Polo del Conocimiento

Pol. Con. (Edición núm. 102) Vol. 10, No 1
Enero 2025, pp. 2200-2217
ISSN: 2550 - 682X
DOI: https://doi.org/10.23857/pc.v10i1.8805

Análisis de seguridad en arquitecturas serverless en la nube

Security analysis in serverless architectures in the cloud

Análise de segurança em arquiteturas serverless na cloud

Fausto Raúl Orozco-Lara [I]
fausto.orozcol@ug.edu.ec
https://orcid.org/0000-0003-4872-3702

Mariela Paola Espinoza-Martinez [II]
mariela.espinozam@ug.edu.ec
https://orcid.org/0000-0003-3677-019X

Mariuxi Lizbeth Balanzátegui-Vinces [III]
mariuxi.balanzateguiv@ug.edu.ec
https://orcid.org/0009-0004-8494-0143

Valeria Emily Castillo-Sánchez [IV]
valeria.castillos@ug.edu.ec
https://orcid.org/0009-0007-3962-918X

Correspondencia: fausto.orozcol@ug.edu.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

*** Recibido:** 07 de noviembre de 2024 ***Aceptado:** 26 de diciembre de 2024 *** Publicado:** 23 de enero de 2025

I. Universidad de Guayaquil, Guayaquil, Ecuador.
II. Universidad de Guayaquil, Guayaquil, Ecuador.
III. Universidad de Guayaquil, Guayaquil, Ecuador.
IV. Universidad de Guayaquil, Guayaquil, Ecuador.

Resumen

Este articulo surge como producto final del trabajo de titulación que tiene como tema Análisis de seguridad en arquitecturas serverless en la nube y estrategias para la mitigación de riesgos el objetivo de la investigación; el análisis de seguridad en arquitecturas serveless en la nube, particularmente en la plataforma como Amazon Web Services (AWS) y conlleva la valoración de riesgos y vulnerabilidades propias de este modelo. En arquitecturas serverless, los usuarios no administran directamente los servidores, lo cual puede incrementar la eficacia y disminuir gastos, pero también plantea nuevos desafíos de seguridad. Entre los riesgos más relevantes se encuentran la susceptibilidad a ataques como inyección de código, la escalabilidad de funciones y problemas de acceso no autorizado a datos a través de interfaces configuradas de manera incorrecta. Como oferta de servicios en la nube, AWS ofrece instrumentos como AWS Lambda, API Gateway e IAM (Administración de Identidad y Acceso) para gestionar la seguridad.

La comparación de los tres escenarios permite comprobar que, en un entorno de arquitecturas de tipo serverless, la amenaza con mayor impacto en el mismo es la segunda, lo que es muy preocupante, indica la evasión de validaciones del cliente, la escalada de privilegios y la exfiltración de secretos, lo que indica que estas amenazas afectan a la autenticación, a la gestión de accesos y a la seguridad de credenciales para llevar a cabo ataques más complejos.

Palabras claves: Arquitectura serverless; riesgos de seguridad; gestión de claves; superficie de ataque; configuración insegura e inyección de datos.

Abstract

This article arises as a final product of the thesis whose topic is Security analysis in serverless architectures in the cloud and strategies for risk mitigation. The objective of the research is the security analysis in serverless architectures in the cloud, particularly in the platform such as Amazon Web Services (AWS) and involves the assessment of risks and vulnerabilities inherent to this model. In serverless architectures, users do not directly manage the servers, which can increase efficiency and reduce costs, but also poses new security challenges. Among the most relevant risks are susceptibility to attacks such as code injection, function scalability, and problems of unauthorized access to data through incorrectly configured interfaces. As a cloud service offering, AWS offers tools such as AWS Lambda, API Gateway, and IAM (Identity and Access Management) to manage security. A comparison of the three scenarios shows that, in a serverless

architecture environment, the threat with the greatest impact is the second one, which is very worrying, since it indicates the evasion of client validations, the escalation of privileges and the exfiltration of secrets, indicating that these threats affect authentication, access management and credential security to carry out more complex attacks.

Keywords: Serverless architecture; security risks; key management; attack surface; insecure configuration and data injection.

Resumo

Este artigo surge como produto final do trabalho de tese cujo tema é Análise de segurança em arquiteturas serverless na cloud e estratégias para a mitigação de riscos como objetivo da investigação; A análise de segurança em arquiteturas sem servidor baseadas na cloud, especialmente em plataformas como a Amazon Web Services (AWS), envolve a avaliação dos riscos e vulnerabilidades inerentes a este modelo. Nas arquiteturas sem servidor, os utilizadores não gerem os servidores diretamente, o que pode aumentar a eficiência e reduzir os custos, mas também representa novos desafios de segurança. Os riscos mais relevantes incluem a suscetibilidade a ataques como a injeção de código, a escalabilidade de funções e problemas com o acesso não autorizado a dados através de interfaces configuradas incorretamente. Como oferta de serviços na cloud, a AWS oferece ferramentas como o AWS Lambda, o API Gateway e o IAM (Identity and Access Management) para gerir a segurança.

A comparação dos três cenários permite verificar que, num ambiente de arquitetura serverless, a ameaça com maior impacto é a segunda, o que é muito preocupante, pois indica a evasão de validações de clientes, a escalada de privilégios e a exfiltração de segredos. indicando que estas ameaças afetam a autenticação, a gestão de acessos e a segurança das credenciais para realizar ataques mais complexos.

Palavras-chave: Arquitetura sem servidor; riscos de segurança; gestão de chaves; superfície de ataque; configuração insegura e injeção de dados.

Introducción

Esta investigación analiza las diferentes manifestaciones de la seguridad, analizando sus efectos y la importancia de llevar a cabo una postura global para abordar los desafíos presentes y futuros.

Hoy en día, en esta era digital, la transición hacia arquitecturas serverless en la nube ha modificado el modo en que las organizaciones crean y despliegan aplicaciones. Estas arquitecturas permiten a los programadores centrarse en las metas del negocio sin la necesidad de tener que pensar en los recursos del servidor, permitiendo una mayor rapidez a nivel operativo. Sin embargo, esta tendencia ha producido la ampliación del propio territorio de los problemas relacionados con la seguridad (Ross, 2020).

La arquitectura serverless es dinámica, está distribuida y deja al alcance de las atacantes vulnerabilidades que pueden ser explotadas; por lo tanto, resulta importante estudiar los riesgos de seguridad asociados a la adopción de arquitecturas serverless y tener una aproximación pragmática de sus posibles formas de mitigación. Proteger la información en una arquitectura sin servidor requiere un enfoque integral y proactivo que resuelva los aspectos técnicos y organizativos a fin de mitigar los riesgos de esta nueva forma de computación en la nube.

Sin embargo, la nube pública presenta diferentes problemas, especialmente porque las empresas tienen poco control sobre la seguridad y la configuración de sus aplicaciones. Por otro lado, el uso de la nube pública implica el compartir recursos con otros consumidores, lo que aumenta el riesgo de vulnerabilidades en la infraestructura que afecta a varios clientes. Así mismo, el uso de un servicio de nube pública puede conllevar una dependencia que dificultaría el poder cambiar de proveedores si se da una eventualidad posterior y dejaría a su empresa con menos opciones y una posible desventaja económica a la hora de cambiar de proveedor o adaptar la plataforma de funcionamiento en un futuro.

La utilización de servicios serverless en la nube, se traduce en dependencia de los servicios y configuraciones que proporciona el proveedor, haciendo que el proceso de adaptación de las aplicaciones a nuevos entornos sea complicado y puede generar un incremento de costes si se intenta trasladar. Asimismo, el control limitado en la configuración de la seguridad las hace vulnerables a brechas, configuraciones erróneas o desconocimiento de las mejores prácticas por su parte que pueden hacer incrementar la exposición o poner en peligro datos sensibles.

Las herramientas disponibles para monitorizar, así como para evaluar la efectividad de aplicaciones serverless son poco extensivas, lo que complica la inspección de situaciones en tiempo real y empeora cualquier efecto negativo determinado por un funcionamiento erróneo o por situaciones de seguridad, comprometiendo la seguridad del servicio y la continuidad del mismo.

El crecimiento de las aplicaciones sin servidor en la nube pública ha transformado el hemisferio; sin embargo, ha provocado muchos problemas de seguridad que, si no se abordan adecuadamente, pueden exponer información privada y deteriorar el funcionamiento del sistema. Tal como sugiere (Sequea Oliveros, J, 2019) fue necesario realizar una investigación para abordar el problema de las vulnerabilidades en las arquitecturas serverless en nubes públicas. Con este fin, se seleccionó la plataforma AWS (Amazon Web Services) como punto focal del estudio. La identificación de las vulnerabilidades existentes y la elaboración de los vectores de mitigación también tienen una alta importancia para el progreso de la investigación en las esferas de seguridad de la nube, ya que permite proteger los datos e información corporativa de las empresas que dependen de estas estructuras para operar en el mundo digital.

Este proyecto de investigación es absolutamente crucial debido a la cuestión que destaca, ya que se ha convertido en un aspecto cada vez más conocido para muchas empresas que utilizan la nube para mejorar sus operaciones digitales, tal como lo menciona (Netalit, 2023), las aplicaciones sin servidor se vuelven más populares, también lo hace la cantidad de amenazas dirigidas a las aplicaciones. Debido a que las administraciones de arquitecturas sin servidor dependen de los proveedores de nube para la administración de infraestructura, las empresas tienen un nivel de control limitado sobre la seguridad, ya que no establecen sus propias medidas y confían en las guías y los mecanismos implementados por el proveedor (ISO/IEC 27001, 2013).

Según (Ruiz, 2020) examina cómo, al disminuir la infraestructura física, las características serverless pueden revelar vulnerabilidades particulares en el manejo de datos, una inquietud que también se encuentra en entornos empresariales. La principal referencia de este trabajo es poder identificar para nosotras las investigadoras las ventajas, los tipos de arquitecturas, características principales de las arquitecturas serverless, como pueden ser los tiempos cortos de ejecución, el pago por uso, y sin administración de infraestructura.

Definir un modelo de seguridad para gestión de vulnerabilidades de servidores en nubes privadas, que contemple lineamientos generales para el diseño de una política de seguridad donde se detallen roles de usuarios y documentación recomendada (Cifre, 2020), un proceso de aseguramiento apoyado sobre actualizaciones, indicadores de vulnerabilidad basado en factores críticos de seguridad, y clasificación de niveles de seguridad fundamentada en la madurez de la organización. La principal referencia de este trabajo es poder identificar sobre las vulnerabilidades ya que son una debilidad en un sistema de información que genera vulnerabilidades, al igual que a protección

de la información está en peligro, permitiendo que un intruso pueda poner en peligro la seguridad de la información. integridad, disponibilidad o privacidad de esta son esenciales, por lo que resulta imprescindible identificarlas y suprimirlas lo más pronto posible (Reglamento, 2016).

Evaluar el rendimiento de los frameworks .NET y Node.js en aplicaciones serverless en AWS (Arizaga, 2024). El propósito es identificar la determinación del framework más eficiente en términos de rendimiento. Una de las principales referencias de este trabajo son las características de la computación en la nube, al igual que los modelos de implementación en la nube, como lo son la nube pública, privada, comunitaria e híbrida.

Según (Guaigua Bucheli, 2021) en este análisis lleva a cabo un examen detallado de algoritmos de seguridad vinculados a la nube y propone estrategias sistemáticas para minimizar riesgos particulares en el almacenamiento de datos. La principal referencia de este trabajo es que hoy en día enfrenta los retos de identificar la seguridad en la nube y sugiere tácticas para reducir riesgos mediante algoritmos de seguridad eficaces.

Finalmente, las infracciones de la seguridad de la información generan efectos adversos, tales como pérdidas económicas, deterioro de la reputación y consecuencias de tipo legal. Según el informe de Verizon sobre vulneraciones de datos, el coste medio de la vulneración de los datos se estima en millones de dólares, así como los efectos a largo plazo para la confianza del consumidor (Verizon Sourcing LLC, 2024)

Metodología

La investigación se enfoca en identificar y evaluar las vulnerabilidades específicas de los entornos serverless, con el objetivo de proponer soluciones efectivas que minimicen los riesgos y fortalezcan la seguridad general de estos sistemas.

El enfoque metodológico de esta investigación no se limita solo a poder identificar y reducir riesgos, sino que también tiene la intención de poder aportar un conocimiento de los conocimientos generales de una forma más robusta sobre la seguridad que pueda presentar la arquitectura serverless.

La investigación se realiza en un entorno controlado y virtual con la finalidad de replicar los ajustes habituales de las arquitecturas sin servidor y evitar los riesgos en sistemas reales. Es un método que, tanto como sea posible, descarta las variables externas de la ecuación, lo que simplifica la ejecución de una evaluación más precisa y adecuada. El laboratorio va a estar provisto de

herramientas y plataformas de simulación, por ejemplo, AWS CloudFormation para el despacho de arquitecturas sin servidor; Datadog o CloudWatch para monitorizar la parte de los logs de las situaciones que se producen.

El entorno además va a recomendar configuraciones de permisos y roles que simulan las situaciones del mundo real, por ello es factible identificar problemas tales como las configuraciones erróneas o el escalado de privilegios, y es por ello planificamos e identificamos las técnicas de laboratorio y escenarios de ataques y amenazas simuladas como se refleja en la siguiente tabla 1:

Tabla 1: *Herramientas de laboratorio*

Componente	**Herramienta/ Software para usarse**	**Descripción**
Plataforma serverless	AWS Lambda, Azure Functions, 34Google Cloud Functions	Contiene despliegue de funciones serverless emulando problemas reales.
Almacenamiento	DynamoDB, Firestore, S3	Contiene la simulación de bases de datos y almacenamiento serverless.
Redes virtuales	Virtual Private Cloud (VPC), Subnetting	Infraestructura para simular tráfico interno y externo.
Simulación de ataques	Metasploit, OWASP ZAP, Postman	Realización de generación de amenazas específicas para evaluar las funciones serverless.
Monitoreo y análisis	CloudTrail, Prometheus, Grafana, Elastic Stack	Herramientas que captan eventos y métricas desde la nube.
Gestión de API	API Gateway, Postman, Burp Suite	Emulando el tráfico API o control de acceso.

La nube AWS también dispone de una documentación técnica exhaustiva y un soporte activo, hecho que justifica la elección de dicha plataforma para implementar arquitecturas sin servidor. Al mismo tiempo se da lugar a evaluar las vulnerabilidades de la misma. En general, la principal razón para elegir AWS es su alta adopción en muchas industrias, haciendo que los resultados y estrategias de esta investigación sean relevantes para la replicación y la aplicación en muchos casos empresariales. Este enfoque hizo posible realizar una investigación aplicada y práctica, llegar a una comprensión profunda de los desafíos de seguridad centrales en las arquitecturas serverless y, al mismo tiempo, proponer soluciones alineadas con las demandas únicas de las empresas adoptando

tecnologías en la nube. Cómo se muestra en la figura 1 una arquitectura serverless en la nube, compuesta por varios servicios de AWS.

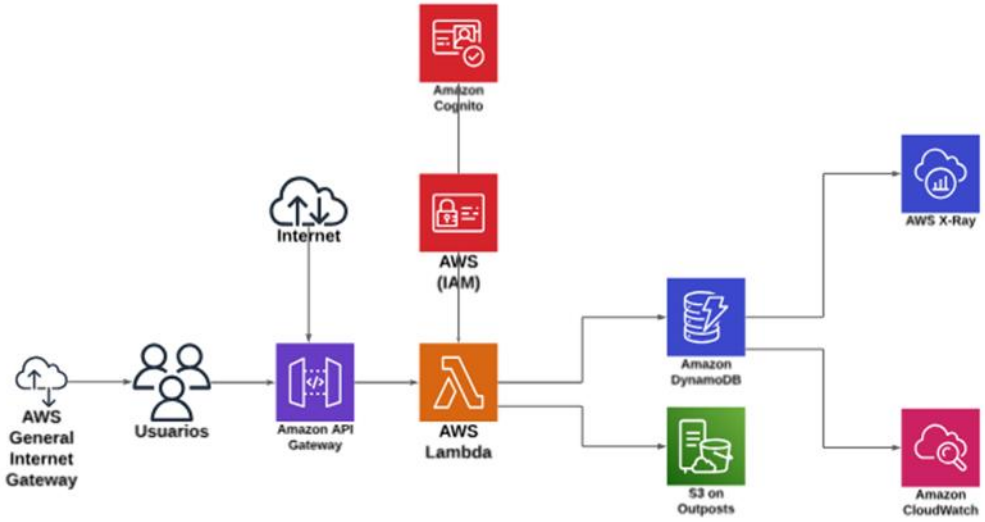

Figura 1: *Topología de AWS*

Escenarios de pruebas

Se han desarrollado tres escenarios de prueba con el objetivo de poder determinar el nivel de seguridad y el nivel de mitigación que se puede alcanzar en las arquitecturas serverless basadas en la nube, en este caso de Amazon Web Services AWS. Estos tres escenarios simulan ataques reales en las cuales personas malintencionadas ponen en riesgo la seguridad del sistema utilizando varios métodos como es la ingeniería social, vulnerabilidades y amenazas internas. Debido a que el enfoque fue en los tres escenarios, también se examinaron las estrategias de respuesta a incidentes de seguridad y la resiliencia de los sistemas sin servidor ante los tres escenarios.

Primer Escenario (Auditoría Interna)

En esta prueba de pentesting el atacante ha comprometido credenciales del servicio de AWS por medio de ingeniería social, donde obtuvo la clave de acceso y el id de acceso, en esta prueba lo que haremos es escalar privilegios al punto de eliminar una instancia llamada “cg-super-critical-security-server”

Descargamos CloudGoat para crear un ambiente de prueba.

Figura 2: *Crear un ambiente de prueba*

Cómo se muestra en la figura 2, después de clonar el repositorio leemos su respectiva documentación por si ha habido cambios.

Figura 3: *Descomprimir el archivo*

La instalación de cloudGoat es porque es una herramienta que ayuda a crear entornos sensibles intencionalmente vulnerables en AWS en la7 cuenta establecida ahora descargamos y descomprimimos la herramienta complementaria terraform.

Cómo se muestra en la figura 3, el archivo se está descomprimido y lo movemos a la ruta especificada y verificamos su instalación.

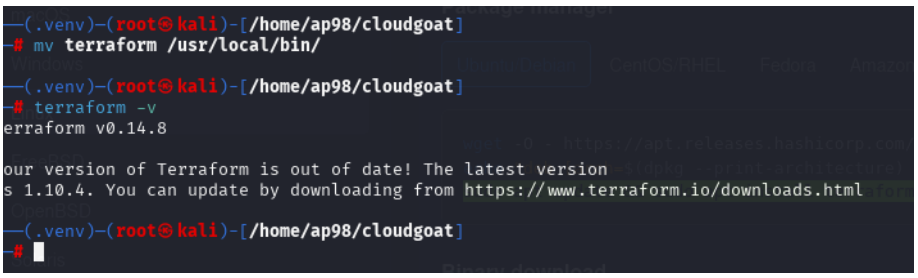

Figura 4: *Configuración*

Cómo se muestra en la figura 4, se está configurando un perfil en cloudgoat.

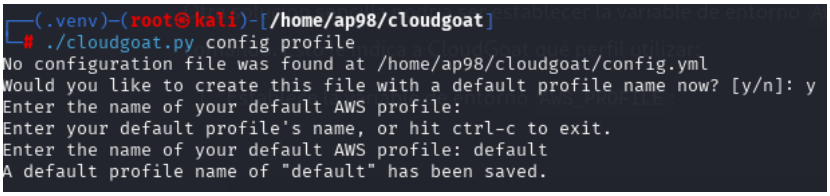

Figura 5: *Creación de ambiente*

Cómo se muestra en la figura 5, se creó nuestro ambiente

Mediante el primer escenario, se evidenciaron errores significativos en el control de accesos y credenciales con la posibilidad de que un atacante con la escalada de privilegios comenzara a eliminar recursos críticos, expusiera credenciales. La escalada de privilegios presenta un riesgo muy elevado (100%) y la exposición de credenciales un riesgo elevado (80%), lo que significa que habría que mejorar la seguridad en IAM y en la protección de las claves. La recomendación de mejora es el principio de menor privilegio, la autenticación multifactor (MFA) y el refuerzo del control de accesos mediante AWS CloudTrail y GuardDuty.

Segundo Escenario (Auditoría Interna)

En esta segunda prueba de pentesting el atacante ha comprometido credenciales del servicio AWS por medio de un trabajador, donde proporcionó información sobre la clave y el ID de acceso, por lo cual este es un ataque de amenaza interna (insider threat). Tenemos una función lambda que aplica políticas a los usuarios y explota una vulnerabilidad en la función para escalar los privilegios de nuestro usuario “bilbo” para buscar secretos (secretsmanager).

Figura 6: *Ambiente controlado*

Cómo se muestra en la figura 6, primero levantamos nuestro ambiente controlado.

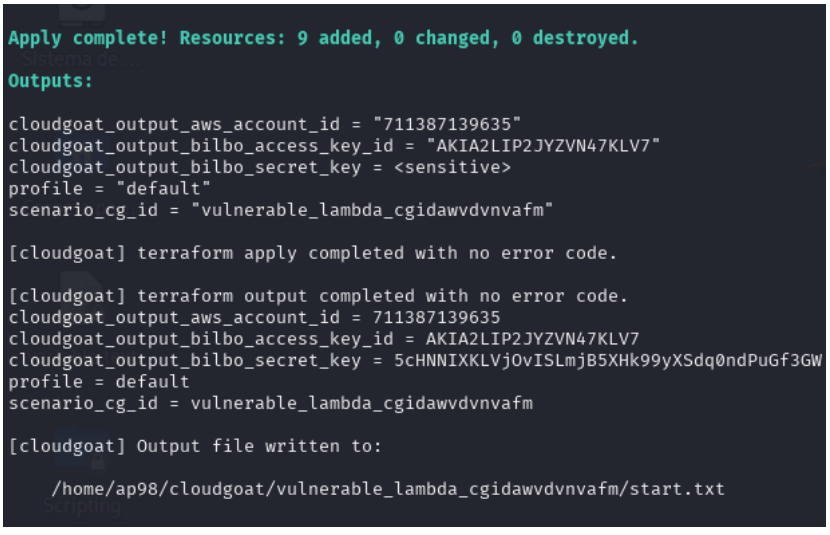

Figura 7: *Consola de AWSCLI*

Cómo se muestra en la figura 7, luego de levantado el ambiente podemos configurar nuestro acceso a la consola de awscli.

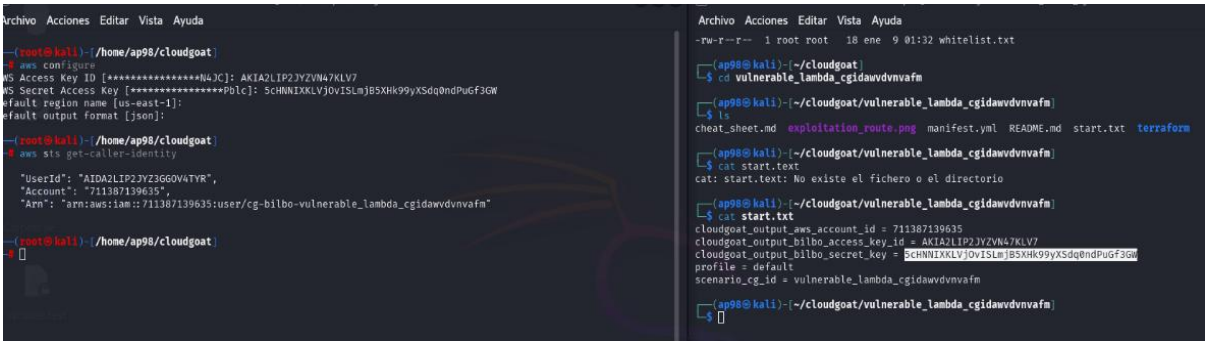

Figura 8: *Comando secretos*

Cómo se muestra en la figura 8, ahora como puede ver no tenemos acceso a él comando de los secretos.

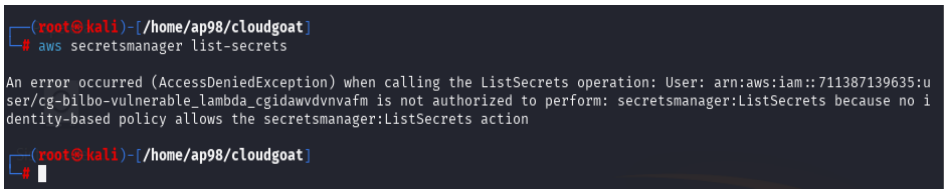

Figura 9: *Nombre del usuario*

Cómo se muestra en la figura 9, después de esto buscamos el nombre del usuario y también sus políticas para ver que tenemos a nuestra disposición.

El segundo escenario puso de manifiesto fallos críticos en la protección de secretos y control de accesos, lo que permitiría la exfiltración de credenciales y una propagación del ataque por la infraestructura (movibles laterales). El riesgo de la exfiltración de secretos es el más elevado (100%), seguido de la falta de control (60%), siendo un indicativo de que habría que reforzar la seguridad en AWS Secrets Manager y la detección de amenazas.

Para mejorar estos riesgos, es posible habilitar la rotación de credenciales automática, restringir los accesos mediante las políticas IAM estrictas y reforzar el control mediante AWS CloudTrail y AWS CloudWatch.

Tercer Escenario (Auditoría Interna)

En el tercer pentesting el atacante ha comprometido credenciales del servicio AWS a partir de un empleado, mediante el cual le proporcionó su clave y su ID de acceso... mediante un ataque de ingeniería social, se trata de un ataque de amenaza interna (insider involuntario)-(phishing). En este escenario se presenta una página de registro de sesión con AWS Cognito en el backend. Se debe evitar las restricciones al igual que explotar las configuraciones erróneas en Amazon Cognito para que eleve sus privilegios y así poder obtener las credenciales de Cognito Identity Pool.

Primero levantamos nuestro ambiente controlado

Figura 10: *Enlace generado*

Cómo se muestra en la figura 10, se visita el enlace generado por el “cloudgoat créate vulnerable cognito” en un navegador. Su nombre es “apigateway url”, se comienza con un formulario de inicio

de sesión y registro, el atacante intenta registrarse usando un correo electrónico, pero recibe un error de validación de correo electrónico.

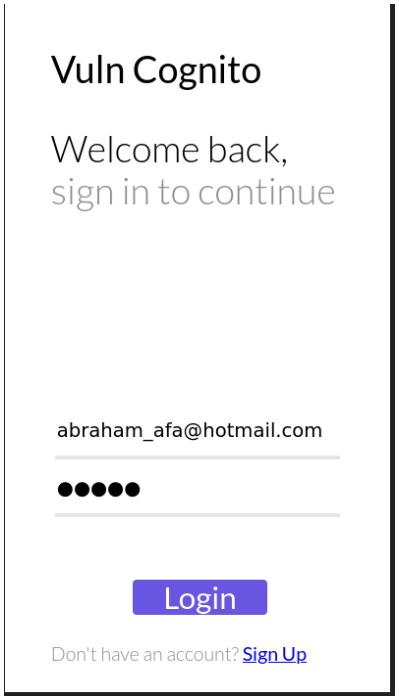

Figura 11: *Vuln Cognito*

Cómo se muestra en la figura 11, el atacante abre el código de fuente de la página web para poder obtener el ID del cliente de Cognito Userpool, luego el atacante procede a utilizar AWS CLI para registrarse y confirmar el correo electrónico manualmente y así poder evitar la verificación del lado del cliente para el correo electrónico.

Figura 12: *Atacante inicia sesión*

Cómo se muestra en la figura 12, el atacante inicia sesión y es redirigido a la página web "reader.html" la cual no contiene ninguna información útil. En Burp Suite, el atacante encuentra un atributo de usuario personalizado agregado después de la confirmación por correo electrónico.

El tercer escenario, evidenció errores críticos en la autenticación y control de accesos, lo que permitiría (100%) evadir una validación de usuario en AWS Cognito, obtener privilegios elevados, lo que evidencia que las debilidades en la validación de clientes permitirían comprometer la infraestructura. La recomendación de mejora es: reforzar las reglas de autenticación de Cognito, autenticación multifactor (MFA) y restricciones estrictas en IAM para evitar accesos indebidos.

Resultados y discusión

Los resultados se exponen de acuerdo con la línea de investigación. se empieza por la delimitación de las debilidades propias de las arquitecturas serverless y se evalúan las políticas de seguridad que están en práctica actualmente. Se enmarca con encuestas a usuarios y administradores de servicios en la nube y con entrevistas a expertos en seguridad, así como también de revisiones de documentos técnicos y aun por la revisión de resúmenes de incidentes de seguridad; de la misma manera, se enmarca con este análisis de resúmenes de incidentes de seguridad.

Resultados del ambiente controlado

Los resultados obtenidos de un entorno controlado son los que se presentan estructurados en 3 escenarios distintos, donde se aborda el desarrollo de distintos riesgos en seguridad de infraestructura en nube; cada escenario es una tabla que enumera el riesgo, el impacto, la probabilidad, el nivel de riesgo y las mitigaciones.

Distribución de riesgo

La evaluación comparativa de los tres escenarios pone de evidencia que la evasión de la validación del cliente 100% y la escalada de privilegios 100% constituyen las amenazas más determinantes en los entornos de arquitecturas serverless, al afectar la autenticación y la gestión de accesos, mientras que la exfiltración de secretos 100% es otra situación de peligro destacable, ya que compromete credenciales para realizar movimientos en el interior de la infraestructura a modo de ataques aún más sofisticados.

La probabilidad de su ocurrencia es mayor en el tercer escenario (100%), lo cual refleja que ataques hacia la autenticación y gestión de permisos son más habituales, o simplemente que son más sencillos de llevar a cabo si no se encuentran correctamente controlados. En el segundo escenario

la falta de monitoreo (80%) pone de manifiesto la importancia de poder implementar herramientas de detección temprana de amenazas para evitar accesos no autorizados y ataques escalonados.

Tabla 2: *Distribución de riesgos*

Escenario	Mayor riesgo identificado	Impacto (%)	Probabilidad (%)	Nivel del riesgo (%)
Primer escenario	Exfiltración de secretos	100%	60%	**100%**
Segundo escenario	Movimientos laterales	100%	60%	**100%**
Tercer escenario	**Ausencia de monitoreo**	**100%**	**100%**	**100%**

Conclusiones

Uno de los problemas más destacados fue la escalada de privilegios puede ser caracterizada, en una vulnerabilidad, pero en este caso de los permisos, ya que es la vulnerabilidad que reside en ese tipo de gestión de permisos en plataformas de AWS y se produce cuando un atacante es capaz de escalar privilegios, es decir, superar una configuración incorrecta asociada a IAM, el módulo AWS Identity and Access Management., presentándose como un problema común en los 3 casos de usabilidad como consecuencia de la incorrecta gestión de la configuración de AWS Identity and Access Management (IAM).

Un atacante a partir de escaladas de privilegio puede llegar a tener acceso a los recursos en su totalidad, haciéndolo capaz de eliminar instancias críticas o modificar información confidencial. La exfiltración de secretos es importante en el sentido que el acceso por medio de unas credenciales mal configuradas a AWS Secrets Manager puede permitir movimientos laterales en la infraestructura para incrementar la extensión del ataque.

Las buenas prácticas de seguridad es el camino que permitirá incorporar la computación serverless a su sentido sin tener que lidiar con el riesgo de encontrarse con muchas vulnerabilidades y riesgos innecesarios. La implementación de los controles adecuados puede reducir hasta el 70% la posibilidad de exposición a ataques, dando a los usuarios de la computación serverless las oportunidades de escalar y conseguir eficiencia sin comprometer la seguridad de sus datos y sistemas.

La arquitectura de seguridad en serverless no se limita de forma absoluta a las herramientas tecnológicas sino también en la configuración, monitoreo y educación del personal responsable.

Amazon garantiza un ecosistema robusto que, combinado con buenas prácticas de seguridad, permite a las organizaciones minimizar riesgos y maximizar la confiabilidad de sus aplicaciones. Al publicarse, busca no solo aportar al conocimiento académico, aporta también la asimilación a profesionales y empresarios que deseen implementar aplicación serverless de forma segura y óptima, contribuyendo a abordar desafíos de escenario tecnológico en la actualidad.

Referencias

1. Arizaga, B. E. (19 de marzo de 2024). Obtenido de Repositorio Institucional: https://repositorio.ug.edu.ec/server/api/core/bitstreams/ccf058f2-d0af-46ce-8678-083d327183e5/content
2. Cifre, S. (2020). Modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas. Santa Fé, Argentina.
3. Guaigua Bucheli, C. J. (2021). Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático. Guayaquil, Ecuador.
4. ISO/IEC 27001. (2013). Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos.
5. Netalit. (2023). Top 7 cloud vulnerabilities in 2024. Obtenido de https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-cloud-security/top-7-cloud-vulnerabilities-in-2024/
6. Reglamento. (27 de abril de 2016). Reglamento (UE) 2016/679. Obtenido de Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de PrProtección de Datos).
7. Ross, A. (2 de diciembre de 2020). Security Engineering. Ingeniería de seguridad: una guía para crear sistemas distribuidos fiables. Obtenido de https://doi.org/10.1002/9781119644682
8. Ruiz, E. S. (2020). Aplicación de tecnologías y arquitecturas serverlesspara el desarrollo desoluciones IoT. Barcelona, Catalunya, España.
9. Sequea Oliveros, J. (2019). Las vulnerabilidades de las nubes públicas y cómo protegerlas. Obtenido de https://gmsseguridad.com/wp-content/uploads/2021/06/7-practicas-nube-publica.pdf

10. Verizon Sourcing LLC. (1 de mayo de 2024). Informe de investigaciones sobre violaciones de datos 2024. El auge de la explotación de vulnerabilidades amenaza la ciberseguridad. Obtenido de https://www.globenewswire.com/news-release/2024/05/01/2872907/0/en/2024