Waylet: seguridad ágil para entornos nativos Cloud

Klikin, responsable de Waylet, la aplicación de pago y fidelización de Repsol, trabaja con Innovate como socio de confianza de su seguridad *cloud* y de aplicación. Cuando el cambio constante, el *time-to-market* y las nuevas tecnologías son un diferenciador de negocio, la seguridad requiere un enfoque de "fidelización" que se adapte a la filosofía y relevancia del producto.

Javier Gorines / Luis Enrique Oliveri

Klikin es una empresa especializada en el desarrollo de soluciones tecnológicas que crea productos como **Waylet**. Waylet es la aplicación de pago y fidelización de **Repsol** que incorpora servicios digitales como el pago del repostaje desde el surtidor, y del parquímetro en zonas reguladas (verde, azul y naranja), entre otros.

Por su naturaleza de negocio nativo digital, Klikin combina talento y tecnología, aplicando procesos propios de las metodologías Lean y Agile para conservar la esencia del modelo *start-up* bajo el paraguas de una gran multinacional.

Ese modelo de *start-up* solo es viable incorporando profesionales (y socios de confianza) especializados y multidisciplinares, altamente cualificados y comprometidos con la excelencia y la calidad a lo largo de todo el proceso de trabajo.

La relación entre Klikin e **Innovate** se remonta a 2021 y cada año colaboran para fortalecer la seguridad de Waylet en un enfoque de socios de confianza.

En una primera colaboración, Innovate hizo una revisión exhaustiva de la seguridad de algunos componentes de Waylet basado en dos perspectivas: con los puntos de vista del Arquitecto de Seguridad, por un lado, y el del Ciber Atacante por otro; abarcando así un mayor espectro de vectores de ataque y controles seguridad.

Evaluación de la arquitectura de seguridad Cloud

El objetivo de esta perspectiva de evaluación fue identificar los *gaps* y mejoras de seguridad sobre la arquitectura Cloud actual; y sobre las propias configuraciones de los servicios y recursos desplegados en la nube AWS, con base en estándares y mejores prácticas de seguridad y la experiencia del personal de Innovate en clientes similares. Para ello, se conformó un equipo de arquitectos y analistas de seguridad AWS certificados que, colaborando con los arquitectos de Klikin, hicieron una revisión en profundidad empleando dos metodologías propietarias de Innovate: la arquitectura de referencia de seguridad AWS y el modelo de operaciones de seguridad AWS.

Siguiendo las capas de arquitectura de seguridad, se revisaron los siguientes elementos y controles en el diseño, configuración y despliegue del *back-end* de Waylet:

- Gobierno de la seguridad *cloud*
- Seguridad de red
- Protección de datos

Para el proyecto se conformó un equipo de arquitectos y analistas de seguridad AWS certificados que, colaborando con los arquitectos de Klikin, hicieron una revisión en profundidad empleando dos metodologías propietarias de Innovate: la arquitectura de referencia de seguridad AWS y el modelo de operaciones de seguridad AWS.

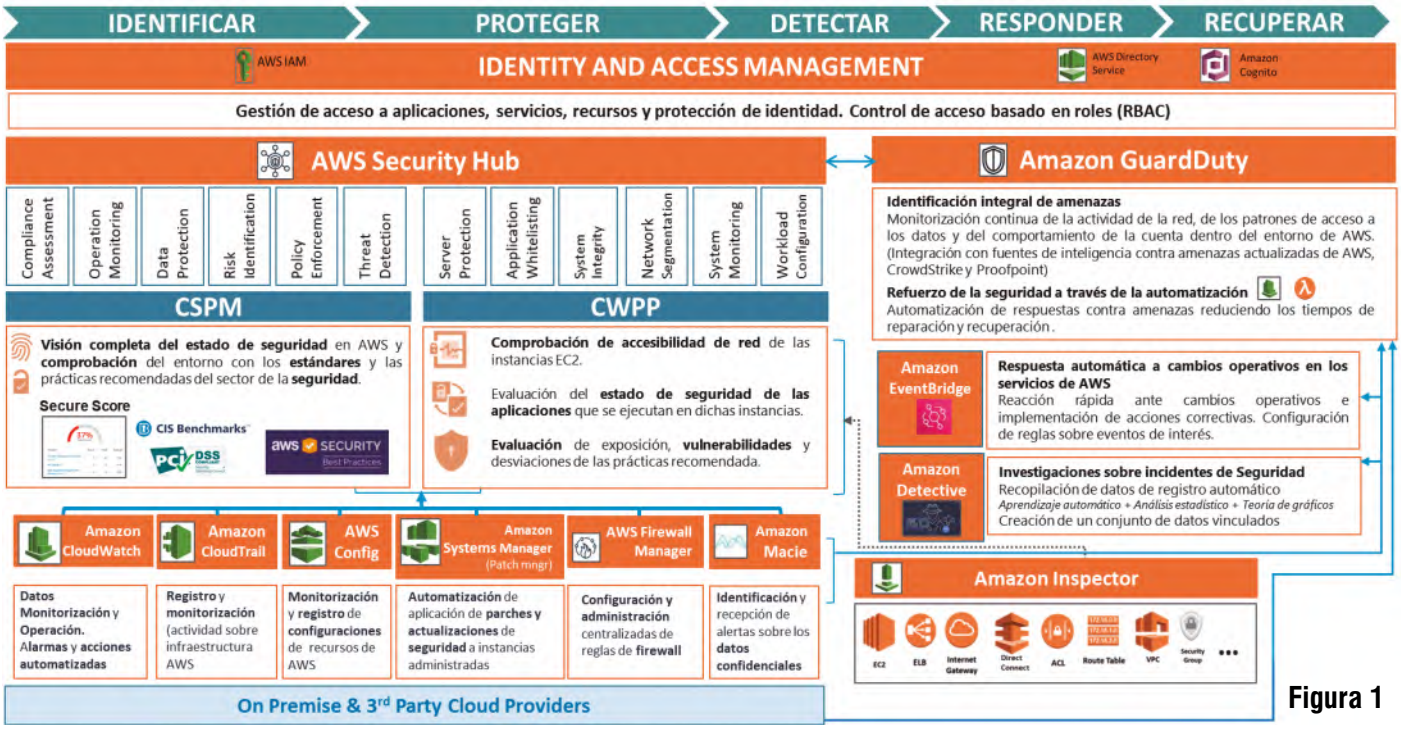

Figura 1

INNOVATE
a MNEMO company

TRANSFORMACIÓN DIGITAL SEGURA

TU SOCIO DE CONFIANZA PARA LA SEGURIDAD CLOUD

La adopción segura de servicios en la nube es hoy una necesidad en un contexto de amenazas crecientes y **transformación digital acelerada**.

Arquitectura de Seguridad Cloud

Seguridad IaaS y PaaS

Seguridad SaaS

Seguridad Cloud Gestionada

Innovate a mnemo company

innovate.mnemo.com

España | México | Colombia | Perú | Ecuador

aws PARTNER Select Tier Services

Microsoft Solutions partner Security

ens

AUTHORIZED TO USE CERT

TF-CSIRT Trusted Introducer

FIRST

- Protección de *workloads* y aplicación
- Gestión de identidades y accesos, y ciberdefensa

Adicionalmente, se revisó cómo se emplean los mecanismos nativos de seguridad de AWS para proporcionar capacidades de detección y respuesta ante eventos de seguridad, tomando como referencia el modelo de operaciones de seguridad AWS de Innovate (figura 1).

Figura 2

El objetivo de la perspectiva de evaluación es identificar fallos en la seguridad específicos de aplicaciones y APIs mediante la detección de vulnerabilidades existentes, tanto de forma automática como manual, y la recomendación de las acciones correctivas correspondientes. Para su ejecución, Innovate se apalanca en los servicios de Attack Surface Reduction de Mnemo.

Como parte del diagnóstico, se realizó una revisión de todas las cuentas AWS de Klikin empleando una herramienta CSPM (*Cloud Security Posture Management*) comercial, que daría información a utilizar en el *assessment* global. Esta tarea incluyó la evaluación de los *templates* CloudFormation de IaC (infraestructura como código) que emplea Klikin para realizar despliegues continuos de distintas versiones de los elementos que conforman Waylet, en una filosofía DevOps.

La revisión del estado actual y la definición del modelo futuro de seguridad Cloud AWS de Waylet se realizó en un periodo de aproximadamente seis semanas. Aunque no se dan aquí detalles de los *findings* identificados, es de destacar el alto nivel de madurez del equipo de Klikin en temas de seguridad AWS, lo que sí permitió identificar áreas de mejora muy específicas en ámbitos totalmente nativos AWS.

Evaluación de la seguridad de aplicación desde la perspectiva de un Ciber atacante

El objetivo de esta perspectiva de evaluación es identificar fallos en la seguridad específicos de aplicaciones y APIs mediante la detección de vulnerabilidades existentes, tanto de forma automática como manual, y la recomendación de las acciones correctivas correspondientes. Para su ejecución, Innovate se apalanca en los servicios de Attack Surface Reduction de Mnemo, que cuentan con un equipo especializado de *pen-testers* y metodología propia de evaluación MAVERIC basada en OSSTMM (*Open Source Security Testing Methodology Manual*) y OWASP (*Open Web Application Security Project*). Adicionalmente, con el objeto de crear una valoración objetiva de las vulnerabilidades se utiliza la metodología CVSS (*Common Vulnerability Scoring System*). Esta metodología se apoya en tres métricas para producir una valoración (*scoring*) contextual a los activos analizados. La elección de esta metodología se fundamenta en la necesidad de tener un sistema de valoración independiente de un fabricante, abierta y apoyada por un organismo como FIRST (Forum of Incident Response and Security Teams).

En una primera evaluación, que acompañó la revisión de arquitectura de seguridad *cloud*, se inspeccionaron elementos *core* del *back-end* de Waylet.

Es importante destacar que durante los últimos años Waylet ha experimentado un crecimiento exponencial, acompañado del lanzamiento de nuevas funcionalidades y servicios, y de la incorporación de nuevos *partners* a su red de comercios. Crecimiento que se ha visto impulsado, entre otras cosas, por la adopción de las medidas recogidas en el Real Decreto_ley 6/2022 de 29 de marzo, y el descuento adicional ofrecido a sus clientes.

Este conjunto de factores ha favorecido la popularidad de la app, llegando a ser, durante varias semanas consecutivas en 2022, la aplicación móvil gratuita más descargada en España, y consolidándose como la aplicación con mayor cuota de mercado en la categoría de aplicaciones de Transporte en nuestro país, con más de 5,6 millones de usuarios.

Estos cambios reflejan por un lado la calidad del equipo responsable de Waylet, pero incrementan el interés de los actores maliciosos y aumentan el riesgo de sufrir ciber ataques.

Por ello, Klikin sabe que no puede bajar la guardia y aunque sigue procesos y prácticas donde la seguridad es clave, ha solicitado a Innovate continuar con revisiones periódicas de las nuevas funcionalidades y ejecutar distintas pruebas de seguridad no solo del *back-end*, sino además de otros módulos e incluso de las aplicaciones móviles Android e iOS.

Estas interacciones refuerzan la filosofía de Innovate en tanto que socios de confianza y permiten a Klikin centrarse en su actividad *core*.

Conclusiones

Los negocios nativos *cloud* como Klikin trabajan en un entorno en continua evolución y adopción de tecnologías emergentes, lo que conlleva un desafío clave: ¿cómo formar parte de la transformación digital a la vez que protege a sus clientes y empleados, asegura las operaciones y cumple con los requisitos regulatorios?

Un factor crítico en la adopción *cloud* es la seguridad y la agilidad de ésta para dar respuesta a las necesidades de los clientes. Sin embargo, existen algunos elementos que complican la adopción *cloud* segura como las fricciones de soluciones tradicionales en ámbitos nativos *cloud*, así como el difícil acceso a recursos especializados.

Por ello, y con el objetivo de centrarse en su *core-business*, organizaciones como Klikin buscan proveedores de confianza y expertos en materia de seguridad cloud (con foco en AWS en este caso). Innovate da respuesta a esas necesidades mediante un equipo experto, experimentado y certificado; así como activos y metodologías específicas de seguridad *cloud* que le permiten interactuar con una filosofía de socios de negocio. ■

Javier Gorines
CIO
KLIKIN

Luis Enrique Oliveri
Director
MNEMO INNOVATE