Ingeniería de la Ciberseguridad
Curso 2023/2024

Práctica 2
Sesión práctica 1:

Programa de ciberseguridad.

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

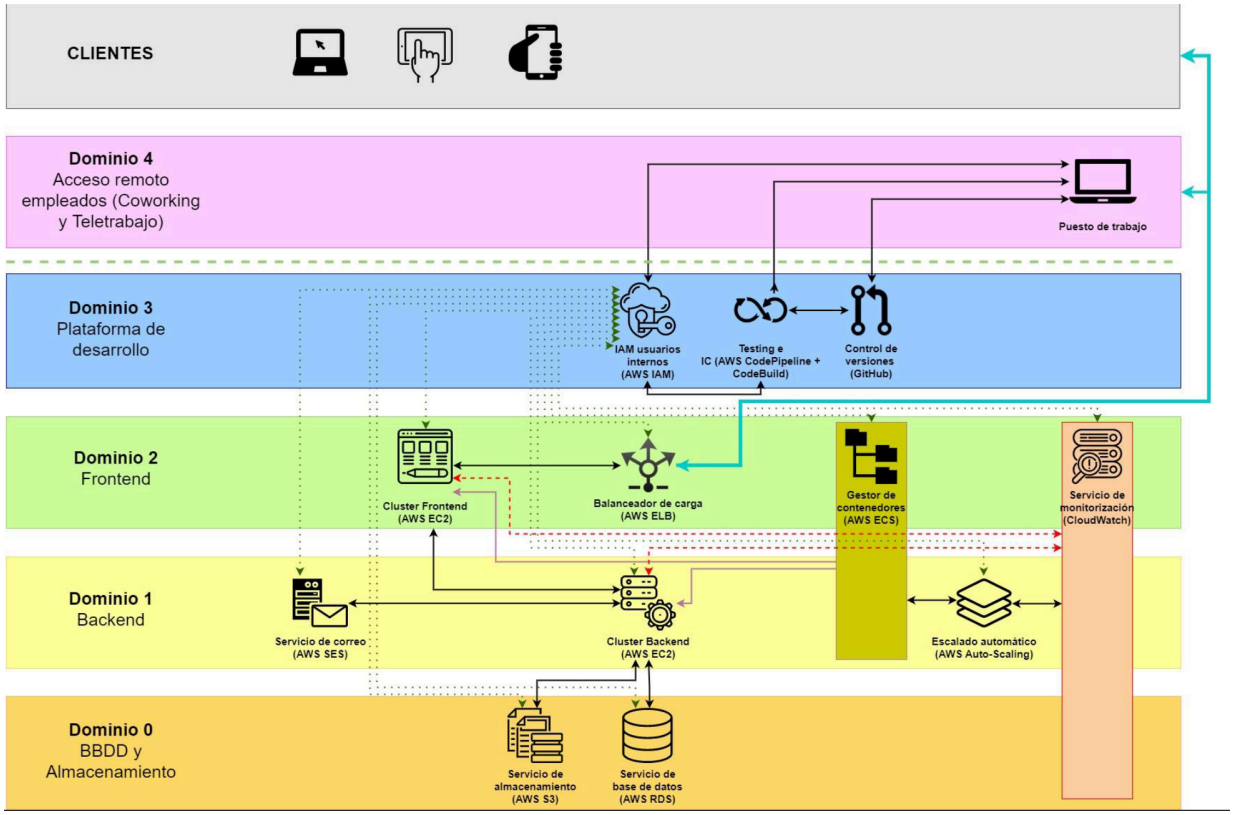
Mario Ruano Diaz

Juan Antonio Suárez Suárez

ÍNDICE

1. Arquitectura de referencia.

La estructura de ChaseMyCash se representa visualmente en el siguiente diagrama, el cual muestra los distintos elementos presentes en cada área principal.



ChaseMyCash opera a través de una aplicación web, lo que la expone principalmente a ataques. Por lo tanto, se propone un modelo de seguridad que incluya un firewall perimetral como primera barrera de defensa. Este firewall bloqueará conexiones que no cumplan con la política de seguridad de la empresa, evitando así que la red corporativa se conecte a Internet de manera no autorizada. El tráfico permitido por el firewall será dirigido al Web Application Firewall (WAF), que protegerá el servidor de aplicaciones web en el backend contra diversos tipos de ataques.

Se implementará un proceso de monitorización que utilizará múltiples logs para detectar y alertar sobre posibles amenazas en todas las etapas de protección. Esto permitirá a ChaseMyCash tener visibilidad en tiempo real sobre el tipo de tráfico al que está expuesto.

En caso de que alguna actividad maliciosa logre evadir las defensas y acceder a la aplicación, se realizará un análisis exhaustivo para determinar su origen. Esta información será crucial para mejorar continuamente las reglas de seguridad tanto del firewall como del WAF, con el objetivo de fortalecer la protección de ChaseMyCash contra futuros ataques.

2. Capacidades de seguridad.

Protección de datos: es fundamental para disminuir las posibilidades de incidentes de fuga de datos de consumidores y ataques de ransomware. Mediante la encriptación y la gestión de accesos a la información, se puede disminuir el riesgo de que los datos resulten comprometidos o sustraídos.

Detección de anomalías y eventos: es esencial para identificar posibles amenazas de ataques de denegación de servicio y ransomware. Implementando sistemas de detección de intrusiones y herramientas de análisis de seguridad en la red, se facilita la rápida identificación y mitigación de cualquier conducta malintencionada en la red.

Gestión de incidentes y recuperación: es crucial asegurar que la organización pueda restablecerse con rapidez tras un incidente de seguridad. Contando con planes de contingencia y estrategias de recuperación ante desastres establecidos, es posible minimizar el tiempo de paralización y atenuar las consecuencias de un incidente.

Monitorización continua: facilita la supervisión ininterrumpida de los sistemas corporativos para detectar posibles amenazas y vulnerabilidades. Es esencial implementar herramientas de monitoreo de la red y del comportamiento de los usuarios para asegurar que todas las acciones sean observadas y documentadas.

Autenticación y control de accesos: es crucial disponer de un método de autenticación robusto que asegure que solo los individuos autorizados tengan acceso a los sistemas y datos de ChaseMyCash. Asimismo, es vital implementar sistemas de autorización que regulen los permisos de acceso a la información.

3. Controles y contramedidas.

Sistemas de autenticación: plataformas como LDAP y Active Directory son fundamentales para comprobar la identidad de los usuarios antes de concederles acceso a los sistemas y datos de ChaseMyCash.

Herramientas de seguimiento de la actividad de los usuarios: tecnologías de monitorización como Ossec y Splunk son esenciales para observar el comportamiento de los usuarios y detectar posibles amenazas.

Sistemas de vigilancia de la red: herramientas como Nagios y Zabbix facilitan la supervisión del rendimiento y la disponibilidad de los sistemas corporativos.

Estrategias de recuperación de desastres: estas soluciones ayudan a restablecer la operatividad normal tras un incidente. Herramientas de respaldo y replicación de datos, tales como Veeam Backup y Replication, son empleadas para tal fin.

Sistemas de detección de intrusiones: facilitan la identificación de comportamientos malintencionados en la red. Se emplean sistemas como IDS (Intrusion Detection System) e IPS (Intrusion Prevention System), utilizando herramientas destacadas como Snort y Suricata.

4. Políticas de seguridad.

Al abordar la seguridad empresarial, es fundamental determinar primero las vulnerabilidades y los activos críticos que requieren protección. Tras realizar esta evaluación, se deben implementar políticas de seguridad adecuadas y eficaces para asegurar la integridad de la organización.

Las políticas de seguridad que ChaseMyCash debería implementar de forma prioritaria son:

1. **Políticas de contraseñas robustas y su renovación regular:** implementar contraseñas complejas puede disminuir notablemente el peligro de accesos no autorizados a los sistemas y datos. Es crucial que ChaseMyCash desarrolle políticas que demanden contraseñas que incluyan una mezcla de letras, números y símbolos, y que estipulen su cambio frecuente. También es vital que la empresa capacite a sus usuarios acerca de la importancia de mantener contraseñas seguras y de evitar compartirlas con terceros.

2. **Políticas de gestión de acceso y autenticación de usuarios:** es crucial implementar políticas que exijan la autenticación multifactor (MFA) y la autorización por roles. La autenticación multifactor proporciona una capa extra de protección en el proceso de verificación de usuarios, mientras que la autorización por roles asegura que solo los usuarios autorizados accedan a la información y funciones correspondientes.

3. **Política de privacidad y manejo de datos de los clientes:** Es esencial que ChaseMyCash desarrolle políticas claras respecto a la privacidad y la seguridad de los datos de los clientes. Esto incluye asegurar la transparencia en el tratamiento de datos personales y el cumplimiento de las legislaciones y normativas vigentes sobre protección de datos. La empresa debe implementar políticas y procedimientos definidos para la administración de datos personales, que abarquen desde la obtención del consentimiento hasta el manejo de peticiones de acceso o supresión de datos.

5. Recursos humanos.

Se sugiere el siguiente plan de asignación de personal y contrataciones requeridas:

En el departamento dirigido por el CEO, centrado en el desarrollo empresarial y el marketing estratégico, se propone la posibilidad de ampliar el equipo actual de 8 personas, encargado de las ventas y atención al cliente, con la contratación de un especialista en marketing digital. Esta incorporación se contempla como una medida para mejorar la visibilidad y el alcance global de la plataforma.

Para el departamento dirigido por el CTO, enfocado en Tecnologías de la Información y el desarrollo de productos, se presenta la siguiente propuesta: Actualmente, el equipo consta de 11 miembros, incluyendo desarrolladores front-end, back-end, y tres arquitectos en la nube, además de dos profesionales dedicados a la seguridad corporativa y del producto. Con el objetivo de reforzar la seguridad de la plataforma, se sugiere contratar lo siguiente:

- Dos expertos en ciberseguridad con experiencia en entornos cloud, encargados de evaluar y mejorar la seguridad de la infraestructura en AWS.

- Un especialista en criptografía, responsable de garantizar la protección de los datos de los usuarios y mejorar los protocolos de cifrado.
- Tres especialistas en CERT/SOC, responsables de la monitorización de los registros y la respuesta ante incidentes.
- Un especialista en pruebas de penetración, encargado de simular escenarios de ataque para las distintas implementaciones propuestas por la empresa, verificando así su correcto funcionamiento.

Para el departamento bajo la dirección del COO, encargado de Finanzas, Recursos Humanos y Legal, actualmente se cuenta con el apoyo de una persona y ayuda subcontratada. Con el objetivo de fortalecer esta área, se sugiere lo siguiente:

- Contratar a un profesional de recursos humanos para una gestión eficiente de las contrataciones y el desarrollo del equipo.
- Contratar a un especialista legal con conocimientos básicos en GDPR, para abordar los aspectos legales y la protección de datos.

En conjunto, se sugiere la incorporación de 10 nuevos empleados para potenciar y consolidar la estructura y seguridad de ChaseMyCash.