AWS Cloud Adoption Framework

Sicherheitsperspektive

Juni 2016

© 2016, Amazon Web Services, Inc. oder Tochterfirmen. Alle Rechte vorbehalten.

Hinweise

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt das aktuelle Produktangebot und die Praktiken von AWS zum Erstellungsdatum dieses Dokuments dar. Änderungen vorbehalten. Kunden sind verantwortlich für ihre eigene Interpretation der in diesem Dokument zur Verfügung gestellten Informationen und für die Nutzung der AWS-Produkte oder -Services. Diese werden alle ohne Mängelgewähr und ohne jegliche Garantie, weder ausdrücklich noch stillschweigend, bereitgestellt. Dieses Dokument gibt keine Garantien, Gewährleistungen, vertragliche Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen Partnern, Zulieferern oder Lizenzgebern. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument gehört, weder ganz noch teilweise, nicht zu den Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Überblick

Das Amazon Web Services (AWS) Cloud Adoption Framework[1] (CAF) gibt Anleitung zum Koordinieren der verschiedenen Bereiche von Organisationen, die zum Cloud Computing migrieren. Die CAF-Anleitung ist in eine Reihe von Schwerpunktbereichen unterteilt, die für die Implementierung cloudbasierter IT-Systeme relevant sind. Diese Schwerpunktbereiche werden als *Perspektiven* bezeichnet, und jede Perspektive ist weiter in *Komponenten* unterteilt. Es gibt ein Whitepaper für jede der sieben CAF-Perspektiven.

Dieses Whitepaper behandelt die Sicherheitsperspektive, die sich darauf konzentriert, Anleitungen und Prozesse für Ihre bestehenden Sicherheitskontrollen bereitzustellen, die spezifisch auf die Nutzung von AWS in Ihrer Umgebung ausgerichtet sind.

Einführung

Sicherheit bei AWS ist oberstes Gebot. Alle AWS-Kunden profitieren von einer Rechenzentrums- und Netzwerkarchitektur, die eingerichtet wurde, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen. AWS und seine Partner bieten Hunderte von Tools und Funktionen an, mit denen Sie Ihre Sicherheitsziele in Bezug auf Sichtbarkeit, Auditierbarkeit, Kontrollierbarkeit und Agilität erfüllen können. Das bedeutet, Sie haben die Sicherheit, die Sie benötigen, jedoch ohne den Kapitalaufwand und mit viel geringerer betrieblicher Verwaltung als bei einer lokal installierten Umgebung.

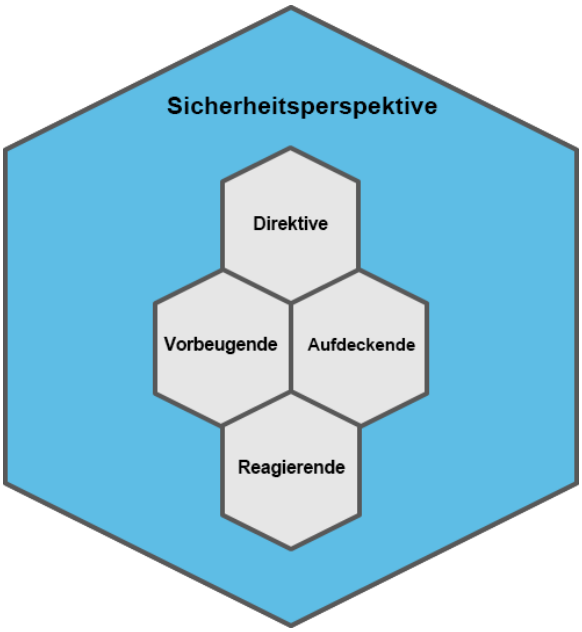

Abbildung 1: AWS CAF-Sicherheitsperspektive

Das Ziel der Sicherheitsperspektive ist es, Sie beim Strukturieren und Implementieren der Kontrollen zu unterstützen, die für Ihre Organisation am besten geeignet sind. Wie in Abbildung 1 gezeigt, geben die Komponenten der Sicherheitsperspektive die Prinzipien vor, die Ihnen dabei helfen, die Umstellung der Sicherheitskultur Ihrer Organisation voranzutreiben. Dieses Whitepaper behandelt für jede Komponente bestimmte Maßnahmen, die Sie ergreifen können, sowie die Mittel, um den Fortschritt zu messen:

- **Direktive** Kontrollen stellen die Modelle für Überwachung, Risiko und Compliance bereit, unter denen die Umgebung ausgeführt wird.
- **Vorbeugende** Kontrollen schützen Ihre Arbeitslasten und entschärfen Sicherheitsrisiken und Schwachstellen.
- **Aufdeckende** Kontrollen bieten volle Sichtbarkeit und Transparenz des Betriebs Ihrer Bereitstellungen in AWS.
- **Reagierende** Kontrollen sorgen für die Korrektur potenzieller Abweichungen von Ihren Sicherheits-Basiswerten.

Die Sicherheit in der Cloud ist bekannt. Die Steigerung der Agilität und die Fähigkeit, Aktionen schneller, in größerem Maßstab und zu niedrigeren Kosten durchzuführen, setzt bewährte Prinzipien der Informationssicherheit nicht außer Kraft.

Nach der Erläuterung der vier Komponenten der Sicherheitsperspektive zeigt Ihnen dieses Whitepaper die Schritte auf, die Sie unternehmen können, um sicherzustellen, dass Ihre Cloud-Umgebung hinreichend abgesichert ist:

- Definieren Sie eine **Strategie für die Sicherheit** in der Cloud. Betrachten Sie vor der Umstellung Ihre geschäftlichen Zielvorgaben, den Ansatz für das Risikomanagement und die Möglichkeiten, die Ihnen die Cloud bietet.
- Stellen Sie ein **Sicherheitsprogramm** zur Entwicklung und Implementierung von Funktionen für Sicherheit, Datenschutz, Compliance und Risikomanagement bereit. Der Umfang kann zu Anfang unüberschaubar erscheinen, daher ist es wichtig, eine Struktur zu erstellen, mit der Ihre Organisation die Sicherheit in der Cloud ganzheitlich sicherstellen kann. Die Implementierung sollte eine interaktive Entwicklung ermöglichen, so dass die Funktionen weiter verbessert werden können, während Programme weiterentwickelt werden. Dadurch wird die Sicherheitskomponente zu einer Art Katalysator für die übrigen Cloud-Einführungsbestrebungen der Organisation.

- Entwickeln Sie robuste Funktionen für **Sicherheitsoperationen**, die ständig gepflegt und verbessert werden. Sicherheitsfunktionen werden immer weiter entwickelt. Wir empfehlen, dass Sie neue Funktionen mit betrieblicher Gründlichkeit aufbauen, so dass durch ständige Iteration eine kontinuierliche Verbesserung erreicht werden kann.

Sicherheitsvorteile von AWS

Cloud-Sicherheit bei AWS ist unsere oberste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die eingerichtet wurde, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Ein Vorteil der AWS-Cloud besteht darin, dass Sie die Möglichkeit zum Skalieren und Entwickeln haben, wobei gleichzeitig eine sichere Umgebung aufrechterhalten wird. Sie zahlen nur für die Services, die Sie nutzen, d. h., Sie bekommen die Sicherheit, die Sie brauchen, aber ohne Vorab-Investitionen und zu niedrigeren Kosten als bei einer lokalen Umgebung.

Dieser Abschnitt behandelt einige der Sicherheitsvorteile der AWS-Plattform.

Auf Sicherheit ausgelegt

Die Infrastruktur der AWS-Cloud wird in AWS-Rechenzentren ausgeführt und ist darauf ausgelegt, auch die Anforderungen äußerst sicherheitssensitiver Kunden zu erfüllen. Die AWS-Infrastruktur ist so angelegt, dass sie hohe Verfügbarkeit gewährleistet und gleichzeitig wirkungsvolle Maßnahmen zum Schutz der Kundendaten bereitstellt. Alle Daten werden in streng gesicherten AWS-Rechenzentren gespeichert. Mit Netzwerk-Firewalls, die in Amazon VPC integriert sind, und Firewall-Funktionen für Webanwendungen in AWS WAF können Sie private Netzwerke erstellen und den Zugriff auf Ihre Instances und Anwendungen kontrollieren.

Wenn Sie Systeme in der AWS-Cloud bereitstellen, hilft Ihnen AWS, indem wir die Sicherheitsverantwortlichkeiten mit Ihnen teilen. Mit Grundsätzen für ein sicheres Design entwickelt AWS die zu Grunde liegende Infrastruktur, und Sie können Ihre eigene Sicherheitsarchitektur für Arbeitslasten implementieren, die in AWS bereitgestellt werden.

Hoch automatisiert

Bei AWS entwickeln wir zweckorientierte Sicherheitstools und passen sie an ihre jeweilige Umgebung, Größe und globalen Anforderungen an. Dadurch, dass Sicherheitstools von Grund auf neu entwickelt werden, kann AWS viele der Routineaufgaben automatisieren, für die Sicherheitsexperten normalerweise Zeit aufwenden müssen. Dadurch können die Sicherheitsexperten von AWS mehr Zeit damit verbringen, Maßnahmen zu konzipieren, die die Sicherheit Ihrer AWS Cloud-Umgebung noch weiter verbessern. Mit einem umfassenden Angebot an APIs und Tools können Sie auch das Sicherheits-Engineering sowie betriebliche Funktionen automatisieren. Identitätsverwaltung, Netzwerksicherheit und Datenschutz sowie Überwachungsfunktionen können mit gängigen, bereits installierten Software-Entwicklungsmethoden vollständig automatisiert und bereitgestellt werden. Sie können auf Sicherheitsprobleme mit automatisierten Tools reagieren. Wenn Sie die automatisierten Funktionen der AWS-Services nutzen, anstatt Mitarbeiter einzusetzen, um die Sicherheit zu überwachen und auf einen Vorfall zu reagieren, wird Ihr System überwacht, überprüft und bei Zwischenfällen eine Reaktion ausgelöst.

Hochverfügbar

AWS baut Rechenzentren in mehreren geographischen Regionen. Innerhalb der Regionen gibt es mehrere Availability Zones, um Resilienz zu gewährleisten. AWS konzipiert die Rechenzentren mit überschüssiger Bandbreite, damit im Fall einer Störung ausreichend Kapazität zur Verfügung steht, um Lasten auszugleichen, den Datenverkehr auf die verbleibenden Standorte umzuleiten und so die Auswirkungen auf unsere Kunden zu minimieren. Sie können diese Strategie mit mehreren Regionen und mehreren AZ ebenfalls nutzen, um äußerst ausfallsichere Anwendungen bei geringen Störfallkosten aufzubauen, um Daten leicht replizieren und sichern zu können und globale Sicherheitskontrollen gleichmäßig verteilt im gesamten Unternehmen bereitzustellen.

Hoch akkreditiert

AWS-Umgebungen werden ständig überprüft und erhalten Zertifizierungen von Akkreditierungsstellen auf der ganzen Welt. Das bedeutet, dass Ihre Compliance-Anforderungen bereits teilweise erfüllt sind. Weitere Informationen über die Sicherheitsvorschriften und -standards, die AWS erfüllt, finden Sie auf der Website zur AWS Cloud Compliance[2]. Um Ihnen bei der Erfüllung bestimmter Behörden-, Industrie- und Unternehmens-Sicherheitsstandards und -vorschriften zu helfen, bietet AWS Zertifizierungsberichte an, in denen beschrieben ist, wie die AWS Cloud-Infrastruktur die Anforderungen einer umfassenden Liste globaler Sicherheitsstandards erfüllt. Verfügbare Compliance-Berichte erhalten Sie bei Ihrem AWS-Kundenbetreuer. Sie können viele von AWS betriebene Kontrollen in Ihre eigenen Compliance- und Zertifizierungsprogramme übernehmen. Dadurch lassen sich die Kosten für die Aufrechterhaltung und Durchführung von Maßnahmen zur Gewährleistung der Sicherheit verringern, wobei gleichzeitig die Kontrollen selbst aufrechterhalten werden. Wenn eine starke Grundlage vorhanden ist, können Sie die Sicherheit Ihrer Arbeitslasten in Bezug auf Agilität, Resilienz und Umfang optimieren.

In den übrigen Kapiteln dieses Whitepapers werden die einzelnen Komponenten der Sicherheitsperspektive vorgestellt. Sie können diese Komponenten dazu nutzen, die von Ihnen benötigten Sicherheitsziele auszuloten, um Ihre Reise in die Cloud erfolgreich zu absolvieren.

Direktive Komponente

Die direktive Komponente der AWS-Sicherheitsperspektive gibt Anleitung zur Planung Ihrer Sicherheitsmethoden, während Sie Ihre Daten zu AWS migrieren. Der Schlüssel zu einer effektiven Planung liegt darin, die Anleitung zu definieren, die Sie den Mitarbeitern geben wollen, die Ihre Sicherheitsumgebung implementieren und ausführen. Die Informationen müssen ausreichend Anleitung geben, um ermitteln zu können, welche Kontrollen benötigt werden und wie sie ausgeführt werden sollen. Anfängliche Bereiche, die berücksichtigt werden müssen, sind beispielsweise Folgende:

- **Kontoführung**– Anleitungen für die Organisation, um einen Prozess und Verfahrensweisen zur Verwaltung von AWS-Konten zu erstellen. Zu definierende Bereiche sind beispielsweise, wie Kontobestände erfasst und aufrechterhalten werden sollen, welche Vereinbarungen und Zusätze vorhanden sind und nach welchen Kriterien ein AWS-Konto erstellt werden soll. Entwickeln Sie einen Prozess, mit dem Konten konsistent erstellt werden können. Stellen Sie sicher, dass alle Anfangseinstellungen angemessen sind und dass eine klare Inhaberschaft festgelegt ist.
- **Kontoinhaberschaft und Kontaktinformationen** – Stellen Sie ein angemessenes Governance-Modell für die in Ihrer Organisation genutzten AWS-Konten auf und bestimmen Sie, wie die Kontaktinformationen für die einzelnen Konten aufrechterhalten werden sollen. Überlegen Sie, ob die AWS-Konten anstatt mit den E-Mail-Adressen von Personen mit E-Mail-Verteilerlisten verknüpft werden sollen. Dadurch kann eine Gruppe von Personen Informationen von AWS über Ihre Kontoaktivität überwachen und darauf reagieren. Außerdem gewährleistet es Resilienz bei internen Personaländerungen, und es bietet eine Möglichkeit, Verantwortlichkeiten für die Sicherheit festzulegen. Listen Sie Ihr Sicherheitsteam als Sicherheitskontaktpunkt auf, um zeitkritische Mitteilungen zu beschleunigen.
- **Kontrollrahmen** – Entwerfen oder nutzen Sie einen Kontrollrahmen nach Industriestandard, und legen Sie fest, ob Sie Änderungen oder Zusätze benötigen, um AWS-Services auf den erwarteten Sicherheitsstufen zu integrieren. Führen Sie eine Compliance-Zuordnungsübung durch, um zu ermitteln, wie sich Compliance-Anforderungen und Sicherheitskontrollen auf die AWS-Service-Nutzung auswirken.
- **Zuständigkeit für Kontrollen** – Ziehen Sie die Informationen über das AWS-Modell übergreifender Verantwortlichkeit[3] auf der AWS-Website zurate, um zu ermitteln, ob Änderungen an der Zuständigkeit für die Kontrollen vorgenommen werden sollten. Überprüfen und aktualisieren Sie Ihre Verantwortlichkeits-Zuordnungsmatrix (RACI-Diagramm), um Zuständigkeiten für Kontrollen hinzuzufügen, die in der AWS-Umgebung ausgeführt werden.

- **Datenklassifizierung** – Überprüfen Sie die aktuellen Datenklassifizierungen und legen Sie fest, wie diese Klassifizierungen in der AWS-Umgebung verwaltet werden sollen und welche Kontrollen angemessen sind.
- **Änderungs- und Komponentenverwaltung** – Legen Sie fest, wie die Änderungs- und die Komponentenverwaltung in AWS ausgeführt werden sollen. Erstellen Sie ein Mittel, um zu bestimmen, welche Komponenten existieren, wofür die Systeme genutzt werden und wie sie sicher verwaltet werden können. Dieses Mittel kann in eine bestehende Konfigurationsmanagement-Datenbank (CMDB) integriert werden. Erstellen Sie nach Bedarf ein Verfahren für die Namensgebung und das Tagging, so dass Identifizierung und Verwaltung auf der erforderlichen Sicherheitsebene ausgeführt werden können. Sie können diesen Ansatz zum Definieren und Verfolgen von Metadaten verwenden, die eine Identifizierung und Kontrolle erlauben.
- **Datenlokalität** – Legen Sie Kriterien für den Speicherort Ihrer Daten fest, um zu bestimmen, welche Kontrollen benötigt werden, um die regionsübergreifende Konfiguration und Nutzung von AWS-Services zu verwalten. Sie wählen die AWS-Region(en) aus, in der (denen) Ihre Inhalte gehostet werden. Wenn Sie bestimmte geografische Anforderungen haben, können Sie Umgebungen an Standorten Ihrer Wahl erstellen. Sie können Inhalte replizieren und in mehreren Regionen sichern, doch AWS verschiebt Kundendaten nicht außerhalb der vom Kunden gewählten Region(en).
- **Zugang mit geringsten Rechten** – Erstellen Sie eine organisatorische Sicherheitskultur, die auf dem Prinzip der geringsten Rechte und starker Authentifizierung beruht. Implementieren Sie Protokolle, um den Zugriff auf vertrauliche Anmeldeinformationen und wichtige Materialien zu schützen, die mit den AWS-Konten verknüpft sind. Legen Sie Erwartungen dazu fest, wie Berechtigungen unter den Software Engineers, dem Betriebspersonal und anderen Job-Funktionen verteilt sein sollen, die an der Einführung der Cloud beteiligt sind.
- **Playbook und Runbooks für Sicherheitsoperationen** – Definieren Sie Sicherheitsmuster, um langfristige Leitlinien zu erstellen, die die Organisation im Laufe der Zeit zurate ziehen kann. Implementieren Sie die Maßnahmen durch Automatisierung als Runbooks; dokumentieren Sie nach Bedarf Eingriffe durch den Bediener.

Überlegungen

- **Erstellen** Sie ein maßgeschneidertes AWS-Modell übergreifender Verantwortlichkeit für Ihr Ökosystem.
- **Implementieren** Sie im Rahmen Ihres Schutzplans eine starke Authentifizierung für alle Teilnehmer Ihres Kontos.
- **Fördern** Sie eine Kultur der Sicherheitszuständigkeit bei den Anwendungsteams.
- **Erweitern** Sie Ihr Datenklassifizierungsmodell mit den Services in AWS.
- **Integrieren** Sie Ziele und Jobfunktionen für die Entwickler-, Einsatz- und Sicherheitsteams.
- **Erstellen** Sie nach Bedarf eine Strategie zur Benennung und Verfolgung von Konten, die zum Verwalten von Services in AWS verwendet werden.
- **Zentralisieren** Sie Telefon- und E-Mail-Verteilerlisten, so dass Teams überwacht werden können.

Vorbeugende Komponente

Die vorbeugende Komponente der AWS-Sicherheitsperspektive gibt Anleitung zum Implementieren einer Sicherheitsinfrastruktur in AWS und innerhalb Ihrer Organisation. Der Schlüssel zum Implementieren der richtigen Kontrollen liegt darin, dass Sie Ihren Sicherheitsteams dabei helfen, das Selbstvertrauen und die Fähigkeiten zu gewinnen, die sie benötigen, um die Automatisierungs- und Bereitstellungsfähigkeiten aufzubauen, die erforderlich sind, um das Unternehmen in der agilen, skalierbaren Umgebung von AWS zu schützen.

Nutzen Sie die direktive Komponente, um die Kontrollen und Anleitungen festzulegen, die Sie benötigen werden. Mit der vorbeugenden Komponente können Sie anschließend bestimmen, wie die Kontrollen effektiv ausgeführt werden. AWS gibt regelmäßig Anleitung zu bewährten Methoden für die Nutzung der AWS-Services und die Arbeitslast-Bereitstellungsmuster, die als Richtschnur für die Implementierung der Kontrollen genutzt werden können. Besuchen Sie das AWS-Sicherheitszentrum und den Blog. Sehen Sie sich die neuesten Sicherheits-Verfolgungsvideos vom AWS-Gipfel und der re:Invent-Konferenz an.

Berücksichtigen Sie die folgenden Bereiche, um zu ermitteln, welche Änderungen Sie (nötigenfalls) an Ihren aktuellen Sicherheitsarchitekturen und -praktiken vornehmen müssen. Dies ist hilfreich für eine reibungslose und planmäßige AWS-Einführungsstrategie.

- **Identität und Zugriff** – Integrieren Sie die Nutzung von AWS in den Belegschafts-Lebenszyklus der Organisation sowie in die Quellen von Authentifizierung und Autorisierung. Erstellen Sie differenzierte Richtlinien und Rollen für die jeweiligen Benutzer und Gruppen. Erstellen Sie Leitlinien, die wichtige Änderungen nur durch Automatisierung erlauben und unerwünschte Änderungen verhindern oder automatisch rückgängig machen. Mit diesen Schritten verringern Sie den menschlichen Zugriff auf Produktionssysteme und -daten.
- **Schutz der Infrastruktur** – Implementieren Sie eine Sicherheits-Baseline mit Vertrauensgrenzen, Systemsicherheits-Konfiguration und -Wartung (z. B. Härten und Patchen) und anderen angemessenen Punkten zur Richtliniendurchsetzung (z. B. Sicherheitsgruppen, AWS WAF, Amazon API Gateway), um die Anforderungen zu erfüllen, die Sie mit der direktiven Komponente ermittelt haben.
- **Datenschutz** – Wenden Sie geeignete Schutzmaßnahmen an, um Daten in der Übertragung und im Ruhezustand zu schützen. Zu den Schutzmaßnahmen gehören differenzierte Zugriffskontrollen zu Objekten, das Erstellen und Kontrollieren der Verschlüsselungsschlüssel, die zum Verschlüsseln der Daten verwendet werden, die Auswahl geeigneter Methoden zur Verschlüsselung oder zur Aufgliederung in Token, Integritätsvalidierung und die angemessene Aufbewahrung von Daten.

Überlegungen

- **Behandeln** Sie Sicherheit als Code. So können Sie die Sicherheitsinfrastruktur so bereitstellen und validieren, dass sie die Organisation im richtigen Umfang und mit der richtigen Agilität schützt.
- **Erstellen** Sie Leitlinien, angemessene Standardwerte, und bieten Sie Vorlagen und bewährte Methoden als Code an.
- **Bauen** Sie Sicherheitsservices auf, die die Organisation für sich ständig wiederholende oder besonders sensible Sicherheitsfunktionen nutzen kann.

- **Definieren** Sie Teilnehmer, und erstellen Sie ein Storyboard mit ihrer Erfahrung bei der Interaktion mit AWS-Services.
- **Nutzen** Sie das Tool AWS Trusted Advisor, um Ihre AWS-Sicherheitslage kontinuierlich zu bewerten; ziehen Sie eine AWS Well Architected-Prüfung in Erwägung.
- **Legen** Sie eine minimal realisierbare Sicherheits-Baseline fest, und stecken Sie das Ziel für die Arbeitslasten, die Sie schützen, immer wieder höher.

Aufdeckende Komponente

Die aufdeckende Komponente der AWS CAF-Sicherheitsperspektive bietet Anleitung, wie Sie sich einen Überblick über die Sicherheitslage Ihrer Organisation verschaffen. Mit Services wie AWS CloudTrail, servicespezifischen Protokollen und API/CLI-Rückgabewerten können wertvolle Daten und Informationen gesammelt werden. Wenn diese Informationsquellen in eine skalierbare Plattform für das Verwalten und Überwachen von Protokollen, Ereignismanagement, Tests und Bestand/Überprüfung eingebunden werden, gibt Ihnen das die Transparenz und betriebliche Agilität, die Sie für die Sicherheit Ihrer Operationen benötigen.

- **Protokollieren und Überwachen** – AWS bietet eine systemeigene Protokollierung und Services, die Sie nutzen können, um Ereignisse in der AWS-Umgebung nahezu in Echtzeit verfolgen zu können. Diese Tools lassen sich in Ihre bestehenden Protokollierungs- und Überwachungslösungen integrieren. Durch eine tiefe Einbettung der Protokollierungs- und Überwachungsergebnisse in den Workflow der IT-Organisation erhalten Sie einen umfassenden Überblick über alle sicherheitsbezogenen Aktivitäten.
- **Sicherheitstests** – Testen Sie die AWS-Umgebung, um sicherzustellen, dass die vorgegebenen Sicherheitsstandards erfüllt werden. Durch die Tests können Sie ermitteln, ob Ihre Systeme beim Auftreten bestimmter Ereignisse wie erwartet reagieren. So sind Sie auf tatsächliche Vorkommnisse besser vorbereitet. Beispiele für Sicherheitstests sind Schwachstellen-Scans, Penetrationstests und Fehlerinjektionen, um zu überprüfen, ob die Standards erfüllt werden. Ziel ist es zu ermitteln, ob Ihre Kontrollen wie erwartet reagieren.

- **Bestandsverwaltung** – Wenn Sie wissen, welche Arbeitslasten bereitgestellt sind und ausgeführt werden, können Sie sicherstellen, dass die Umgebung auf den Sicherheitsstufen ausgeführt wird, die durch die Sicherheitsstandards erwartet und vorgegeben sind.
- **Änderungserkennung** – Um sich auf die Grundsicherung durch vorbeugende Kontrollen verlassen zu können, muss auch bekannt sein, wann sich diese Kontrollen ändern. Richten Sie Maßnahmen ein, mit denen sich Abweichungen zwischen der sicheren Konfiguration und dem aktuellen Zustand ermitteln lassen.

Überlegungen

- **Bestimmen** Sie, welche Protokollierungsinformationen Sie für Ihre AWS-Umgebung erfassen, überwachen und analysieren wollen.
- **Bestimmen** Sie, wie die Geschäftsfunktionen Ihres bestehenden Security Operations Centers (SOC) die Sicherheitsüberwachung und -verwaltung von AWS in bestehende Praktiken integrieren sollen.
- **Führen Sie** ständig Schwachstellen-Scans und Penetrationstests gemäß den entsprechenden AWS-Verfahren durch.

Reagierende Komponente

Die reagierende Komponente der AWS CAF-Sicherheitsperspektive bietet Anleitungen für den reagierenden Teil des Sicherheitssystems Ihrer Organisation. Wenn Sie die AWS-Umgebung in Ihr existierendes Sicherheitssystem integrieren und anschließend Aktionen vorbereiten und simulieren, die Reaktionen erfordern, können Sie besser auf real auftretende Vorfälle reagieren.

Durch die automatisierte Vorfallreaktion und Wiederherstellung sowie die Möglichkeit der Schadensbegrenzung durch Notfallwiederherstellung ist es möglich, den primären Fokus des Sicherheitsteams von der Reaktion auf die Spurensicherung und Ursachenanalyse zu lenken. Unter anderem sollten folgende Aspekte bei der Anpassung Ihres Sicherheitssystems berücksichtigt werden:

- **Vorfallreaktion** – Während eines Vorfalls die Auswirkungen einzudämmen und zu einem bekannten guten Zustand zurückzukehren, sind wichtige Elemente eines Reaktionsplans. Wenn Sie diese Funktionen beispielsweise mit AWS Config-Regeln und AWS Lambda-Responder-Scripts automatisieren, können Sie die Reaktion bei Internetgeschwindigkeit skalieren. Überprüfen Sie die aktuellen Vorfallreaktionsprozesse und ermitteln Sie, ob und wie die automatische Reaktion und Wiederherstellung ausgelöst wird und wie sie bei AWS-Komponenten verwaltet wird. Die Funktionen des Security Operations Centers sollten fest in die AWS-APIs integriert sein, damit Reaktionen schnellstmöglich ausgelöst werden können. Dies wird durch die Sicherheitsüberwachungs- und -verwaltungsfunktion für die AWS Cloud-Einführung erreicht.
- **Simulierte Reaktionen auf Sicherheitsvorfälle** – Durch das Simulieren von Vorfällen können Sie überprüfen, ob die eingerichteten Kontrollen und Verfahren erwartungsgemäß reagieren. Mit dieser Methode können Sie ermitteln, ob die Wiederherstellung und Reaktion auf Vorfälle im Ernstfall wirkungsvoll funktioniert.
- **Forensik** – In den meisten Fällen werden Ihre bestehenden forensischen Werkzeuge in der AWS-Umgebung ausgeführt. Die Forensik-Teams profitieren von der regionsübergreifenden automatischen Bereitstellung von Tools und der Möglichkeit, große Datenvolumen schnell und reibungslos zu erfassen, indem sie die gleichen robusten, skalierbaren Services verwenden, auf denen die geschäftskritischen Anwendungen basieren, z. B. Amazon Simple Storage Service (S3), Amazon Elastic Block Store (EBS), Amazon Kinesis, Amazon DynamoDB, Amazon Relational Database Service (RDS), Amazon RedShift, und Amazon Elastic Compute Cloud (EC2).

Überlegungen

- **Aktualisieren** Sie Ihre Vorfallreaktionsprozesse, so dass die AWS-Umgebung erkannt wird.
- **Nutzen** Sie in AWS enthaltene Services, so dass Ihre Bereitstellungen durch Automatisierung und entsprechende Funktionsauswahl forensisch vorbereitet sind.
- **Automatisieren** Sie die Reaktionen, um Robustheit und die richtige Skalierung zu erreichen.

- **Nutzen** Sie Services in AWS zur Datensammlung und -analyse, um Untersuchungen zu unterstützen.
- **Überprüfen** Sie Ihre Vorfallreaktionsfunktionen durch Simulationen und Reaktionen auf Sicherheitsvorfälle.

Auf der Reise – Definieren einer Strategie

Überprüfen Sie Ihre aktuelle Sicherheitsstrategie, um zu ermitteln, ob bestimmte Teile der Strategie im Rahmen der Cloud-Einführung geändert werden sollten. Passen Sie Ihre Strategie zur Einführung der AWS-Cloud an die Risikostufe an, die Ihr Unternehmen zu akzeptieren bereit ist, an Ihre Methode zur Erfüllung von Behörden- und Compliance-Anforderungen sowie an Ihre Definitionen, welche Aspekte geschützt werden müssen und wie dieser Schutz erfolgt. Tabelle 1 gibt ein Beispiel einer Sicherheitsstrategie, bei der eine Reihe von Prinzipien formuliert sind, die dann bestimmten Initiativen und Arbeitsabläufen zugeordnet werden.

Prinzip	Beispielaktionen
Infrastruktur als Code.	Sicherheitsteam in Code und Automatisierung schulen; zu DevSecOps übergehen.
Leitlinien entwickeln, keine offenen Tore.	Richtiges Verhalten für Laufwerke definieren.
Die Cloud nutzen, um die Cloud zu schützen.	Sicherheits-Tools in der Cloud aufbauen, ausführen und verwalten.
Aktuell bleiben; sicher ausführen.	Neue Sicherheitsfunktionen nutzen; häufig patchen und ersetzen.
Abhängigkeit von ständigem Zugang verringern.	Rollenkatalog aufstellen; KMI über Secrets Service automatisieren.
Vollständige Sichtbarkeit.	AWS-Protokolle und Metadaten mit Betriebssystem- und Anwendungsprotokollen sammeln.
Tiefe Einblicke.	Ein Sicherheits-Data Warehouse mit BI und Analysen implementieren.
Skalierbare Vorfallreaktion (Incident Response, IR).	Standard-Betriebsverfahren (Standard Operating Procedure, SOP) für IR und Forensik für den gemeinsamen Verantwortungsrahmen aktualisieren.
Selbstreparatur.	Korrektur und Wiederherstellung auf bekannten guten Zustand automatisieren.

Tabelle 1: Beispiel-Sicherheitsstrategie

Während sich Ihre Strategie weiterentwickelt, können Sie mit der Iteration Ihrer Assurance Frameworks von Drittanbietern und der betrieblichen Sicherheitsanforderungen beginnen und ein Risikomanagement-System aufstellen, das Sie bei Ihrer Reise zu AWS anleitet. Es ist oft eine effektive Methode, Ihre Compliance-Zuordnung zu entwickeln, während Sie ein besseres Verständnis der Anforderungen Ihrer Arbeitslasten in der Cloud und der von AWS bereitgestellten Sicherheitsfunktionen erlangen.

Ein weiteres wichtiges Element Ihrer Strategie ist die Zuordnung des Modells der übergreifenden Verantwortlichkeit zu Ihrem Ökosystem. Zusätzlich zu der Makro-Beziehung, die Sie mit AWS verbindet, sollten Sie innerbetriebliche übergreifende Verantwortlichkeiten und solche untersuchen, die Sie an Ihre Geschäftspartner weitergeben wollen. Unternehmen können ihr Modell der übergreifenden Verantwortlichkeit in drei Hauptbereiche unterteilen: einen Kontrollrahmen; ein verantwortliches, zuständiges, beratenes, informiertes Modell (RACI); und ein Risikoregister. Der Kontrollrahmen beschreibt, wie die Sicherheitsaspekte des Unternehmens funktionieren sollen und welche Kontrollen für das Risikomanagement eingerichtet werden sollen. Sie können das RACI verwenden, um eine Person zu ermitteln und zu ernennen, die für die Kontrollen im Kontrollrahmen verantwortlich ist. Verwenden Sie ein Risikoregister, um Kontrollen ohne ordnungsgemäße Zuständigkeit zu erfassen. Priorisieren Sie die Restrisiken, die identifiziert wurden; gleichen Sie deren Behandlung mit den neu eingerichteten Arbeitsabläufen und Initiativen ab, um sie zu aufzuheben.

Während Sie diese übergreifenden Verantwortlichkeiten zuordnen, finden Sie wahrscheinlich neue Gelegenheiten, um Vorgänge zu automatisieren und den Workflow zwischen kritischen Teilnehmern in Ihrer Sicherheits-, Compliance- und Risikomanagement-Community zu verbessern. Abbildung 2 zeigt ein Beispiel für ein erweitertes Modell übergreifender Verantwortlichkeit.

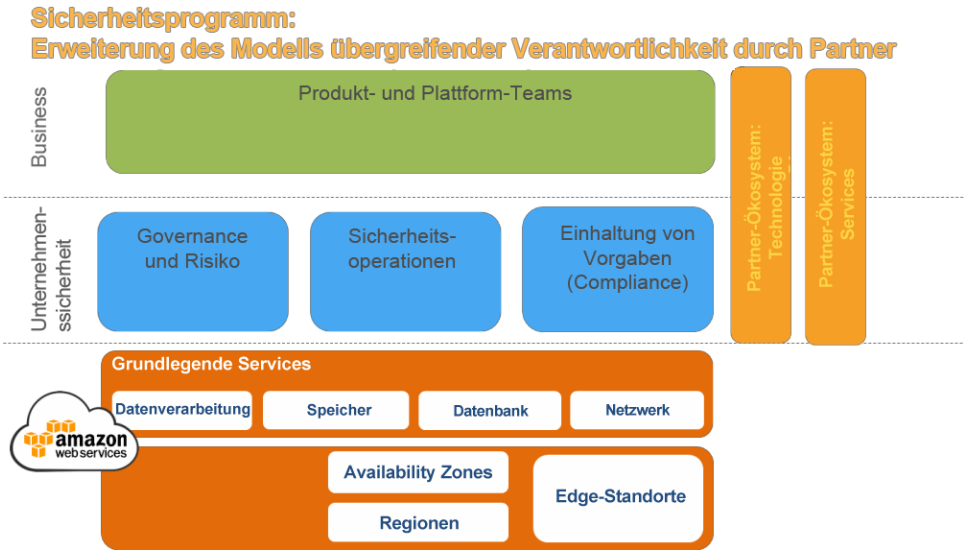

Abbildung 2: Beispiel für Modell übergreifender Verantwortlichkeit

Überlegungen

- **Erstellen** Sie eine maßgeschneiderte Strategie, die Ihrem Unternehmensansatz entspricht, Sicherheit in der Cloud zu implementieren.
- **Setzen** Sie in Ihrer gesamten Strategie so weit wie möglich automatisierte Funktionen ein.
- **Formulieren** Sie zuerst deutlich Ihren Ansatz für die Cloud.
- **Fördern** Sie Agilität und Flexibilität, indem Sie Leitlinien definieren.
- **Betrachten** Sie die Strategie als kurze Übung, die den Ansatz Ihrer Organisation für Informationssicherheit in der Cloud definiert.
- **Iterieren** Sie schnell, während Sie festlegen, was die Strategie ist. Ihr Ziel ist es, eine Reihe von Prinzipien zu haben, die den Kern der Bemühungen vorantreiben – die Strategie selbst ist nicht das Endziel. Gehen Sie schnell voran, und seien Sie bereit zum Anpassen und Weiterentwickeln.
- **Definieren** Sie strategische Prinzipien, die die Kultur vermitteln, die Sie bei der Sicherheit haben möchten und die über die von Ihnen getroffenen Konstruktionsentscheidungen informieren, und nicht eine Strategie, die spezifische Lösungen beinhaltet.

Auf der Reise – Bereitstellen eines Programms

Wenn die Strategie festgelegt ist, kann sie jetzt in die Praxis umgesetzt und die Implementierung initiiert werden, die Ihre Sicherheitsorganisation transformieren und die Reise in die Cloud absichern wird. Da Sie eine Bandbreite an Optionen und Funktionen zur Verfügung haben, sollte die Implementierung kein langwieriges Bemühen sein. Dieser Prozess der Entwicklung und Implementierung, wie verschiedene Funktionen zusammenarbeiten, stellt eine Gelegenheit dar, sich schnell mit dem System vertraut zu machen und zu lernen, wie Sie Ihre Entwicklungen so iterieren können, dass sie Ihre Anforderungen bestmöglich erfüllen. Lernen Sie frühzeitig aus der tatsächlichen Implementierung; nehmen Sie mit kleinen Änderungen Anpassungen und Weiterentwicklungen vor, während Sie lernen.

Abbildung 3: AWS CAF-Sicherheits-Epics

Zur Unterstützung bei der Implementierung können Sie die CAF-Sicherheits-Epics verwenden. (Siehe Abbildung 3.) Die Sicherheits-Epics bestehen aus einer Reihe von User-Storys (Anwendungsfälle und Missbrauchsfälle), die Sie während einzelner Sprints bearbeiten können. Jedes dieser Epics beinhaltet mehrere Iterationen, die immer komplexere Anforderungen behandeln und in der Robustheit abgestuft sind. Obwohl wir die Verwendung von Agile empfehlen, können die Epics auch als allgemeine Arbeitsabläufe oder Themen behandelt werden, die bei der Priorisierung und Strukturierung der Bereitstellung mit jedem anderen Rahmen helfen. Eine vorgeschlagene Struktur besteht aus den folgenden 10 Sicherheits-Epics (Abbildung 4), um Sie bei der Implementierung anzuleiten.

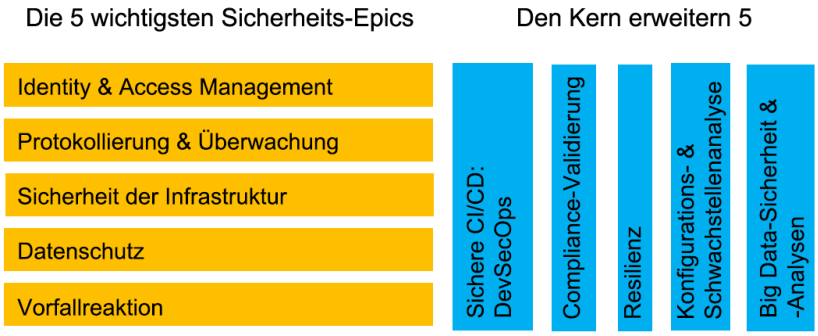

Abbildung 4: Zehn Sicherheits-Epics für AWS

Die wichtigsten Fünf

Die folgenden fünf Epics sind die wichtigsten Kontroll- und Funktionskategorien, die Sie frühzeitig berücksichtigen sollten, weil sie für den Beginn Ihrer Reise von grundlegender Bedeutung sind.

- **IAM** – AWS Identity and Access Management (IAM) bildet das Rückgrat Ihres AWS-Systems. In der Cloud müssen Sie ein Konto einrichten und über bestimmte Privilegien verfügen, bevor Sie Ressourcen bereitstellen oder zuteilen können. Typische Automatisierungsfunktionen sind beispielsweise die Zuordnung von Berechtigungen/Genehmigungen/Prüfungen, die Verwaltung geheimer Materialien, die Durchsetzung des Vier-Augen-Prinzips und des Prinzips der geringstmöglichen Zugriffsrechte, Just-in-Time-Privilegmanagement sowie die Verringerung der Abhängigkeit von langfristigen Anmeldeinformationen.
- **Protokollierung und Überwachung** – Die AWS-Services bieten eine Vielzahl von Protokollierungsdaten, mit denen Sie Ihre Interaktionen mit der Plattform überwachen können. Die Leistung der AWS-Services basiert auf Ihrer Konfigurationsauswahl und der Möglichkeit, Betriebssystem- und Anwendungsprotokolle einzubinden, um einen gemeinsamen Referenzrahmen zu erstellen. Typische Automatisierungsstorys sind Protokollaggregation, Schwellenwerte/Alarme/Benachrichtigungen, Anreicherung, Suchplattform, Visualisierung, Stakeholder-Zugriff sowie Workflow und Ticketing, um eine Unternehmensreaktion im geschlossenen Kreis zu initiieren.

- **Infrastruktursicherheit** – Wenn Sie Infrastruktur als Code betrachten, wird die Sicherheitsinfrastruktur zu einer Arbeitslast der ersten Stufe, die ebenfalls als Code bereitgestellt werden muss. Dieser Ansatz bietet Ihnen die Möglichkeit, AWS-Services programmatisch zu konfigurieren und Sicherheitsinfrastruktur von AWS Marketplace-Partnern oder selbst entwickelte Lösungen bereitzustellen. Typische Automatisierungsstorys sind beispielsweise das Erstellen benutzerdefinierter Vorlagen, um AWS-Services für die Erfüllung Ihrer Anforderungen zu konfigurieren, das Implementieren von Sicherheits-Architekturmustern und Sicherheits-Betriebsmaßnahmen als Code, das Erstellen benutzerdefinierter Sicherheitslösungen mithilfe von AWS-Services, die Verwendung von Patch-Managementstrategien wie Blau-/Grün-Bereitstellungen, die Verringerung ungeschützter Angriffsflächen und die Überprüfung der Wirksamkeit von Bereitstellungen.
- **Datenschutz** – Der Schutz wichtiger Daten ist ein kritisches Element beim Aufbau und Betrieb von Informationssystemen. AWS bietet Services und Funktionen, die Ihnen robuste Optionen zum Schutz Ihrer Daten über den gesamten Lebenszyklus an die Hand geben. Typische Automatisierungsstorys sind beispielsweise das Treffen von Entscheidungen zur Arbeitslastverteilung, das Implementieren eines Tagging-Schemas, das Erstellen von Mechanismen zum Schutz von übertragenen Daten wie VPN- und TLS/SSL-Verbindungen (einschließlich AWS Certificate Manager), das Erstellen von Mechanismen zum Schutz von Daten im Ruhezustand durch Verschlüsselung auf geeigneten Stufen in Ihrer Infrastruktur, die Implementierung/Integration mithilfe von AWS Key Management Service (AWS KMS), die Bereitstellung von AWS CloudHSM, das Erstellen von Plänen zur Aufgliederung in Token sowie das Implementieren und Ausführen von AWS Marketplace-Partnerlösungen.
- **Vorfallreaktion** – Die Automatisierung bestimmter Aspekte Ihres Vorfallmanagements verbessert die Zuverlässigkeit und erhöht die Reaktionsgeschwindigkeit. Oft generiert sie auch eine Umgebung, auf die bei nachträglichen Auswertungen leichter zugegriffen werden kann. Typische Automatisierungsstorys sind beispielsweise die Nutzung der AWS Lambda-Funktion „Responders“, die auf bestimmte Änderungen in der Umgebung reagiert, die Orchestrierung von automatischen Skalierungsereignissen, die Isolierung verdächtiger Systemkomponenten, die Bereitstellung investigativer Just-in-Time-Tools sowie das Erstellen von Workflows und Ticketing, um eine Unternehmensreaktion im geschlossenen Kreis zu beenden und daraus zu lernen.

Den Kern erweitern

Diese fünf Aspekte repräsentieren die Themen, mit denen sich durch Verfügbarkeit, Automatisierung und Prüfungen eine kontinuierlich exzellente Leistung erreichen lässt. Integrieren Sie diese Aspekte mit Bedacht in jeden Sprint. Wenn eine zusätzliche Vertiefung erforderlich ist, können Sie sie als eigene Epics behandeln.

- **Resilienz** – Hohe Verfügbarkeit, Betriebskontinuität, Robustheit und Resilienz sowie Notfallwiederherstellung sind häufige Gründe für Cloud-Bereitstellungen mithilfe von AWS. Typische Automatisierungsstorys sind beispielsweise die Verwendung von Multi-AZ- und Multi-Region-Bereitstellungen, das Verändern der verfügbaren Angriffsfläche, das Skalieren und Verschieben der **Zuordnung** von Ressourcen, um Angriffe zu absorbieren, der Schutz gefährdeter Ressourcen und das absichtliche Herbeiführen eines Ressourcenausfalls, um die Kontinuität der Systemfunktionen zu überprüfen.
- **Compliance-Validierung** – Wenn Sie Compliance umfassend in Ihr Sicherheitsprogramm integrieren, verhindern Sie dadurch, dass Compliance auf das Aktivieren eines Kontrollkästchens oder ein Overlay reduziert wird, das nach der Bereitstellung erfolgt. Dieses Epic behandelt die Plattform, die die Compliance-Artefakte zusammenfasst und rationalisiert, die durch die anderen Epics erzeugt wurden. Typische Automatisierungsstorys sind beispielsweise das Erstellen von Sicherheitseinheit-Tests, die bestimmten Compliance-Anforderungen zugeordnet sind, das Entwickeln von Services und Arbeitslasten zur Unterstützung der Compliance-Beweissammlung, das Erstellen von Compliance-Benachrichtigungs- und Visualisierungs-Pipelines aus Beweisfunktionen, ständige Überwachung sowie das Erstellen von DevSecOps-Teams, die auf die Bearbeitung von Compliance-Funktionen ausgerichtet sind.
- **Sichere CI/CD (DevSecOps)** – Durch eine Software-Versorgungskette, die sich durch den Einsatz vertrauenswürdiger und geprüfter Tool-Chains zur fortlaufenden Integration und Bereitstellung auszeichnet, lassen sich während der Migration zur Cloud ausgereifte Sicherheitsfunktionen erreichen. Typische Automatisierungsstorys sind beispielsweise das Härten und Patchen der Tool-Chain, Zugriff auf die Tool-Chain mit geringstmöglichen Zugriffsrechten, Protokollieren und Überwachen des Produktionsprozesses, Sicherheitsintegration/Bereitstellungsvisualisierung und Überprüfen der Code-Integrität.

- **Konfigurations- und Schwachstellenanalyse** – Die Konfigurations- und Schwachstellenanalyse wird in hohem Maß durch den Umfang, die Agilität und die Automatisierung unterstützt, die von AWS bereitgestellt werden. Typische Automatisierungsstorys sind beispielsweise das Aktivieren von AWS Config und das Erstellen kundenspezifischer AWS Config-Regeln, die Verwendung von Amazon CloudWatch-Ereignissen und AWS Lambda, um auf Änderungserkennung zu reagieren, das Implementieren von Amazon Inspector, die Auswahl und Bereitstellung kontinuierlicher Überwachungslösungen aus dem AWS Marketplace, die Bereitstellung ausgelöster Scans und das Einbetten von Bewertungs-Tools in die CI/CD-Tool-Chains.
- **Sicherheits-Big Data und Predictive Analytics** – Sicherheitsoperationen profitieren von Big Data-Services und -lösungen ebenso wie alle anderen Aspekte des Unternehmens. Die Nutzung von Big Data erlaubt Ihnen tiefere Einblicke in kürzerer Zeit, verbessert somit Ihre Agilität und die Fähigkeit, angemessen auf Ihre Sicherheitslage zu iterieren. Typische Automatisierungsstorys sind beispielsweise das Erstellen von Sicherheits-Datenseen, das Entwickeln von Analyse-Pipelines, das Erstellen von Visualisierungen zur Förderung der Entscheidungsfindung bei der Sicherheit sowie das Erstellen von Feedback-Mechanismen für autonome Reaktionen.

Nachdem diese Struktur definiert ist, kann ein Implementierungsplan entwickelt werden. Die Funktionen ändern sich mit der Zeit, und Verbesserungsmöglichkeiten werden kontinuierlich erfasst. Zur Erinnerung: Die oben beschriebenen Themen oder Funktionskategorien können als Epics einer agilen Methodik behandelt werden, die eine Reihe von User-Storys enthalten, die sowohl Anwendungsfälle als auch Missbrauchsfälle beschreiben. Mehrere Sprints führen zu einer höheren Reife, wobei die Flexibilität erhalten bleibt, sich an das geschäftliche Tempo und die Nachfrage anzupassen.

Beispiel-Sprintserie

Ziehen Sie in Erwägung, eine Probesequenz von sechs zweiwöchigen Sprints zu organisieren (eine Gruppe von Epics, die über ein zwölfwöchiges Kalendervierteljahr durchgeführt werden), einschließlich einer kurzen Vorbereitungszeit, und die Sequenz folgendermaßen durchzuführen. Ihr Ansatz hängt ab von der Ressourcenverfügbarkeit, Priorität und der gewünschten Reifestufe bei den einzelnen Fähigkeiten, während Sie sich Ihrer minimal realisierbaren Produktionsfähigkeit (MVP) nähern.

- **Sprint 0** – Sicherheitskartographie: Compliance-Zuordnung, Richtlinien-Zuordnung, anfängliche Bedrohungsmodellprüfung, Erstellung des Risikoregisters; Aufbau eines Bestands an Nutzungs- und Missbrauchsfällen; Planen der Sicherheits-Epics
- **Sprint 1** – IAM; Protokollierung und Überwachung
- **Sprint 2** – IAM; Protokollierung und Überwachung; Infrastrukturschutz
- **Sprint 3** – IAM; Protokollierung und Überwachung; Infrastrukturschutz
- **Sprint 4** – IAM; Protokollierung und Überwachung; Infrastrukturschutz; Datenschutz
- **Sprint 5** – Datenschutz, Automatisierung von Sicherheitsoperationen, Vorfallreaktionsplanung/Tooling; Resilienz
- **Sprint 6** – Automatisierung der Sicherheitsoperationen, Vorfallreaktion; Resilienz

Ein wichtiges Element bei der Compliance-Validierung besteht darin, die Validierung durch Sicherheits- und Compliance-Testfälle in jeden Sprint zu integrieren und anschließend in den Produktionsprozess einzubinden. Wenn eine Compliance-Validierungsfunktion ausdrücklich erforderlich ist, können die Sprints so eingerichtet werden, dass sie sich speziell auf diese User-Storys beziehen. Im Laufe der Zeit kann mit Iteration eine kontinuierliche Validierung eingerichtet und nötigenfalls eine Autokorrektur für Abweichungen implementiert werden.

Der Gesamtansatz zielt darauf ab, klar zu definieren, was eine MVP oder Baseline ist, die anschließend dem ersten Sprint in jedem Bereich zugeordnet wird. In den Anfangsstadien muss das Endziel noch nicht klar definiert sein, aber es wird eine deutliche Roadmap für die ersten Sprints erstellt. Mit Timing, Erfahrung und Iteration wird der Endzustand verfeinert und angepasst, bis er für Ihre Organisation genau richtig ist. In der Praxis kann sich der Endzustand ständig verschieben, aber letztendlich führt der Prozess zu kontinuierlicher Verbesserung bei höherem Tempo. Dieser Ansatz kann effektiver sein und größere Kosteneinsparungen bewirken als ein „Big-Bang-Ansatz“, der lange Zeitvorgaben und hohe Kapitalaufwendungen voraussetzt.

Genauer betrachtet kann der erste Sprint für IAM daraus bestehen, die Kontostruktur zu definieren und die wichtigsten bewährten Methoden zu implementieren. Bei einem zweiten Sprint kann der Verbund implementiert werden. Bei einem dritten Sprint kann die Kontenverwaltung zur Aufnahme mehrerer Konten erweitert werden, usw. IAM-User-Storys, die eine oder mehrere dieser anfänglichen Taten umfassen, könnten Storys wie die folgenden enthalten:

„Als Zugriffsadministrator will ich eine anfängliche Anzahl an Benutzern zum Verwalten von privilegierten Zugriffen und vertrauenswürdige Beziehungen mit dem Verbund-Identitätsanbieter erstellen.”

„Als Zugriffsadministrator will ich Benutzern in meinem bestehenden Unternehmensverzeichnis Funktionsrollen oder Zugriffsberechtigungen auf der AWS-Plattform zuordnen.“

„Als Zugriffsadministrator will ich Multi-Factor Authentication bei allen Interaktionen interaktiver Benutzer mit der AWS-Konsole durchsetzen.“

In diesem Beispiel können die folgenden User-Storys zu Protokollierung und Überwachung eine oder mehrere anfängliche Sprints umfassen:

„Als Analyst für Sicherheitsoperationen will ich eine Protokollierung auf Plattformebene für alle AWS-Regionen und AWS-Konten erhalten.“

„Als Analyst für Sicherheitsoperationen will ich, dass alle Protokolle auf Plattformebene von allen AWS-Regionen und -Konten an einem gemeinsamen Ort bereitgestellt werden.”

„Als Analyst für Sicherheitsoperationen will ich Benachrichtigungen bei jedem Vorgang erhalten, der Benutzern, Gruppen oder Rollen IAM-Richtlinien zuordnet.“

Sie können die Funktionen parallel oder seriell aufbauen und die Flexibilität aufrechterhalten, indem Sie User-Storys zu Sicherheitsfunktionen in den Gesamt-Produktionsbestand aufnehmen. Sie können die User-Storys auch zu einem auf Sicherheit fokussierten DevOps-Team auslagern. Sie können diese Entscheidungen regelmäßig überprüfen; so können Sie Ihre Bereitstellung im Laufe der Zeit genau an die Bedürfnisse der Organisation anpassen.

Überlegungen

- **Überprüfen** Sie Ihren bestehenden Kontrollrahmen, um zu ermitteln, wie die AWS-Services ausgeführt werden, damit sie die erforderlichen Sicherheitsstandards erfüllen.
- **Definieren** Sie Teilnehmer, und erstellen Sie ein Storyboard mit ihrer Erfahrung bei der Interaktion mit AWS-Services.
- **Definieren** Sie, was der erste Sprint ist und was zu Anfang längerfristig das oberste Ziel sein soll.
- **Legen** Sie eine minimal realisierbare Sicherheits-Baseline fest, und stecken Sie das Ziel für die Arbeitslasten und Daten, die Sie schützen, immer wieder höher.

Auf der Reise – Entwickeln robuster Sicherheitsoperationen

In einer Umgebung, in der die Infrastruktur aus Code besteht, muss die Sicherheit auch als Code behandelt werden. Die Komponente „Sicherheitsoperationen“ stellt ein Mittel bereit, um die Grundlagen für die Sicherheit als Code zu kommunizieren und zu operationalisieren:

- Die Cloud nutzen, um die Cloud zu schützen.
- Die Sicherheitsinfrastruktur sollte die Cloud berücksichtigen.
- Stellen Sie Sicherheitsfunktionen über die API als Services bereit.
- Automatisieren Sie alles, so dass Sicherheit und Compliance skaliert werden können.

Um dieses Governance-Modell praktikabel zu machen, organisieren sich Geschäftsbereiche oft als DevOps-Teams, um Infrastruktur und Geschäftssoftware zu erstellen und bereitzustellen. Sie können die Kerngrundsätze des Governance-Modells erweitern, indem Sie Sicherheit in Ihre DevOps-Kultur oder -Praxis integrieren. Dies wird manchmal als DevSecOps bezeichnet. Stellen Sie ein Team nach den folgenden Prinzipien zusammen:

- Das Sicherheitsteam ist für DevOps-Kulturen und -Verhaltensweisen zuständig.
- Die Entwickler schreiben offen den Code, der zum Automatisieren von Sicherheitsoperationen verwendet wird.
- Das Sicherheitsoperationsteam ist berechtigt, sich am Testen und der Automatisierung des Anwendungscodes zu beteiligen.
- Der Ehrgeiz des Teams besteht darin, möglichst schnell und häufig Aktualisierungen bereitzustellen. Häufigere Bereitstellungen mit kleineren Änderungen verringern das Betriebsrisiko und zeugen von schnellem Fortschritt bei der Sicherheitsstrategie.

Die Teams für integrierte Entwicklung, Sicherheit und Operationen haben drei wichtige gemeinsame Missionen.

- Festigung der Tool-Chain für kontinuierliche Integration/Bereitstellung.
- Aktivierung und Förderung der Entwicklung resilienter Software, während sie die Tool-Chain durchläuft.
- Bereitstellung der gesamten Sicherheitsinfrastruktur und -software durch die Tool-Chain.

Die Ermittlung von Änderungen (falls nötig) an aktuellen Sicherheitspraktiken hilft Ihnen bei der Planung einer reibungslosen AWS-Einführungsstrategie.

Schlussfolgerung

Während Ihrer Akzeptanzphase von AWS müssen Sie Ihr Sicherheitssystem so aktualisieren, dass der AWS-Teil in der Umgebung berücksichtigt wird. Dieses Whitepaper zur Sicherheitsperspektive beschreibt eine Methode, wie Sie die Vorteile nutzen können, die AWS für Ihr Sicherheitssystem hat. Weitere Informationen zur Systemsicherheit sind auf der AWS-Website verfügbar, wo Sicherheitsfunktionen detailliert beschrieben sind und weitere Anleitungen für häufige Implementierungen gegeben werden. Dort gibt es auch eine umfassende Liste mit sicherheitsbezogenen Inhalten,[4] die verschiedene Mitglieder Ihres Sicherheitsteams durchsehen sollten, während Sie die AWS-Einführungsinitiativen vorbereiten.

Anhang A: Verfolgung des Fortschritts bei der AWS CAF-Sicherheitsperspektive

Sie können die wichtigsten Sicherheitsassistenten und das Fortschrittsmodell für Sicherheits-Epics, das in diesem Anhang behandelt wird, zum Messen des Fortschritts und der Reife Ihrer Implementierung der AWS CAF-Sicherheitsperspektive verwenden. Die Assistenten und das Fortschrittsmodell können zu Projektplanungszwecken, zum Bewerten der Robustheit von Implementierungen oder einfach als Mittel verwendet werden, das Gespräch über die durchzuführenden Schritte voranzubringen.

Wichtige Sicherheitsassistenten

Wichtige Sicherheitsassistenten sind Orientierungspunkte, die Ihnen dabei helfen, auf dem richtigen Weg zu bleiben. Wir verwenden ein Bewertungsmodell, das aus drei Werten besteht: Unbehandelt, in Bearbeitung und Abgeschlossen.

- Cloud-Sicherheitsstrategie [Unbehandelt, in Bearbeitung, Abgeschlossen]
- Stakeholder-Kommunikationsplan [Unbehandelt, in Bearbeitung, Abgeschlossen]
- Sicherheits-Kartographie [Unbehandelt, in Bearbeitung, Abgeschlossen]
- Dokumentation des Modells übergreifender Verantwortlichkeit [Unbehandelt, in Bearbeitung, Abgeschlossen]
- Playbook & Runbooks für Sicherheitsoperationen [Unbehandelt, in Bearbeitung, Abgeschlossen]
- Plan für Sicherheits-Epics [Unbehandelt, in Bearbeitung, Abgeschlossen]
- Sicherheitsvorfall-Reaktionssimulation [Unbehandelt, in Bearbeitung, Abgeschlossen]

Fortschrittsmodell für Sicherheits-Epics

Das Fortschrittsmodell für Sicherheits-Epics hilft Ihnen, Ihren Fortschritt bei der Implementierung der 10 in diesem Paper beschriebenen Sicherheits-Epics zu bewerten. Wir verwenden ein Bewertungsmodell von 0 (null) bis 3 zum Messen der Robustheit. Es sind Beispiele für die Epics des Identity and Access Management und der Protokollierung und Überwachung enthalten, damit Sie sehen können, wie dieser Fortschritt funktioniert.

Die 5 wichtigsten

Sicherheits-Epics

0- Nicht behandelt

1- Bei Architektur und Plänen behandelt

2- Minimal realisierbare Implementierung

3- Unternehmensgerechte Produktionsimplementierung

Sicherheits-Epic	0	1	2	3
Identitäts- und Zugriffsverwaltung	Beispiel: Keine Beziehung zwischen lokalen und AWS-Identitäten.	Beispiel: Eine Methode für das Identitätsmanagement des Belegschaft-Lebenszyklus wird definiert. Die IAM-Architektur wird dokumentiert. Job-Funktionen werden den IAM-Richtlinienanforderungen zugeordnet.	Beispiel: IAM implementiert, wie in der Architektur definiert. Es sind IAM-Richtlinien implementiert, die einigen Job-Funktionen zugeordnet sind. IAM-Implementierung überprüft.	Beispiel: Automatisierung von IAM-Lebenszyklus-Workflows.
Protokollieren und Überwachen	Beispiel: Keine Nutzung von durch AWS bereitgestellten Protokollierungs- und Überwachungslösungen.	Beispiel: Eine Methode für die Protokollaggregation, Überwachung und Integration in Sicherheitsereignis-Verwaltungsprozesse wird definiert.	Beispiel: Protokollierung auf Plattformebene und Serviceebene wird aktiviert und zentralisiert.	Beispiel: Ereignisse mit Auswirkungen auf die Sicherheit werden tief in den Sicherheits-Workflow und die Vorfallmanagementprozesse und -systeme integriert.
Sicherheit der Infrastruktur				
Datenschutz				
Vorfall-management				

Den Kern erweitern 5

0- Nicht behandelt

1- Bei Architektur und Plänen behandelt

2- Minimal realisierbare Implementierung

3- Unternehmensgerechte Produktionsimplementierung

Sicherheits-Epic	0	1	2	3
Resilienz				
DevSecOps				
Compliance-Validierung				
Konfigurations- und Schwachstellen-management				
Big Data-Sicherheit				

CAF-Klassifizierung und -Begriffe

Das Cloud Adoption Framework (CAF) ist der Bezugsrahmen, den AWS erstellt hat, um Anleitungen und bewährte Methoden aus früheren Kundenprojekten zu erfassen. Eine AWS CAF-*Perspektive* stellt einen Schwerpunktbereich dar, der für die Implementierung cloudbasierter IT-Systeme in Organisationen relevant ist. Die Sicherheitsperspektive stellt beispielsweise Anleitungen und Verfahren zum Bewerten und Verbessern Ihrer bestehenden Sicherheitskontrollen bereit, während Sie auf die AWS-Umgebung umstellen.

Jede CAF-Perspektive besteht aus Komponenten und Aktivitäten. Eine *Komponente* ist ein Unterbereich einer Perspektive, die einen bestimmten Aspekt darstellt, der berücksichtigt werden muss. Dieses Whitepaper untersucht die Komponenten der Sicherheitsperspektive. Eine *Aktivität* gibt Anleitungen zum Erstellen umsetzbarer Pläne, die die Organisation nutzen kann, um zur Cloud zu migrieren und cloudbasierte Lösungen kontinuierlich auszuführen.

Beispielsweise ist die *Direktive* Komponente Bestandteil der Sicherheitsperspektive; die Anpassung eines AWS-Modells übergreifender Verantwortlichkeit an Ihr Ökosystem kann eine Aktivität innerhalb dieser Komponente sein.

Wenn sie kombiniert werden, können das Cloud Adoption Framework (CAF) und die Cloud Adoption Methodology (CAM) als Anleitung für Ihre Reise in die AWS-Cloud verwendet werden.

Hinweise

[1] https://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

[2] https://aws.amazon.com/compliance/

[3] https://aws.amazon.com/compliance/shared-responsibility-model/

[4] https://aws.amazon.com/security/security-resources/