Informationen.

Erreichen von Ausfallsicherheit

Die Planung des Schutzes von Daten und der Notfallwiederherstellung sollte bei der IT-Governance aller Organisationen ganz oben auf der Liste stehen. Der Nutzen einer Notfallwiederherstellung steht außer Frage. Alle Organisationen sind daran interessiert, nach einem Notfall oder einer Katastrophe den Betrieb schnellstmöglich wieder aufzunehmen. Doch die Implementierung von Governance im Umfeld der Ausfallsicherheit von IT-Ressourcen kann teuer und komplex und außerdem mühsam und zeitaufwendig sein. Organisationen sehen sich einer wachsenden Anzahl von Ereignissen gegenüber, die für ungeplante Ausfallzeiten und Betriebsstörungen sorgen können. Diese Ereignisse können durch technische Probleme (z. B. Viren, beschädigte Daten, menschliche Fehler usw.) oder Naturereignisse (z. B. Brände, Überschwemmungen, Stromausfälle, wetterbedingte Ausfälle usw.) verursacht werden. Und aufgrund des unaufhörlichen Datenwachstums müssen Organisationen den Anstieg von Kosten und Komplexität bei Planung, Tests und Betrieb lokaler Failover-Standorte bewältigen.

Angesichts dieser Herausforderungen ermöglicht die Servervirtualisierung beim Cloud Computing, dass Programme zur Sicherstellung der Ausfallsicherheit realisierbar und wirtschaftlich sind. AWS bietet zahlreiche Funktionen, mit deren Hilfe Sie mühelos und wirksam Ausfallsicherheit für Ihre IT-Ressourcen erreichen können. Diese Funktionen, dazugehörige Anleitungen und Links zu weiteren Informationen zu den Funktionen finden Sie nachstehend:

AWS-Funktion zur Ermöglichung von Governance	Sicherheit nach Maß
Amazon EBS-Snapshots	Hochverfügbare, überaus zuverlässige und berechenbare Speicher-Volumes mit der Möglichkeit inkrementeller zeitpunktbezogener Sicherungen von Serverdaten. Weitere Informationen.
Amazon RDS – Multi-AZ-Bereitstellungen	Die Fähigkeit zum Schutz Ihrer Daten im Ernstfall mithilfe automatisierter Kontrollen der Verfügbarkeit und einer homogenen ausfallsicheren Architektur. Weitere Informationen.

AWS Import/Export	Die Möglichkeit zum lokalen Verschieben riesiger Datenmengen durch das rasche Erstellen von Import- und Exportaufträgen unter Einsatz des internen Hochgeschwindigkeitsnetzwerks von Amazon. Weitere Informationen.
AWS Storage Gateway	Eine reibungslose und sichere Integration Ihrer lokalen IT-Umgebung mit der AWS-Speicherinfrastruktur durch die Planung von Snapshots, die das Gateway in Amazon S3 in Form von Amazon EBS-Snapshots speichert. Weitere Informationen.
AWS Trusted Advisor	Bietet ein automatisiertes Leistungsmanagements und eine Verfügbarkeitskontrolle, indem Möglichkeiten zum Steigern der Verfügbarkeit und Redundanz Ihrer AWS-Anwendung ermittelt werden. Weitere Informationen.
Umfassende Lösungen anderer Anbieter	Ermöglichen eine sichere Datenspeicherung und automatisierte Kontrolle der Verfügbarkeit, indem Sie sich einfach mit einem Angebot von Anwendungen und Tools verbinden. Weitere Informationen.
Verwaltete AWS No-SQL/SQL-Datenbankservices	Bieten eine sichere und beständige Datenspeicherung mit automatischer Replikation von Datenelementen in mehrere Availability Zones in einer Region, um hohe Verfügbarkeit und Datenbeständigkeit integriert zu gewährleisten. Weitere Informationen: • Amazon Dynamo DB • Amazon RDS
Bereitstellung in mehreren Regionen	Bietet eine geografischen Vielfalt bei Datenverarbeitungsstandorten, Energieversorgungsnetzen, Störungszonen usw. Weitere Informationen.
Route 53 – Zustandsprüfungen und DNS-Failover	Überwachung der Verfügbarkeit gespeicherter Sicherungsdaten, indem Sie ein DNS-Failover in Aktiv/Aktiv-, Aktiv/Passiv- und gemischter Konfiguration einrichten können, um die Verfügbarkeit Ihrer Anwendung zu steigern. Weitere Informationen.

Index der Governance-Funktionen für Services

Die Informationen wurden bislang nach Governance-Bereich vorgestellt. Zu Ihrer Referenz enthält die folgende Tabelle eine Übersicht der Governance-Funktionen gemäß dem jeweiligen AWS-Service:

AWS-Service	Governance-Funktion
Amazon EC2	Amazon EC2 – Idempotenz beim Start von Instances Amazon EC2 – Versehen von Ressourcen mit Tags Amazon Linux-AMIs (Amazon Machine Images, Computerabbilder) Amazon EC2 – Dedicated Instances Amazon EC2 – Assistent zum Starten von Instances Amazon EC2-Sicherheitsgruppen
Elastic Load Balancing	Elastic Load Balancing – Verteilung von Datenverkehr
Amazon VPC	Amazon VPC Amazon VPC – Logische Isolierung Amazon VPC – Netzwerk-ACLs Amazon VPC – Private IP-Adressen Amazon VPC-Sicherheitsgruppen Lokale hardware-/softwaregestützte VPN-Verbindungen
Amazon Route 53	Amazon Route 53-Latenz – Ressourcendatensätze Route 53 – Zustandsprüfungen und DNS-Failover
AWS Direct Connect	AWS Direct Connect
Amazon S3	Amazon S3 – Zugriffskontrolllisten (ACLs) Amazon S3 – Bucket-Richtlinien Amazon S3 – Abfrage-String-Authentifizierung Amazon S3 – Verschlüsselung auf dem Client Amazon S3 – Verschlüsselung auf dem Server Amazon S3 – Ablauf von Objekten Amazon S3-Serverzugriffsprotokolle Amazon S3 – TCP Selective Acknowledgement Amazon S3 – TCP Window Scaling

Amazon Glacier	Amazon Glacier – Bestand von Archivdatenspeichern Amazon Glacier-Archive
Amazon EBS	Amazon EBS-Snapshots
AWS Import/Export	AWS Import/Export – Übertragen großer Datenmengen
AWS Storage Gateway	AWS Storage Gateway-Integration AWS Storage Gateway-APIs
Amazon CloudFront	Amazon CloudFront Amazon CloudFront-Zugriffsprotokolle
Amazon RDS	Amazon RDS-Datenbankprotokolle Amazon RDS – Multi-AZ-Bereitstellungen Verwaltete AWS No-SQL/SQL-Datenbankservices
Amazon Dynamo DB	Verwaltete AWS No-SQL/SQL-Datenbankservices
AWS Management Console	Seite "Account Activity" AWS-Fakturierung AWS-Services – Preise AWS Trusted Advisor Fakturierungsbenachrichtigungen Konsolidierte Fakturierung Nutzungsbasierte Preise AWS CloudTrail Amazon Incident Management Team Amazon Simple Notification Service Bereitstellung in mehreren Regionen
AWS Identity and Access Management (IAM)	AWS IAM – Multifaktor-Authentifizierung (MFA) AWS IAM – Kennwortrichtlinie AWS IAM-Berechtigungen AWS IAM-Richtlinien AWS IAM-Rollen

Amazon CloudWatch	AWS CloudWatch-Dashboard Amazon CloudWatch-Alarme
AWS Elastic Beanstalk	AWS Elastic Beanstalk-Überwachung
AWS CloudFormation	AWS CloudFormation-Vorlagen
AWS Data Pipeline	AWS Data Pipeline – Task Runner
AWS CloudHSM	CloudHSM-Schlüsselspeicher
AWS Marketplace	Umfassende Lösungen anderer Anbieter
Rechenzentren	Physische AWS-Zugangskontrollen gemäß SOC1 Physische AWS-Zugangskontrollen gemäß SOC 2 Physische AWS-Zugangskontrollen gemäß PCI DSS Physische AWS-Zugangskontrollen gemäß DIN ISO 27001 Physische AWS -Zugangskontrollen gemäß FedRAMP

Schlussfolgerung

Der Hauptschwerpunkt von IT-Governance ist das Management von Ressourcen, Sicherheit und Leistung, um in Abstimmung auf die Geschäftsziele für einen Nutzen zu sorgen. Angesichts der Wachstumsrate und steigenden Komplexität von Informationstechnologie wird es in lokalen Umgebungen immer schwieriger, ein Maß zu erreichen, um die differenzierten Kontrollen und Funktionen bereitzustellen, die für IT-Governance hoher Qualität auf wirtschaftliche Weise benötigt werden. Aus denselben Gründen, aus denen die Bereitstellung von Infrastruktur in der Cloud Vorteile gegenüber der lokalen Bereitstellung hat, ermöglicht Cloud-basierte Governance niedrigere Einstiegskosten, einen einfacheren Betrieb und mehr Agilität. Es wird mehr Übersicht und Automatisierung geboten, damit sich Organisationen auf ihr Geschäft konzentrieren können.

Referenzen und weiterführende Literatur

Wozu kann ich AWS verwenden? http://aws.amazon.com/solutions/aws-solutions/.

Wie sehen die ersten Schritte mit AWS aus? http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws-intro.html