Implementación de Políticas de Seguridad en la Nube utilizando AWS

Mario Camacho

Sergio de la Coba

Diego González

Fundamentos de la Computación en la Nube

ÍNDICE

3. ¿Cómo implementarías políticas de seguridad en la nube?

Es esencial establecer políticas de seguridad en la nube para asegurar la integridad, privacidad y disponibilidad de los datos y recursos de una entidad. AWS proporciona una gama de herramientas y servicios que facilitan la implementación de medidas de seguridad sólidas. A continuación, se detallan las tácticas y soluciones que se pueden utilizar para asegurar un ambiente seguro en AWS.

4. Evaluación de Riesgos de AWS

Antes de implementar cualquier política de seguridad, es crucial realizar una evaluación de riesgos para identificar posibles vulnerabilidades y amenazas que puedan afectar la infraestructura en la nube. La evaluación de riesgos implica varios pasos esenciales:

1. Reconocimiento de Activos: Establecer qué recursos se encuentran en AWS, que incluyen bases de datos, servidores, aplicaciones y espacio de almacenamiento.
2. Evaluación de Protecciones: Analizar las potenciales amenazas tanto internas como externas, tales como ataques de malware, intrusiones no permitidas o fallos en la configuración.
3. Análisis de Debilidades: Utilización de instrumentos como Amazon Inspector para identificar fallos en configuraciones de seguridad y aplicaciones.
4. Clasificación del Riesgo: Priorización de amenazas con base en su impacto potencial y probabilidad de ocurrencia.

Herramientas recomendadas en AWS

- AWS Security Hub: Consolida y gestiona hallazgos de seguridad de diferentes servicios en AWS, proporcionando una visión centralizada de la postura de seguridad.

- Amazon Inspector: Escanea instancias EC2 y contenedores para detectar vulnerabilidades y configuraciones débiles.

- AWS Trusted Advisor: Proporciona recomendaciones sobre seguridad, rendimiento, optimización de costos y mejoras en la infraestructura de AWS.

- AWS GuardDuty: Monitorea continuamente la actividad en la cuenta de AWS para detectar comportamientos sospechosos.

- AWS Config: Ayuda a rastrear cambios en configuraciones y detectar desviaciones de las mejores prácticas de seguridad.

5. Control de Acceso

El control de acceso es un componente esencial para garantizar que solo las personas autorizadas puedan acceder a los recursos en AWS. Un mal control de accesos puede resultar en brechas de seguridad y accesos no autorizados. Las principales estrategias de control de acceso son:

1. Principio de Menor Privilegio: Asignar los permisos mínimos necesarios para que un usuario o servicio ejecute sus funciones.
2. Uso de IAM (Identity and Access Management): Crear usuarios, grupos y roles con permisos bien definidos.
3. Autenticación Multifactor (MFA): Obligar el uso de MFA para todas las cuentas con privilegios elevados.
4. AWS Organizations y SCPs (Service Control Policies): Implementar restricciones a nivel de organización para limitar acciones no deseadas.
5. AWS SSO (Single Sign-On): Gestionar accesos centralizados para usuarios en diferentes aplicaciones.

Herramientas recomendadas en AWS

- AWS IAM: Administra usuarios, grupos, roles y permisos.

- AWS IAM Access Analyzer: Identifica permisos excesivos o accesos no intencionados.

- AWS CloudTrail: Registra todas las actividades relacionadas con IAM y accesos.

- AWS Organizations & SCPs: Aplica políticas de control a nivel organizacional.

- AWS SSO: Gestiona accesos de manera centralizada.

- AWS Secrets Manager: Protege y administra credenciales de acceso a bases de datos y servicios.

- AWS Security Hub: Centraliza información de seguridad, incluyendo alertas de IAM.

6. Protección de Datos

Proteger los datos almacenados en AWS es fundamental para garantizar la confidencialidad y prevenir fugas de información. La mejor estrategias para proteger los datos en AWS:

1. Cifrado de datos en reposo: Utilizar AWS Key Management Service (KMS) para cifrar datos en Amazon S3, RDS, DynamoDB, EBS y Redshift.

   El cifrado de datos consiste en proteger los datos mediante técnicas de cifrado. Con KMS se pueden cifrar datos utilizando claves gestionadas por el propio AWS y también personalizadas, de esta forma nos aseguramos que los datos sean indescifrables en caso de no disponer de las claves adecuadas.

2. Cifrado de datos en tránsito: Implementar SSL/TLS para la transmisión segura de información.

   El cifrado de datos en tránsito se dedica a proteger los datos mientras circula y se transmite entre los clientes y los servidores de AWS. En esta tarea implementa Secure Sockets Layer / Transport Layer Security para garantizar que los datos no son obtenidos ni manipulados por terceros durante la transmisión entre los servidores y los usuarios. Al activar HTTPS, se garantiza que las comunicaciones entre los clientes y los servidores estén cifradas, protegiendo la privacidad y la integridad de los datos. Este cifrado es crucial para evitar ataques de intermediarios o "man-in-the-middle".

3. Protección contra fugas de datos: Uso de Amazon Macie para detectar información sensible.

   La protección contra fugas de datos significa asegurarse de que información sensible no sea compartida o expuesta sin querer. Amazon Macie es una herramienta de AWS que usa inteligencia artificial para encontrar datos importantes (como números de tarjetas de crédito o información personal) guardados en Amazon S3. Macie revisa automáticamente estos datos y avisa si detecta que algo puede estar en riesgo de ser filtrado. Por ejemplo, si alguien accede a datos sin permiso o si se almacenan archivos de forma incorrecta, Macie lo detecta y avisa, ayudando a prevenir que esta información se difunda sin nuestro consentimiento.

4. Copias de seguridad y recuperación: Implementación de AWS Backup para garantizar la disponibilidad de la información.

   Las copias de seguridad y recuperaciones nos garantizan que durante todos los procesos no se pierdan datos en caso de que haya algún error. AWS backup ofrece un servicio de copias de seguridad de forma automática, como EBS, RDS o DynamoDB. También se ofrece un servicio en el que puedes configurar copias de seguridad periódicas, de manera que siempre tengas una versión actualizada de los datos.

Herramientas recomendadas basadas en la protección de datos en AWS

- AWS KMS (Key Management Service): Promueve la administración de claves de encriptación para salvaguardar los datos en almacenamiento, garantizando que únicamente usuarios con autorización tengan acceso a los datos guardados en servicios como S3, RDS y EBS.

- AWS Certificate Manager (ACM): Gestión de certificados SSL/TLS, facilitando la encriptación de datos en movimiento y asegurando conexiones seguras entre clientes y servidores en AWS.

- Macie Amazon: Emplea inteligencia artificial para detectar información delicada guardada en Amazon S3, contribuyendo a evitar pérdidas de datos y a acatar regulaciones de seguridad.

- AWS Backup: Ofrece un servicio automatizado de respaldos para diversos servicios de AWS, garantizando la recuperación de datos en situaciones de errores o pérdidas involuntarias.

- AWS CloudTrail: Registra y verifica todas las acciones y accesos a la información en AWS, lo que permite identificar acciones ilegítimas o no permitidas en la infraestructura.

- Amazon S3 Object Lock: Evita alteraciones o supresión no permitidas en objetos guardados en S3, garantizando la integridad y la disponibilidad de los datos.

7. Monitoreo y Respuesta

El monitoreo continuo y la respuesta a incidentes son esenciales para detectar actividades sospechosas y mitigar riesgos. Las mejores estrategias de monitoreo:

1. Registro de eventos: Uso de AWS CloudTrail para rastrear acciones en la cuenta.

   El registro de eventos es una forma de seguir lo que sucede en tu cuenta de AWS. AWS CloudTrail es una herramienta que te permite registrar todas las acciones realizadas en tu cuenta, como quién accedió a qué recursos y qué cambios se hicieron. Esto es útil para tener un historial detallado de lo que está pasando, lo que te ayuda a identificar actividades sospechosas o no autorizadas. Con CloudTrail, puedes revisar los eventos pasados, asegurarte de que se cumplan las políticas de seguridad y solucionar problemas si algo sale mal.

2. Monitoreo de recursos: Implementación de Amazon CloudWatch para analizar métricas y alertas.

   El monitoreo de recursos es una herramienta para ver cómo están funcionando los servicios y recursos en tu cuenta de AWS. Por otro lado Amazon CloudWatch es una herramienta que permite monitorear el rendimiento y funcionamiento de tus recursos dentro de la plataforma de AWS, como servidores o bases de datos. Con esta herramienta podemos ver información como el uso de memoria, tráfico de red etc. Además se pueden configurar alertas para que el sistema te avise en caso de un mal funcionamiento, errores o sobrecargas, de esta manera es más fácil para una empresa una rápida detección y solución de problemas.

   Esta herramienta te permite ver cómo están funcionando los servicios y recursos de tu cuenta de AWS

3. Detección de amenazas: Uso de AWS GuardDuty para análisis de comportamiento malicioso.

   La detección de amenazas hace referencia a detectar comportamientos sospechosos o malintencionados en tu cuenta de AWS. AWS GuardDuty es un servicio de seguridad que examina la conducta de tus recursos con el fin de identificar amenazas, tales como accesos no permitidos o acciones atípicas. GuardDuty emplea inteligencia artificial y aprendizaje automático para examinar registros de sucesos, tráfico en la red y conductas inusuales. Si identifica algún riesgo, como un potencial ataque o una infracción de seguridad, te informará de forma inmediata. Esto te permite responder con rapidez para salvaguardar tus datos y recursos de potenciales amenazas.

4. Automatización de respuestas: Implementar respuestas automáticas con AWS Lambda y AWS Systems Manager. La automatización de respuestas, como indica el nombre, permite que el sistema realice acciones de manera automática sin necesidad de intervención manual.

AWS Lambda permite ejecutar código automáticamente en respuesta a eventos, como un cambio en los datos o una alerta de seguridad. Por ejemplo, si se detecta un acceso no autorizado, Lambda puede ejecutar un script para bloquear ese acceso sin que tengas que hacerlo manualmente.

AWS Systems Manager facilita la automatización de tareas administrativas, como la actualización de software o la configuración de servidores, a través de automatizaciones. Se pueden programar respuestas automáticas a diversas situaciones, asegurando que las acciones se tomen rápidamente y de manera consistente.

Juntando todas estas herramientas es mucho más fácil mejorar la eficiencia y la seguridad, ya que se responde de manera inmediata y automática a situaciones de riesgo para el cliente o empresa.

Herramientas recomendadas en AWS

- Amazon CloudWatch: Administra los registros y métricas de los servicios en AWS, ofreciendo alertas y paneles de control en tiempo real para identificar irregularidades en el desempeño y la seguridad.

- CloudTrail de AWS: Logra sucesos y operaciones en la cuenta de AWS, facilitando la auditoría y seguimiento de accesos y cambios en los recursos.

- AWS GuardDuty: Examina los registros y el tráfico de red para detectar conductas malintencionadas, intentos de acceso no permitidos y posibles amenazas en la infraestructura de AWS.

- Amazon Lambda: Facilita la realización de acciones automatizadas frente a sucesos de seguridad, como desactivar cuentas comprometidas o bloquear direcciones IP poco confiables sin necesidad de intervención humana.

- AWS Systems Manager: Promueve la automatización y administración de incidentes en AWS, posibilitando la implementación de actualizaciones, la realización de órdenes a distancia y la monitorización de recursos en diversos servicios.

8. Cumplimiento y Normativas

AWS proporciona herramientas que ayudan a cumplir con normativas como ISO 27001, PCI DSS, HIPAA, SOC 2, entre otras. Las mejores estrategias de cumplimiento son:

1. Automatizar auditorías: El AWS Audit Manager simplifica la automatización de las auditorías de cumplimiento, posibilitando la ejecución de revisiones constantes y la elaboración de informes exhaustivos sobre la observancia de las regulaciones. Esta herramienta facilita la identificación de áreas de mejora y garantiza que los controles internos se ajusten a las prácticas y normativas óptimas.
2. Revisión de configuraciones: AWS Config facilita el seguimiento y la revisión constante de las configuraciones de recursos en la cuenta de AWS. Esta herramienta contribuye a asegurar la correcta configuración de los recursos y su cumplimiento con las políticas de seguridad y cumplimiento, facilitando la detección de desviaciones y la implementación de acciones correctivas en tiempo real.
3. Generación de reportes: AWS Artifact ofrece acceso a documentos e informes relacionados con las certificaciones de cumplimiento de AWS. Esto abarca revisiones y valoraciones externas acerca de los sistemas de seguridad puestos en marcha en la infraestructura de AWS. Los reportes producidos por AWS Artifact permiten a las entidades evidenciar el acatamiento de regulaciones y compartir datos con auditores externos.

Herramientas recomendadas en AWS

- AWS Audit Manager: Promueve la automatización de auditorías y revisiones de cumplimiento, posibilitando la ejecución de auditorías constantes y la elaboración de informes exhaustivos que contribuyen a asegurar que las políticas de cumplimiento se mantengan al día.

- AWS Config: Vigila y garantiza que las configuraciones de recursos en AWS se ajusten a las políticas y estándares de seguridad fijados, lo que permite identificar desviaciones y rectificarlas de forma eficaz.

- AWS Artifact: Ofrece acceso a informes y documentación exhaustiva acerca de las certificaciones de cumplimiento de AWS, lo que posibilita a las entidades evidenciar su cumplimiento con las regulaciones y simplificar auditorías externas.

9. Capacitación del Personal

La capacitación del personal es esencial para evitar fallos humanos y optimizar la administración de riesgos en la infraestructura de AWS. Un equipo adecuadamente capacitado puede detectar y atenuar con rapidez incidentes de seguridad, salvaguardando los datos y sistemas de la compañía. Existen algunas tácticas de formación del personal, las cuales mencionaré a continuación, son las más destacadas y reconocidas:

1. Programas de Formación con AWS Training and Certification: Cursos como el AWS Certified Security – Specialty y el AWS Certified Solutions Architect contribuyen a que los trabajadores obtengan habilidades avanzadas en seguridad y administración de la nube.
2. Simulaciones de Ataques y Ejercicios de Respuesta a Incidentes:Actividades prácticas, tales como simulaciones de ataques DDoS, intrusiones o fugas de datos, facilitan a los trabajadores la práctica de la reacción frente a circunstancias reales y potencian la capacidad de resistencia de la infraestructura.
3. Concienciación sobre Amenazas como Phishing y Malware: Se instruye al personal en la detección y prevención de ataques de phishing y malware, a través de capacitación práctica y ejercicios de simulación para fortalecer la seguridad.

Estas capacitaciones nombradas dan unos beneficios y yo he destacado estos 3, ya que pienso que son los más importantes:

- Reducción de Errores Humanos: Minimiza los fallos de configuración y exposición accidental de datos.

- Mejora de la Respuesta ante Incidentes: Facilita una reacción rápida y efectiva ante ataques.

- Cultura de Seguridad: Fomenta un ambiente organizacional centrado en la protección de los activos digitales.

10. Revisión y Mejora Continua

La seguridad en AWS debe ser un proceso continuo, con políticas que se revisen y actualicen regularmente para mantenerse alineadas con las amenazas emergentes. Para lograr una mejora continua, es fundamental seguir estas buenas prácticas:

1. Auditorías Periódicas con AWS Security Hub: Realizar auditorías frecuentes utilizando AWS Security Hub para detectar configuraciones incorrectas, vulnerabilidades y brechas de seguridad en la infraestructura. Esto asegura que las políticas de seguridad se mantengan actualizadas y se cumplan adecuadamente.

2. Evaluación de Vulnerabilidades con Amazon Inspector: Utilizar Amazon Inspector para llevar a cabo evaluaciones automáticas de seguridad, identificando vulnerabilidades en las aplicaciones y sistemas. Este proceso ayuda a detectar fallos antes de que puedan ser explotados, permitiendo una respuesta rápida y medidas correctivas oportunas.

3. Aplicación de Parches de Seguridad: Aplicar de forma regular parches de seguridad tanto en sistemas operativos como en aplicaciones es crucial para evitar que atacantes exploten vulnerabilidades conocidas. La actualización constante de estos parches garantiza que la infraestructura esté protegida contra amenazas emergentes.

Los beneficios de la revisión y mejora continua que he encontrado son:

- Identificación Temprana de Vulnerabilidades: Las auditorías y evaluaciones periódicas ayudan a detectar fallos y amenazas antes de que puedan ser explotadas.

- Cumplimiento de Normativas: Asegura que la infraestructura cumpla con los estándares de seguridad y regulaciones locales e internacionales.

- Mitigación de Riesgos: La aplicación regular de parches reduce la probabilidad de que un atacante explote vulnerabilidades conocidas.