



Práctica 2

Sesión práctica 2:

Plan director de seguridad

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

1. Proyectos que se realizarán en los próximos 12 meses

1.1. Proyecto para la implementación de soluciones de copias de seguridad eficiente y segura.

El propósito de este proyecto es establecer métodos de respaldo efectivos y fiables para asegurar la duplicidad de los datos de ChaseMyCash y su capacidad de recuperación en caso de emergencias.

- **Identificación de datos críticos para respaldar:** Evaluar la información y determinar cuáles son esenciales para el funcionamiento de ChaseMyCash. Estos datos se incluirán en los respaldos.
- **Evaluación y selección de soluciones de respaldo disponibles en el mercado:** Se optará por AWS Backup para gestionar de manera centralizada y automatizada los respaldos de Amazon RDS y S3. Este servicio permite proteger los datos en ambos servicios y almacenar los respaldos de forma segura en un repositorio cifrado. También facilita la programación, retención y restauración de datos.
- **Configuración de la solución de respaldo seleccionada según las necesidades específicas de la empresa:** Ajustar las instantáneas de RDS y el almacenamiento en S3, incluyendo frecuencia y políticas de retención.
- **Planificación de contingencia y recuperación ante desastres:** Diseñar un plan para manejar situaciones de emergencia y restaurar datos desde los respaldos en caso de pérdida.
- **Mantenimiento del plan de respaldo actualizado:** Revisar periódicamente las políticas y configuraciones para asegurar la efectividad y relevancia continua de los respaldos para ChaseMyCash.

Para el proyecto de implementación de soluciones de respaldo eficientes y seguras, se designarán los siguientes responsables:

- **El CTO de ChaseMyCash** liderará el proyecto y se encargará de garantizar el cumplimiento de los objetivos y la asignación de recursos necesarios.
- **Dos expertos en ciberseguridad con experiencia en entornos cloud, junto con un arquitecto cloud,** serán responsables de identificar los riesgos de seguridad y asegurar que las soluciones de respaldo seleccionadas sean seguras y estén configuradas adecuadamente.
- **Un experto en pruebas de penetración** realizará pruebas para garantizar la eficacia de las soluciones de respaldo y asegurar que cumplan con los objetivos.

En cuanto a la planificación temporal:

Se estima que la implementación del proyecto para ChaseMyCash tomará aproximadamente tres meses, aunque una vez implementado, el proyecto continuará de manera indefinida. Dentro de estos tres meses, se abordará la definición de la política de respaldo y la implementación de la solución de respaldo en sí. Se estima que la identificación de datos críticos y la elaboración de la política de respaldo llevarán dos semanas. La investigación, selección, configuración y puesta en marcha de la solución de respaldo tomará entre 8 y 10 semanas adicionales. Por lo tanto, se espera que aproximadamente en tres meses se puedan realizar respaldos de forma rutinaria.

La configuración de redundancia, las pruebas y la elaboración del plan de contingencia y recuperación ante desastres se llevarán a cabo en el tercer mes del proyecto.

En cuanto a los recursos necesarios:

Para el almacenamiento de respaldos, ChaseMyCash utilizará Instantáneas de base de datos de Amazon RDS y Amazon S3 de AWS.

Las instantáneas de Amazon RDS proporcionarán protección y acceso rápido a los datos de la base de datos, mientras que Amazon S3 ofrecerá almacenamiento seguro y escalable.

El costo mensual total de los respaldos será de 680 USD, con 570 USD destinados a Amazon RDS y 110 USD a Amazon S3.

1.2. Proyecto para garantizar el acceso seguro a los recursos de la aplicación

El propósito de este proyecto es aumentar la seguridad y dificultar los intentos de los atacantes de obtener datos o código de la aplicación, ya sea a través del robo de equipos, la obtención de credenciales mediante phishing, u otros métodos. Se incluyen en el alcance del proyecto todos los equipos proporcionados por ChaseMyCash a sus empleados.

Este proyecto implica una carga técnica significativa para fortalecer las medidas de acceso, lo cual será responsabilidad del equipo de IT. Además, será crucial proporcionar un curso de formación a los empleados para mejorar su conocimiento y conciencia sobre estos temas de seguridad.

- Actualización de la política de contraseñas: La política de contraseñas de ChaseMyCash será revisada y actualizada para incluir criterios más estrictos, como longitud mínima, caracteres especiales, evitar el uso de información personal, establecer periodos de caducidad, restringir el uso de contraseñas antiguas o comunes, y promover el uso de gestores de contraseñas. Se proporcionará formación regular a los empleados sobre la importancia de la seguridad de las contraseñas.

- Control de accesos y privilegios en el repositorio de Github: Se restringirá el acceso al repositorio únicamente a los desarrolladores y se utilizarán los roles proporcionados por Github para controlar los permisos.
- Gestión de roles: Se ajustarán los roles de los empleados para seguir el principio de mínimo privilegio, asignando únicamente los permisos necesarios para sus tareas.
- Activación de la autenticación en dos pasos: Se implementará la autenticación en dos pasos para los empleados que accedan a recursos clave, como el repositorio de código, la base de datos y el bucket.

El departamento liderado por el CTO y el equipo de IT, compuesto por un experto en cloud y un experto en criptografía, serán responsables de llevar a cabo las tareas técnicas. Mientras tanto, el departamento liderado por el CEO será responsable de diseñar y desarrollar el material educativo para los empleados. La colaboración entre estos departamentos, con el liderazgo del CTO y la coordinación del COO, será fundamental para el éxito del proyecto.

En cuanto a la temporización:

- La actualización de la política de contraseñas tomará una semana para establecer y definir los nuevos requisitos.
- Las tareas de control de accesos y privilegios al repositorio, así como la activación del segundo factor de autenticación, se llevarán a cabo en paralelo con la actualización de la política, estimando un mes para completarlas. Se considera que pueden surgir problemas en la definición de roles y permisos, por lo que se elaborará una guía para que los empleados activen el doble factor.
- La impartición del curso formativo se llevará a cabo después de la actualización de la política, en un plazo máximo de dos meses. El curso se impartirá en línea para facilitar el acceso a todos los empleados, quienes tendrán reuniones de seguimiento para resolver sus dudas.

En cuanto a los recursos necesarios, para la actualización de la política de contraseñas, se utilizará la guía NIST Password Guidelines como referencia. Para el control de accesos y privilegios del repositorio de Github, se utilizarán herramientas como Github Access Control y GitGuardian. Para mitigar el riesgo de dar permisos de administrador a todos los empleados en sus equipos, se puede implementar una solución de gestión de acceso privilegiado (PAM) como CyberArk. Para la activación del doble factor de autenticación, se utilizará Google Authenticator, una aplicación gratuita y fácil de usar que se puede descargar en los teléfonos de los empleados.

1.3. Proyecto para la integración de Firewall y WAF

El proyecto implica la implementación de un Firewall y un WAF (Web Application Firewall) para la empresa ChaseMyCash. El propósito es salvaguardar la red y las aplicaciones web de la compañía contra posibles ataques externos.

Las tareas son las siguientes:

Configuración del Firewall: Establecer reglas de seguridad para bloquear tráfico no deseado y restringir el acceso a la red. Definir políticas de seguridad para permitir el acceso a servicios y puertos necesarios.

Configuración del WAF: Proteger la aplicación web contra posibles ataques externos como inyecciones SQL, XSS, CSRF, etc. Definir reglas de seguridad y acciones a tomar en caso de detectar un ataque.

Auditoría de seguridad: Realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad, identificar vulnerabilidades y aplicar correcciones.

Mantenimiento y actualizaciones: Realizar mantenimiento regular y actualizaciones del Firewall y el WAF para garantizar su eficacia ante la evolución de la infraestructura y nuevas amenazas.

Se asignaran los siguientes responsables:

Se requerirá **personal especializado en seguridad informática** para la implementación, configuración y auditorías de seguridad. También se necesitará personal de TI capacitado para integrar el WAF con la aplicación web y realizar mantenimiento.

Se asignarán **dos expertos en ciberseguridad con experiencia en la nube, 2 arquitectos cloud y 1 experto en pruebas de penetración** para verificar la eficacia de la implementación.

En cuanto a la temporización:

- Selección de hardware y software: 1 semana.
- Configuración del Firewall: 2-4 semanas.
- Configuración del WAF: 2-4 semanas.
- Integración del WAF con la aplicación web: 1-2 semanas.
- Auditoría de seguridad: Se realizará durante la configuración del WAF.
- Mantenimiento y actualizaciones: 1-2 días por mes.

En total, se estima un plazo de 12 a 16 semanas (3-4 meses) para completar todas las tareas.

Los recursos necesarios serán:

- Se requerirá presupuesto para la adquisición de hardware y software.
- Se utilizará el servicio de AWS Network Firewall para el Firewall y AWS WAF para el WAF, que ofrecen control detallado del tráfico de red y protección de aplicaciones web respectivamente.

1.4. Proyecto de implementación de una solución combinada de seguridad (SIEM,EDR y NDR).

El proyecto elegido implica la implementación de una solución de seguridad combinada, que incluye Wazuh como SIEM (Security Information and Event Management) y EDR (Endpoint Detection and Response), la pila ELK como plataforma de análisis de logs y Suricata como NIDS (Network Intrusion Detection System). Este proyecto se caracteriza por su ambición en abordar múltiples aspectos de la seguridad de la información y la detección de amenazas.

Selección de herramientas:

Se eligieron Wazuh, ELK Stack y Suricata debido a su funcionalidad, compatibilidad entre herramientas, nivel de soporte y documentación disponible. Estas herramientas cumplen con los requisitos necesarios para la solución buscada.

Instalación y configuración de Wazuh:

Se seguirán los pasos para instalar y configurar Wazuh, incluyendo la descarga de la distribución todo en uno, instalación en un servidor adecuado, configuración de la comunicación con ELK para análisis de logs, monitorización de eventos en sistemas y red, y configuración de alertas para comportamientos anómalos.

Integración de Suricata:

Suricata, un NIDS de código abierto, se integrará con Wazuh. Esto incluirá la descarga e instalación de Suricata en los sistemas a monitorear, configuración para enviar logs a Wazuh, y definición de alertas para intrusiones detectadas.

Configuración de políticas de seguridad:

Se configurarán políticas de seguridad esenciales para proteger la infraestructura y datos de la empresa, como políticas de contraseñas seguras, reglas de firewall, autenticación multifactor, permisos de usuarios y grupos, y políticas de actualización de sistemas y software.

El CTO y tres especialistas en CERT/SOC serán responsables de llevar a cabo el proyecto, incluyendo infraestructura e ingeniería, monitorización y respuesta ante incidentes.

Temporización:

- Se estima que la implementación completa tomará aproximadamente 6 meses, incluyendo la selección de herramientas, instalación de Wazuh con ELK Stack, integración de Suricata, configuración de políticas de seguridad, y capacitación de empleados.

Recursos necesarios:

- Se necesitarán servidores con suficiente capacidad, un sistema operativo compatible, y capacitación para el personal en el uso de la solución. La solución propuesta es gratuita y fácil de implementar al ser herramientas de código abierto con amplia documentación y soporte comunitario. La utilización de una distribución todo en uno simplifica aún más la implementación.

2. Análisis de riesgos con FAIR.

	BRECHA DE DATOS DE CODIGO	BRECHA DE DATOS DE CLIENTES	RANSOMWARE	DoS
IMPLEMENTACION DE COPIAS DE SEGURIDAD	Mejora media	Mejora media	Mejora alta	Mejora alta
GARANTIZAR ACCESO SEGURO	Mejora alta	Mejora alta	Mejora alta	Mejora media
INTEGRACION DE FIREWALL	Mejora baja	Mejora media	Mejora media	Mejora alta
IMPLEMENTACION SIEM	Mejora baja	Mejora media	Mejora media	Mejora media
<div><div></div> Mejora alta</div> <div><div></div> Mejora media</div> <div><div></div> Mejora baja</div>				

2.1 Evaluación del riesgo.

En este caso no vamos a repetir el FAIR por completo por lo que vamos indicar solo las cosas que hemos cambiado y el resto significa que lo hemos dejado igual. Aquellos puntos que han sufrido algún cambio significativo se resaltan en **naranja**, por el contrario, los apartados que no sufren cambios se reutilizan de la práctica 1.

2.1.1. Brecha de datos del código

Objetivo

El objetivo es estimar la probabilidad e impacto asociados que tendrá nuestra empresa ChaseMyCash en caso de sufrir una brecha de datos debido a un posible acceso no autorizado.

Contexto

Durante un análisis de seguridad llevado a cabo por la empresa, se descubrió que los empleados tenían privilegios de administrador. Esto implicaba que un empleado tenía la capacidad de descargar un archivo infectado con malware en su computadora portátil de trabajo. Este escenario plantea la posibilidad de que un atacante remoto pudiera acceder a la red corporativa y comprometer el código fuente de la aplicación.

Activos

Los activos en riesgo frente a la eventualidad de este incidente incluyen principalmente el código de la aplicación alojado en GitHub, el cual engloba toda la lógica de la aplicación. Otro activo afectado sería la reputación de la compañía, así como la información sensible, dado que el código de la aplicación podría contener datos confidenciales.

Adversario

El potencial adversario podría ser un ciberdelincuente o un grupo cibercriminal con el objetivo de obtener información valiosa del código de la aplicación para su beneficio personal o para perjudicar la reputación de la compañía.

Tipo de amenaza

La naturaleza de la amenaza es maliciosa, ya que los adversarios no deberían tener acceso al código bajo ningún concepto. Por lo tanto, la única manera de obtener acceso sería a través de una intrusión no autorizada en un dispositivo.

Impacto de la amenaza

Principalmente, este riesgo impacta en la confidencialidad, dado que la información del código de la aplicación puede ser expuesta y comprometida. Asimismo, puede afectar a la integridad, ya que el código de la aplicación podría ser modificado por un atacante, lo que conlleva a un comportamiento no deseado de la aplicación. Por último, podría influir en la disponibilidad, dado que una brecha de datos podría resultar en la interrupción del servicio o en la pérdida de datos.

Alcance

Activo en riesgo	Adversario	Tipo de amenazas	Impacto de la amenaza
Código de la aplicación	Persona/Grupo externo	Intención maliciosa	Confidencialidad
Código de la aplicación	Persona/Grupo externo	Intención maliciosa	Integridad
Código de la aplicación	Persona/Grupo externo	Intención maliciosa	Disponibilidad

Análisis

Frecuencia de contacto al año

Dado que los empleados utilizan portátiles y aplicaciones/servicios de terceros para llevar a cabo sus tareas, la frecuencia de contacto al año es alta, lo que aumenta las oportunidades de una brecha de datos que pueda afectar al código de la aplicación.

Para salvaguardar la seguridad de la propiedad intelectual de ChaseMyCash, se ha definido una métrica llamada Frecuencia de Acceso, que se refiere al número de veces que terceros acceden de manera no autorizada al código de la aplicación. Tras un extenso análisis y discusión, se determinó que el número promedio de accesos no autorizados al código sería de 2 por año, considerando diversas posibilidades de vulnerabilidad como el robo de portátiles empresariales y la presencia de malware en los equipos.

Además, se ha establecido un límite máximo de 5 accesos no autorizados al código por año, con el objetivo de reducir el riesgo de exposición y pérdida de la propiedad intelectual de ChaseMyCash. Se

ha acordado también que la frecuencia mínima de incidentes sería de al menos una vez cada tres años, lo que permitirá a ChaseMyCash identificar y abordar cualquier debilidad en sus sistemas de seguridad, garantizando así la protección continua de su propiedad intelectual.

Probabilidad de Acción

Existen diversas formas en las que un adversario podría intentar obtener acceso al código de la aplicación, incluyendo el phishing, el malware, la explotación de vulnerabilidades o el robo del dispositivo.

Dado que no todos los empleados de la empresa son programadores y, por lo tanto, no todos necesitan acceso al código, se ha limitado considerablemente la probabilidad de acción. Con 9 programadores dentro de una organización de un total de 18 empleados, el máximo de acceso al código se estableció en un 50%, ya que la mitad de los empleados tendrían dicho acceso. Considerando esta limitación y el hecho de que estos empleados pueden estar sujetos a medidas de seguridad adicionales, como la autenticación multifactorial, se podría establecer un porcentaje medio del 25%. Además, se establece un porcentaje mínimo del 10%, reconociendo que siempre existe la posibilidad de que un adversario logre acceder al código de la aplicación, independientemente de las medidas de seguridad implementadas.

Capacidad de Amenaza

La capacidad de amenaza puede variar significativamente, ya que depende de la habilidad y los recursos del adversario. Sin embargo, se considera que puede ser alta debido a la presencia de numerosos actores malintencionados interesados en obtener información valiosa del código de la aplicación. Si tomamos en cuenta que el atacante posee conocimientos avanzados en ciberseguridad, la capacidad de amenaza aumentaría considerablemente, ya que es probable que requiera menos tiempo para acceder a dicha información sensible o valiosa.

Por lo tanto, se establece un rango de probabilidad de entre el 30% y el 90% para reflejar esta variabilidad en la capacidad de amenaza.

Fuerza resistencia.

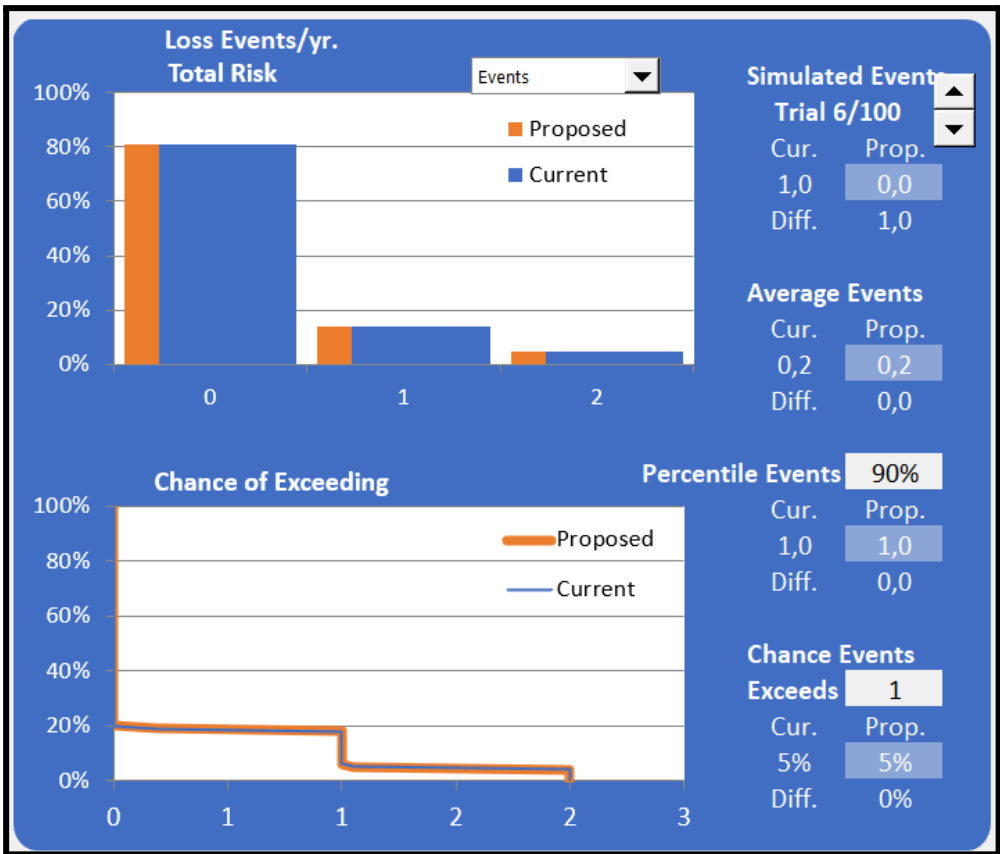
Al determinar los estándares de seguridad para esta área en particular, se ha priorizado evitar la extracción y eliminación del código en caso de que el dispositivo sea accedido por personas no autorizadas. Se ha concluido que únicamente dos medidas pueden garantizar esto: la autenticación del usuario al iniciar sesión en el dispositivo y las credenciales de GitHub. Después de implementar mejoras, se ha fortalecido la política de contraseñas, se ha optimizado la gestión de roles y accesos al repositorio de GitHub, además de incorporar autenticación de doble factor. Todo esto aumenta la complejidad para que un tercero no autorizado acceda al código. Para garantizar una protección adecuada, se ha establecido un rango de resistencia del 55% al 70%, con un valor más probable del

62%. De este modo, se busca asegurar que, incluso en caso de robo del dispositivo y compromiso de las medidas de seguridad, el código pueda protegerse en gran medida.

RESUMEN DE VALORES UTILIZADOS

Contact Frequency/yr.			Probability of Action			Threat Capability			Resistance Strength		
	Cur.	Pro.		Cur.	Pro.		Cur.	Pro.		Cur.	Pro.
Min	0		Min	10%		Min	30%		Min	55%	
ML	2		ML	25%		ML	60%		ML	62%	
Max	5		Max	50%		Max	90%		Max	70%	

ANÁLISIS DE PROBABILIDADES DE OCURRENCIA



Conclusiones:

- El código de la aplicación de ChaseMyCash será robado una vez cada 10 años.
- La probabilidad de que suceda al menos 1 evento de este tipo al año es del 5%.

- La probabilidad de que no suceda ningún evento de este tipo al año es del 17%

Impacto

Pérdidas Primarias

Productividad: Anticipamos una ligera disminución en la productividad, ya que, después de implementar mejoras, las copias de seguridad se realizan manualmente a intervalos frecuentes utilizando GitHub, siguiendo una política establecida que requiere hacer una copia al finalizar cada sprint o mes. Esto significa que, en caso de un error catastrófico, podría perderse parte del trabajo realizado durante ese periodo si la última copia de seguridad no se ha completado. No sería necesario que todos los empleados dediquen tiempo completo a la recuperación, sino que bastaría con incorporar los cambios más recientes. Se estima que se necesitarán solo 2 desarrolladores, lo que resultará en un costo promedio de alrededor de 5000€ debido al retraso en el proyecto.

Reemplazo: Para agilizar la producción, no será necesario contratar personal adicional, pero se ofrecerá un incentivo a los empleados encargados de la recuperación. Se estima que los costos promedio serán de 2000€.

Respuesta: Dado que contamos con personal capacitado para realizar pruebas de intrusión, no se requerirá ningún gasto adicional para llevar a cabo estas pruebas.

Pérdidas secundarias

Probabilidad de pérdida secundaria:

Como pérdida secundaria, se considera el impacto en la imagen y la reputación de la empresa, que sufriría un daño significativo como resultado de estos eventos. Se estima que en el 50% de las ocasiones será necesario emplear recursos adicionales para mitigar los efectos adversos en la imagen y la reputación de la empresa.

Respuesta:

La contratación de un proyecto forense con el fin de determinar las causas del incidente y prevenir su recurrencia implica gastos adicionales de respuesta. Se estima que el gasto promedio para este tipo de contratación será de unos 15.000€.

Reputación:

Los gastos relacionados con la reputación se centran en la captación de nuevos clientes. Esta tarea sería difícil debido a que se generarían sentimientos de desconfianza entre los usuarios existentes. Por lo tanto, será necesario destinar recursos adicionales para atraer nuevos clientes, como campañas de marketing u ofertas en las diferentes licencias del producto, con un costo promedio estimado de 3.500€.

Se prevé que los clientes más antiguos o las entidades relacionadas con la empresa seguirán

siendo leales. Sin embargo, se estima una pérdida promedio de 30.000€ debido a la pérdida del 5% de los clientes que utilizan las licencias más económicas.

Ventaja competitiva:

La capacidad de querer destacar frente a otras empresas será complicado de implementar ya que se verá estancado durante los 2 meses que se están invirtiendo para reconstruir el código de la app. En este tiempo se prevé que 250 clientes nuevos con un precio medio de 50€ por suscripción lo que sería 12.500€.

Juicios:

Los procedimientos legales estarán condicionados por los resultados obtenidos de la prueba forense. Si se demuestra que el incidente fue provocado por una empresa externa, se iniciará un proceso judicial. Se ha establecido un valor promedio para este tipo de acciones legales en 15.000€.

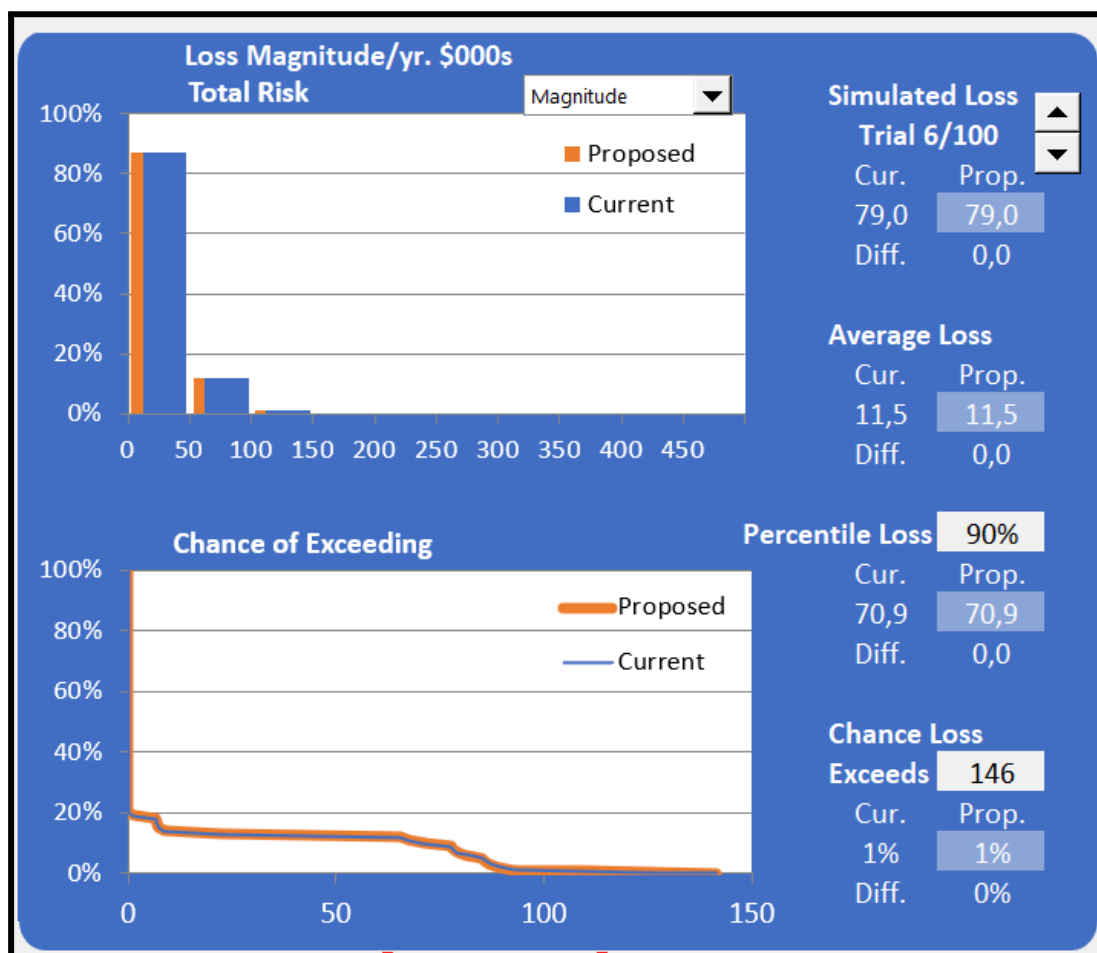
RESUMEN DE VALORES UTILIZADOS

Primary Loss Magnitude			
Current	Min	ML	Max
Productivity	4	5	6
Replacement	1	2	3
Response	0	0	0
Reputation			
Competitive Adv.			
Judgments			
Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Secondary Loss Magnitude			
SLEF	Min	ML	Max
Current	30%	50%	70%
Proposed			
Current	Min	ML	Max
Productivity			
Replacement			
Response	3	9	15
Reputation	23	35	45
Competitive Adv.	3	10	20
Judgments	10	15	20
Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Copyright © 2018 The Open Group®. All Rights Reserved.

ANÁLISIS COSTE ESTIMADO



Conclusiones

- El coste medio que va a suponer para las arcas de ChaseMyCash es de 11.500€ al año.
- A la vista de los datos, el coste máximo que puede tener al cabo del año ronda los 146.000€, es decir, más del doble de lo que ChaseMyCash genera anualmente

2.1.2. Ransomware

Objetivo

El objetivo es estimar la probabilidad e impacto asociados que tendrá nuestra empresa ChaseMyCash en caso de que un ransomware se propague por nuestra empresa debido a un acceso no autorizado, por un dispositivo externo a la empresa o bien por culpa de algún empleado.

Contexto

Visto que la empresa ChaseMyCash no proporciona móviles corporativos y se permite a los empleados el uso de sus propios teléfonos móviles para trabajar nos deja ver un posible vector de entrada de amenazas para la compañía ya que los teléfonos móviles personales no están configurados con las medidas de seguridad requeridas por la empresa. Además, al no ser un dispositivo de la empresa, esta no tendrá el control total sobre el mismo para poder proteger la posible información confidencial y sensible perteneciente a la empresa.

Activos

Los posibles activos en riesgo serán tanto los dispositivos personales de los empleados como todo lo relacionado con el código de la aplicación, la información sensible de la empresa que tenga almacenada en el teléfono personal y la reputación corporativa.

Adversario

Los posibles adversarios podrían ser tanto atacantes solitarios como grupos de ciberdelincuentes que buscan beneficio económico pidiendo rescate, dañar la imagen de la empresa o simplemente destruir datos.

Tipo de amenaza

El ransomware se clasifica como una amenaza perjudicial y deliberada, ya que tiene como objetivo obtener ganancias económicas mediante la extorsión a la víctima. El perpetrador suele emplear tácticas como el correo electrónico fraudulento o la explotación de vulnerabilidades en la infraestructura de red de la empresa para introducir el software malicioso y encriptar los archivos.

Impacto amenaza

Un ataque de ransomware puede incidir en múltiples aspectos fundamentales de la ciberseguridad. En primer lugar, la accesibilidad de los datos de la empresa se ve gravemente comprometida, dado que los archivos encriptados quedan inaccesibles para el personal. Además, la confidencialidad de la información sensible de los usuarios se ve comprometida, puesto que los atacantes pueden acceder a los datos cifrados. Por último, la integridad de los datos corre peligro si los archivos encriptados no pueden ser recuperados o si los atacantes optan por filtrarlos o eliminarlos. En general, un ataque de ransomware puede generar repercusiones económicas, operativas y de reputación significativas para la empresa afectada.

Alcance

Datos de ChaseMyCash se refiere a tanto código de la aplicación como a la información sensible.

Activo en riesgo	Adversario	Tipos de Amenaza	Impacto de la amenaza
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Integridad
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Confidencialidad
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Disponibilidad
Dispositivos y servicios ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Disponibilidad

Análisis

Frecuencia de contacto.

En este caso, la frecuencia de contacto se define como la cantidad de horas que los empleados utilizan sus dispositivos personales para acceder a servicios o sistemas internos de ChaseMyCash. Esta evaluación se ha llevado a cabo mediante una serie de cuestionarios dirigidos a todos los empleados, donde se especifica que, durante un año laboral típico, los dispositivos personales se utilizan durante aproximadamente 1000 horas (equivalentes a 41,66 días). Basándose en esta medida, se establece un mínimo de 500 horas al año (equivalente a 20,83 días) y un máximo de 1500 horas al año (equivalente a 62,5 días).

Probabilidad de acción.

La "probabilidad de acción" se define como la posibilidad de que un empleado cometa un error de seguridad que resulte en la propagación de malware dentro de la empresa. Dado que ChaseMyCash no ofrece dispositivos con configuración empresarial, es probable que muchos de los dispositivos utilizados por los empleados carezcan de las medidas de seguridad adecuadas, como la falta de software antivirus. Es altamente probable que los requisitos mínimos de seguridad necesarios para proteger los datos tanto de la empresa como de sus clientes no se cumplan. Por lo tanto, se establece que el porcentaje mínimo de esta probabilidad sea del 15%, con un promedio del 25% y un máximo del 35%.

Capacidad de amenaza

Dado que estamos estimando la probabilidad y el impacto asociado a un ransomware nos basaremos en las estadísticas oficiales de Sophos de 2023. 50% (Percentage of Organizations Hit by Ransomware In the Last Year). Vamos a establecer este valor como el máximo, siendo el promedio 33% y el mínimo 16%.

Fuerza Resistencia

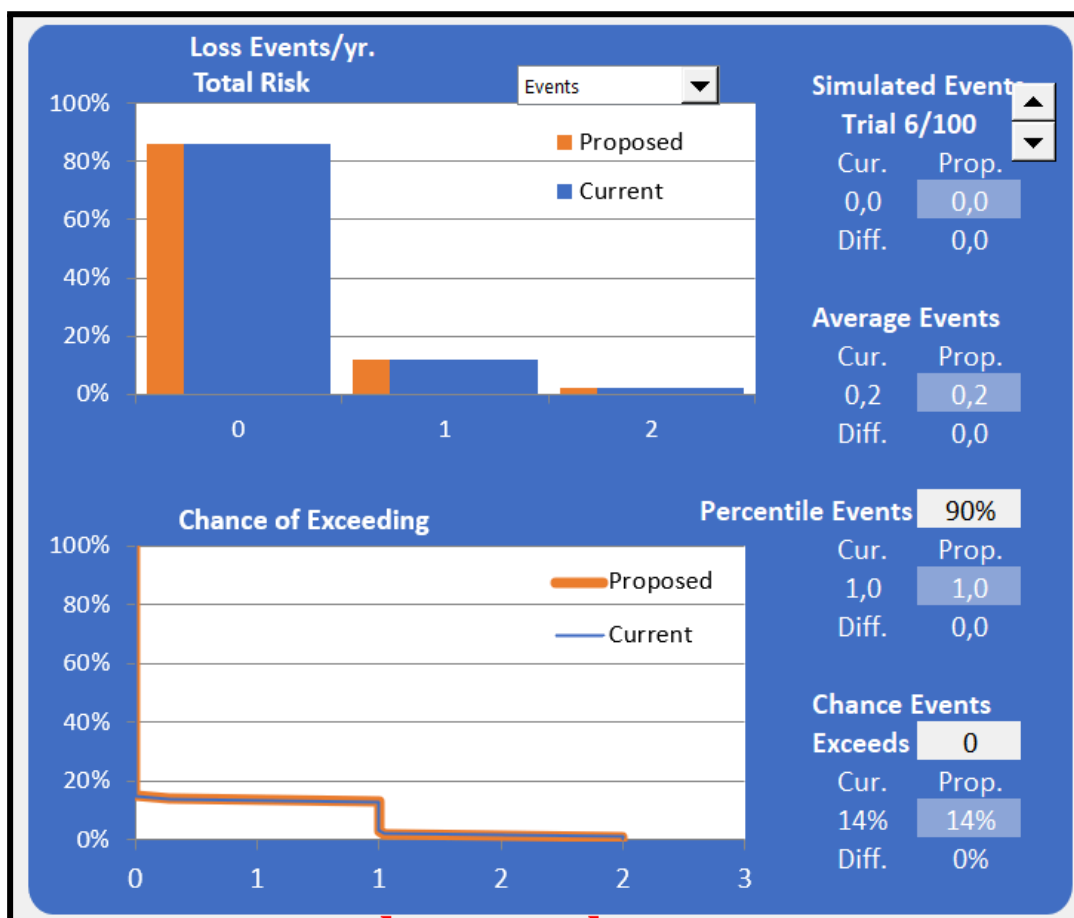
Después de completar todas las tareas de los distintos proyectos, hemos abordado el problema desde la protección de la red y la aplicación hasta la detección y respuesta a amenazas avanzadas. Como resultado, la combinación de todos nuestros proyectos nos permite prevenir de alguna manera la pérdida de datos críticos, reducir al mínimo el impacto de una infección de ransomware y proteger la empresa contra el pago de rescate a los atacantes.

En consecuencia, los valores definidos son: un máximo del 70%, un promedio del 60% y un mínimo del 40%.

RESUMEN VALORES UTILIZADOS

Contact Frequency/yr.	Probability of Action	Threat Capability	Resistance Strength
Cur. Pro.	Cur. Pro.	Cur. Pro.	Cur. Pro.
Min 21	Min 15%	Min 16%	Min 40%
ML 42	ML 25%	ML 33%	ML 60%
Max 63	Max 35%	Max 50%	Max 70%

ANÁLISIS PROBABILIDAD DE OCURRENCIA



CONCLUSIONES

- Se observa que ChaseMyCash recibe de media 1 propagación de ransomware cada 5 años.
- La probabilidad de que no haya ninguna propagación al año es del 14%.
- La probabilidad de que suceda al menos 1 evento de este tipo al año es del 2%

Impacto

Pérdidas primarias

Productividad:

El porcentaje de dinero que no se recibe durante un mes por parte del coste de las licencias de los clientes se ha calculado siguiendo las siguientes estimaciones: Se ha deducido que de los 20.000 clientes el 20% (4.000 clientes) tienen la licencia Premium (100€/año -> 8,33 €/mes), el 30% (6.000 clientes) tienen la licencia Large (75€/año aprox. -> 6,25€/mes). Otro 20% (4.000 clientes) tiene la licencia Medium (50€/año -> 4,16€/mes y el 30% restante (6.000 clientes) tienen la licencia Small

(20€/año -> 1,66 €/mes).

Por tanto, ChaseMyCash dejaría de ganar como máximo durante ese mes 97.420€, un promedio de 75.720€/mes (10% Premium, 10% Large, 40% Medium, 40% Small) y un mínimo (20% Large, 30% Medium y 50% Small) de 66.290€/mes.

Para evitar lo máximo posible esta pérdida de productividad se ha pedido a los empleados que hagan horas extras hasta un máximo de 4 horas al día. Siendo estas horas extras pagadas a 35€/hora. Según los datos recogidos en el informe oficial sobre ransomware de Sophos se tarda de media un mes en recuperarse de un ransomware, por lo que el precio promedio en caso de que los 9 empleados de IT hagan las 50 horas extra/mes aproximadamente sería de 15.750€/mes. En el caso máximo de 80 horas extra/mes sería de 25.200€ y el mínimo 20 horas extra/mes de 6.300€.

Reemplazo:

Por norma general el ransomware no ocasiona la necesidad de reemplazo de personal o equipos. Por los que estableceremos un valor mínimo de 2.000€, un valor medio de 5.000€ y un máximo de 7.500€.

Respuesta:

El costo promedio de responder al ransomware puede variar considerablemente dependiendo de la gravedad del ataque y la extensión del daño causado. Por lo general, este costo incluirá el pago del rescate (si se opta por hacerlo), la eliminación del ransomware, la restauración de los datos afectados y la implementación de medidas de seguridad adicionales para prevenir futuros ataques. Se estipula que el costo máximo será de 30.000€, con un promedio de 20.000€ y un mínimo de 10.000€.

Pérdidas secundarias

Probabilidad de pérdidas secundarias:

Dado el mayor riesgo asociado con el uso de dispositivos personales por parte de los empleados, se ajustan los porcentajes para reflejar esta mayor probabilidad. Se establece que la probabilidad mínima de ocurrencia de pérdidas secundarias sea del 20%, con un promedio del 40% y un máximo del 60%.

Respuesta:

Con el objetivo de mitigar las pérdidas secundarias y reducir la probabilidad de futuros ataques de ransomware, se tomará la decisión de adquirir dispositivos móviles empresariales para todos los empleados, los cuales contarán con las medidas de seguridad necesarias. Se ha establecido que el costo mínimo de esta inversión será de aproximadamente 4000€, con un promedio de 6000€ y un máximo de 8000€.

Reputación:

Relacionado con la probabilidad de pérdida secundaria, los costos de reputación se enfocarán en la adquisición de nuevos clientes, lo cual podría resultar desafiante debido a la creación de desconfianza entre los usuarios. Por lo tanto, se requerirá la asignación de recursos adicionales para la captación de nuevos clientes, como campañas de marketing u ofertas en las diversas licencias del producto, con un costo promedio estimado de 3.000€. Se prevé que los clientes más antiguos o aquellos asociados directamente con la empresa seguirán siendo leales. Sin embargo, se estima una pérdida promedio de 20.000€ debido a la pérdida del 5% de los clientes con las licencias más económicas.

Ventaja competitiva:

Un ataque de ransomware puede tener un impacto significativo en la capacidad operativa de una empresa, lo que a su vez podría afectar su posición competitiva. Por ejemplo, si una empresa se ve imposibilitada de acceder a sus datos y sistemas durante un período prolongado, podría perder la capacidad de cumplir con los pedidos de los clientes o de responder de manera ágil a las demandas del mercado, lo que potencialmente permitiría a los competidores ganar una ventaja competitiva.

Por tanto, se han establecido valores para cuantificar este impacto. El costo máximo de este impacto se estima en 9.000€, con un promedio de 6.000€ y un mínimo de 3.000€.

Juicios:

Es crucial considerar que el enjuiciamiento de los autores de ransomware puede ser un proceso complejo, costoso y prolongado, que podría requerir la participación de varios departamentos gubernamentales y agencias de aplicación de la ley. El costo promedio asociado a este proceso se estima en 15.000€.

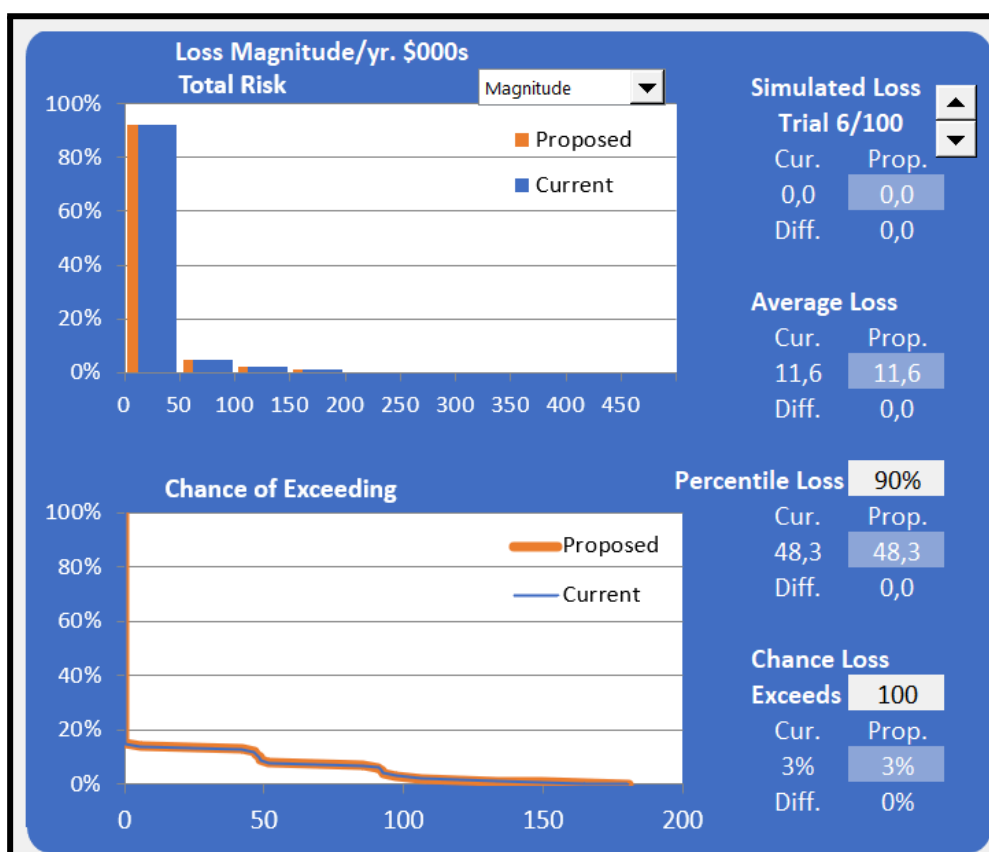
RESUMEN DE VALORES UTILIZADOS

Primary Loss Magnitude			
Current	Min	ML	Max
Productivity	8	16	25
Replacement	2	5	8
Response	10	20	30
Reputation			
Competitive Adv.			
Judgments			
Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Secondary Loss Magnitude				
SLEF	Current	Min	ML	Max
	Proposed	20%	40%	60%
Current		Min	ML	Max
Productivity				
Replacement				
Response		4	6	8
Reputation		16	23	32
Competitive Adv.		3	6	9
Judgments		10	15	20
Proposed		Min	ML	Max
Productivity				
Replacement				
Response				
Reputation				
Competitive Adv.				
Judgments				

Copyright © 2018 The Open Group®. All Rights Reserved.
SaaS FAIR™ is a trademark of The Open Group.

ANÁLISIS COSTE ESTIMADO



CONCLUSIONES

- El coste medio que va a suponer para ChaseMyCash es de 11.600€ al año.
- La probabilidad de que en un año este incidente genere pérdidas de más de 100.000 euros es del 3%.
- A la vista de los datos, el coste máximo que puede tener al cabo del año ronda los 185.000 euros

2.1.2. Brecha de datos de clientes

Objetivo

El propósito es detectar los riesgos y consecuencias potenciales vinculados a una eventual filtración de información confidencial del cliente, originada por un acceso no autorizado tanto a la base de datos como al servicio de almacenamiento

Contexto

Durante una revisión interna de pruebas de penetración, los informes revelaron un hallazgo preocupante: se encontraron ciertos puertos accesibles desde el exterior, incluido el puerto 3306.

Además, se observó que el servicio de almacenamiento utilizado (bucket de Amazon S3) estaba configurado de manera que no cifraba ningún elemento almacenado en él. Este informe se calificó como extremadamente grave.

Activos en riesgo

Los datos en riesgo incluyen toda la información necesaria para iniciar sesión de los usuarios (nombres de usuario, correos electrónicos, contraseñas, roles, permisos, etc.), así como información personal relacionada con sus objetivos, preferencias y alertas configuradas. Además, los archivos XLS o CSV cargados por los usuarios, así como archivos que contienen facturas, declaraciones de impuestos y otros documentos similares almacenados en el bucket, también están en peligro. Esta situación afectará no solo a la información sensible, sino también a la reputación tanto del cliente como de la compañía.

Adversario

El adversario puede ser cualquier individuo o grupo que busque obtener acceso no autorizado a la información almacenada en la base de datos de la empresa. Esto podría incluir hackers, empleados deshonestos o cualquier persona con acceso a la red o los dispositivos de la empresa. Además, no se puede descartar la posibilidad de que un empleado con acceso legítimo tenga intenciones maliciosas.

Tipo de amenaza

La amenaza puede darse de forma accidental, como cuando un empleado no sigue los procedimientos de seguridad establecidos o debido a debilidades en el software utilizado. Lo que podría resultar en una filtración de datos. Sin embargo, en la mayoría de los casos, el peligro proviene de un ataque deliberado por parte de un hacker informático que busca acceder a información confidencial y comprometer la seguridad de la empresa.

Impacto de la amenaza

Una violación de datos de clientes tiene un impacto primordial en la confidencialidad, ya que la información personal de los clientes corre el riesgo de ser comprometida, lo que potencialmente puede amenazar su privacidad y seguridad. En términos de integridad, los datos almacenados en la base de datos pueden ser alterados o eliminados, lo que podría resultar en pérdidas de información crítica. Por último, en lo que respecta a la disponibilidad, una brecha de datos de clientes podría resultar en una negación de servicio, ya que los sistemas de la empresa podrían verse afectados y no estar disponibles para su funcionamiento normal.

Alcance

ACTIVO EN RIESGO	ADVERSARIO	TIPO DE AMENAZAS	IMPACTO DE LA AMENAZA
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Confidencialidad
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Integridad
Datos de ChaseMyCash	Persona/Grupo externo	Intención maliciosa	Disponibilidad

ANÁLISIS.

Frecuencia de contacto al año.

Según la definición en la tabla anterior, los agentes involucrados en estas actividades son externos. Por esta razón, la frecuencia de contacto se ha definido como el número de consultas o intentos de acceso a la base de datos desde direcciones IP no registradas en la lista blanca, es decir, desde dispositivos o redes externas que no han sido previamente autorizadas y que podrían ser potencialmente maliciosas. Dado que el puerto 3306 está expuesto a Internet y que ningún elemento almacenado en el bucket de S3 está cifrado, es posible que los atacantes intenten acceder a la base de datos en busca de información valiosa de los clientes. Por lo tanto, se estima que la frecuencia media de intentos de acceso no autorizado podría ser de 50 intentos por día, lo que equivaldría a un promedio de 18.250 intentos de acceso no autorizado por año.

Probabilidad de acción.

Hemos identificado diversas amenazas relacionadas con este riesgo. Desde un atacante que obtiene acceso a datos no autorizados hasta posibles empleados que puedan filtrar algún tipo de información. Dado que hay varias formas de lograr el mismo objetivo y considerando ciertas debilidades en la empresa, hemos establecido un valor promedio moderado del 40% para estas amenazas.

Capacidad de amenaza.

Por un lado, si el atacante posee un alto nivel de habilidades técnicas, podría aprovechar una configuración de seguridad inadecuada para explotar vulnerabilidades y obtener así información valiosa de la base de datos de clientes. Por lo tanto, la capacidad de amenaza dependerá de la motivación y habilidades del atacante. Considerando todos estos aspectos, estimamos que la capacidad de amenaza tendrá un porcentaje medio del 40%.

Fuerza de resistencia.

Se ha implementado el cifrado del bucket, aunque persiste la falta de una política para eliminar datos que ya no son necesarios o redundantes. Se han aplicado controles como el cifrado en reposo en AWS RDS y el uso de JSON Web Token para autenticación, junto con la gestión de permisos personalizados en ExpressJS, con el fin de reducir la posibilidad de una brecha de seguridad. Además, se ha fortalecido la política de contraseñas, se ha añadido autenticación de doble factor y se ha mejorado la gestión de roles. Se realizan copias de seguridad de los datos sensibles de manera regular.

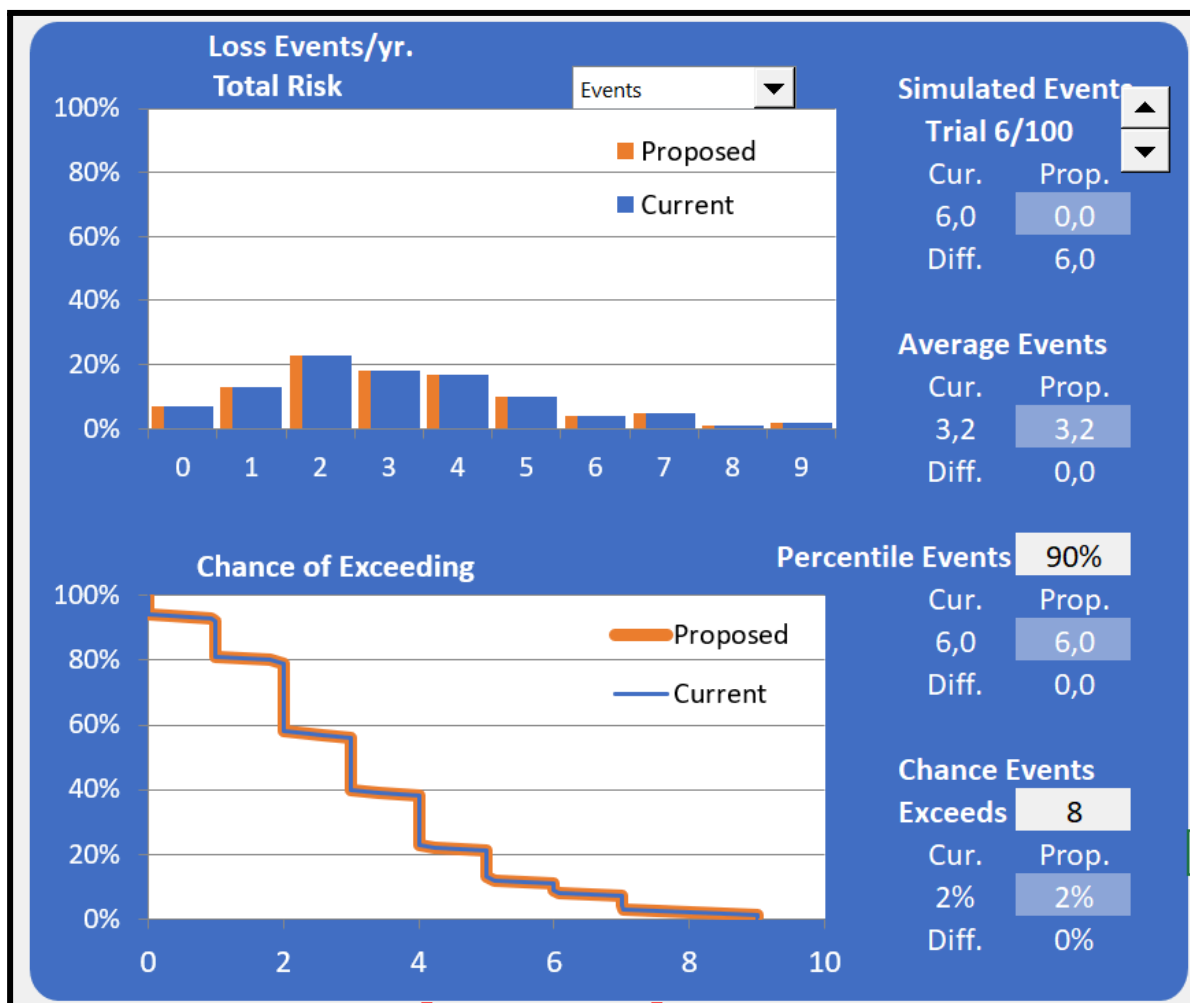
Uno de los principales riesgos sigue siendo el phishing y el robo de credenciales, aunque se espera reducirlo mediante la monitorización constante, permitiendo a los endpoints detectar tales intentos. Sin embargo, es importante tener en cuenta que esto no garantiza la prevención total, ya que los usuarios podrían caer en enlaces maliciosos que no siempre serán bloqueados. Lo mismo ocurre con los ataques web, como la inyección SQL, los ataques de scripting entre sitios (XSS), el recorrido de directorios y los intentos de fuerza bruta. El firewall y el WAF se encargarán de bloquear las solicitudes maliciosas que podrían exponer datos almacenados tanto en el bucket como en la base de datos.

Se estima que la resistencia a la intrusión tendrá un nivel medio del 40%.

RESUMEN VALORES UTILIZADOS

Contact Frequency/yr.	Probability of Action	Threat Capability	Resistance Strength
Cur. Pro.	Cur. Pro.	Cur. Pro.	Cur. Pro.
Min 8	Min 20%	Min 20%	Min 30%
ML 18	ML 40%	ML 40%	ML 40%
Max 28	Max 60%	Max 60%	Max 55%

ANÁLISIS PROBABILIDADES DE OCURRENCIA



CONCLUSIONES:

- Se observa que la información de clientes de ChaseMyCash será expuesta de media 3 veces al año.
- Es muy poco probable (un 2%) que en el mismo año ocurra 8 veces este incidente
- La probabilidad de que suceda al menos 1 evento de este tipo al año es del 80%.

IMPACTO

PÉRDIDAS PRIMARIAS:

Productividad: Cuando ocurren este tipo de incidentes, los programadores y otros miembros del equipo de tecnología de la empresa no necesitan invertir una cantidad significativa de tiempo y esfuerzo en resolver el problema. La identificación de la fuente de la brecha es más sencilla gracias a la monitorización, y la restauración de los datos comprometidos se facilita mediante los backups. Sin embargo, la capacidad de los programadores para llevar a cabo sus tareas diarias puede verse ligeramente comprometida, y la productividad de la empresa puede sufrir un impacto. Por lo tanto, se estima un costo promedio de productividad de 2000€

Reemplazo: En cuanto al reemplazo del personal, consideraremos valores bajos, ya que generalmente no es necesario sustituir al personal ante una situación de este tipo. Esto se debe a que no se considera que la falta de seguridad al 100% sea completamente culpa de los desarrolladores. Sin embargo, en el caso excepcional de que sea necesario, tendríamos que cubrir el salario de un nuevo empleado y el finiquito de la persona despedida. Por lo tanto, estimaremos un costo promedio de 10.000€, con un mínimo de 5.000€ y un máximo de 15.000€

Respuesta: La empresa ha tomado medidas adecuadas para fortalecer la seguridad de sus sistemas y datos, como el cifrado de los datos almacenados en el bucket S3. Sin embargo, la empresa podría enfrentarse a multas y sanciones por no proteger adecuadamente los datos de sus clientes o por no cumplir con las regulaciones de privacidad. Además, podría ser necesario pagar indemnizaciones a las personas afectadas por el robo de datos. Ante estos escenarios, establecemos un costo mínimo de 10.000€, un costo promedio de 25.000€ y un máximo de 45.000€.

PÉRDIDAS SECUNDARIAS

Probabilidad de pérdida secundaria

Entre ellos, destacan los costos de notificación y cumplimiento. La empresa podría incurrir en gastos significativos relacionados con la notificación a los clientes, la realización de investigaciones, la implementación de medidas de seguridad adicionales y el cumplimiento de las regulaciones. Por otro lado, los clientes afectados por la filtración de datos podrían presentar demandas contra la empresa por daños y perjuicios, lo que podría resultar en costos legales significativos y dañar aún más la reputación de la empresa. Por lo tanto, se ha estimado un valor promedio del 30% para estos costos secundarios.

Respuesta

Para evitar futuros ataques de este tipo, es importante que la empresa implemente medidas adicionales. Por ejemplo, se sugiere establecer políticas claras de eliminación de datos y configurar

copias de seguridad automáticas para asegurar que los datos críticos estén respaldados y eliminados de manera oportuna. Se estima un costo promedio de 4.000€ para implementar estas medidas, con un rango mínimo de 2.000€ y máximo de 6.000€.

Reputación

Tomando en cuenta una posible pérdida de reputación significativa, si la empresa emite un comunicado explicando el problema ocurrido, es probable que muchos clientes perciban a la empresa como vulnerable y poco confiable en términos de seguridad, lo que podría resultar en la pérdida de clientes. Ante esta situación, será necesario invertir recursos adicionales en la atracción de nuevos clientes, lo que podría incluir el desarrollo de estrategias de marketing específicas para recuperar la confianza del mercado y atraer a nuevos clientes. Estimamos un costo promedio de 4.000€ para implementar estas estrategias de recuperación de reputación y atracción de nuevos clientes.

Ventaja competitiva

Dado que se trata de información de clientes, es poco probable que la ventaja competitiva de la empresa se vea especialmente afectada, ya que estos datos no proporcionan ninguna información relevante para las empresas competidoras. Sin embargo, como consecuencia negativa, estas empresas competidoras podrían aprovechar la filtración de datos para desarrollar campañas publicitarias dirigidas específicamente a los clientes afectados.

Juicios

Dado que la información expuesta corresponde a datos de clientes, la empresa enfrentará gastos legales significativos. ChaseMyCash podría enfrentar multas por no cumplir con las regulaciones de privacidad, como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea. Estas multas podrían ser significativas y dependerán del número de usuarios afectados, la gravedad de la violación y la naturaleza de los datos expuestos. Además, la empresa podría enfrentar demandas por parte de los clientes cuyos datos se vieron comprometidos en la brecha. Los costos legales asociados pueden establecer un costo promedio estimado de alrededor de 30.000€ para cubrir estos gastos legales.

RESUMEN DE LOS VALORES UTILIZADOS

Primary Loss Magnitude

Current	Min	ML	Max
Productivity	1	2	3
Replacement	5	10	15
Response	10	25	45
Reputation			
Competitive Adv.			
Judgments			

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Secondary Loss Magnitude

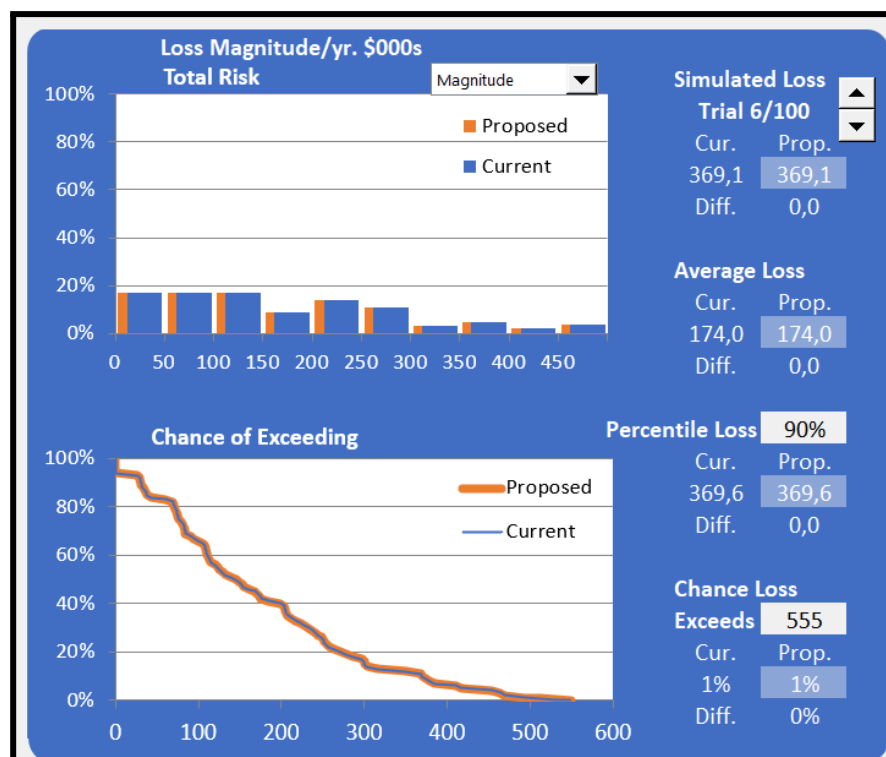
		Min	ML	Max
SLEF	Current	20%	30%	60%
	Proposed			

Current	Min	ML	Max
Productivity			
Replacement			
Response	2	4	6
Reputation	2	3	6
Competitive Adv.	4	6	8
Judgments	15	30	45

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Copyright © 2018 The Open Group®. All Rights Reserved.

ANÁLISIS COSTE ESTIMADO



CONCLUSIONES

- El coste medio que va a suponer para las arcas de ChaseMyCash es de 174.000€ al año.
- La probabilidad de que en un año este incidente genere pérdidas de más de 400.000€ es del 7%.
- A la vista de los datos, el coste máximo que puede tener al cabo del año ronda los 555.000€

2.1.3. Denegación de servicio

Objetivo

El objetivo es evaluar el riesgo de denegación de servicio provocado por la eliminación accidental de datos de la base de datos. Esto podría conducir a la pérdida de acceso a información sensible de los usuarios, como datos de inicio de sesión, información personal y detalles del producto. Es crucial analizar este riesgo para prevenir interrupciones en el servicio y salvaguardar la reputación tanto de la empresa como de sus clientes.

Contexto

La empresa ha identificado que la ausencia de una política de eliminación automática de elementos en la base de datos, junto con la realización manual de copias de seguridad, podría incrementar el riesgo de una eventual denegación de servicio en caso de un fallo en la base de datos.

Activos en riesgo

El activo en riesgo es la reputación de la empresa. Una denegación de servicio podría comprometer la disponibilidad del servicio y ocasionar insatisfacción entre los clientes, lo que eventualmente podría perjudicar la imagen y reputación de la compañía

Tipo de amenaza

En este caso, la amenaza podría ser tanto accidental como intencionada. Una eliminación accidental de la información de la base de datos podría ser causada por un error humano o técnico, mientras que una eliminación intencional podría ser causada por un usuario malintencionado o un atacante externo.

Impacto de la amenaza

En términos de integridad, una interrupción del servicio podría ocasionar la pérdida o corrupción de datos, lo cual afectaría la confiabilidad de la empresa. En relación a la disponibilidad, una denegación de servicio impactaría directamente la capacidad de la empresa para ofrecer sus servicios, lo que podría resultar en consecuencias financieras negativas.

Alcance

ACTIVO EN RIESGO	ADVERSARIO	TIPO DE AMENAZAS	IMPACTO DE LA AMENAZA
Servicios de ChaseMyCash	Persona/Grupo externo/interno	Intención maliciosa/accidental	Disponibilidad
Datos de ChaseMyCash	Persona/Grupo externo/interno	Intención maliciosa/accidental	Integridad

ANÁLISIS

Frecuencia de contacto al año

La frecuencia de contacto se interpreta como la cantidad de días al año en los que un usuario legítimo no puede acceder al servicio ofrecido por la empresa debido a una denegación de servicio, sin importar la causa. Esta métrica nos ayuda a evaluar la disponibilidad de la aplicación de la empresa.

En este contexto, la frecuencia de contacto se utiliza para valorar la calidad y fiabilidad de un servicio digital. Se ha establecido que, en promedio, la empresa no puede ofrecer sus servicios durante 12 días al año, con un mínimo de 6 días y un máximo de 24 días.

Probabilidad de acción.

La posibilidad de que un adversario lleve a cabo un ataque de denegación de servicio varía según varios factores, como la visibilidad de la empresa, la naturaleza de su actividad y si hay alguien motivado para realizar dicho ataque. Otros elementos que pueden contribuir a estos ataques incluyen fallas en la infraestructura, errores de programación y la falta de medidas de seguridad adecuadas, como la ausencia de políticas de copias de seguridad. Por consiguiente, la probabilidad media de que se produzca una acción de este tipo se estima en alrededor del 35%, con un mínimo del 20% y un máximo del 45%.

Capacidad de amenaza.

En general, la capacidad de amenaza en un ataque DDoS es alta, ya que los atacantes pueden aprovechar herramientas automatizadas para inundar el sistema con tráfico malintencionado y sobrecargar la infraestructura de la empresa, lo que podría resultar en una interrupción del servicio y dejar la aplicación inoperable. Además, los ataques DDoS están siendo cada vez más frecuentes y sofisticados, lo que implica que las empresas deben estar preparadas para enfrentar este tipo de amenazas y tomar medidas preventivas para reducir la probabilidad de interrupciones en el servicio. Por todo lo mencionado, la capacidad de amenaza se sitúa en un nivel moderado, con un valor promedio del 45%.

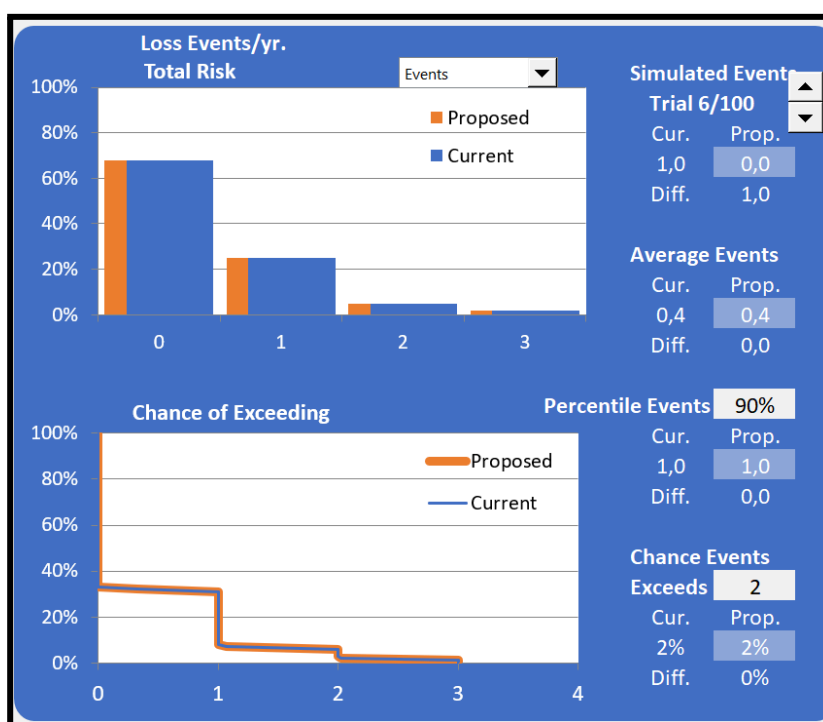
Fuerza de resistencia.

Tanto la implementación de un Firewall y WAF como la combinación de soluciones de seguridad (SIEM, EDR y NDR) pueden contribuir a prevenir ataques de denegación de servicio (DoS). El Firewall y el WAF tienen la capacidad de filtrar el tráfico de red malicioso y detectar comportamientos de tráfico anormales para evitar ataques DoS. Por otro lado, la solución combinada de seguridad puede detectar de manera temprana actividades maliciosas y responder rápidamente a los ataques DoS. En conjunto, estas soluciones son esenciales para prevenir ataques DoS y salvaguardar la red y los sistemas de la organización. Además, contar con copias de seguridad hace que la restauración de la base de datos borrada debido a una denegación sea fácilmente viable. Se estima un porcentaje medio de eficacia del 60%.

RESUMEN VALORES UTILIZADOS

Contact Frequency/yr.	Probability of Action	Threat Capability	Resistance Strength
Cur. Pro.	Cur. Pro.	Cur. Pro.	Cur. Pro.
Min 6	Min 20%	Min 35%	Min 50%
ML 12	ML 35%	ML 45%	ML 60%
Max 24	Max 45%	Max 65%	Max 70%

ANÁLISIS PROBABILIDADES DE OCURRENCIA



CONCLUSIONES

- ChaseMyCash sufrirá de tiempo de denegación de servicio, de media, 0.4 días cada año
- Es muy poco probable que haya más de 2 días de indisponibilidad al año, puesto que su probabilidad es inferior al 2%

IMPACTO

PÉRDIDAS PRIMARIAS

Productividad

Una denegación de servicio puede tener un impacto perjudicial en la productividad de una empresa, ya que puede afectar no solo los servicios en línea de la empresa, sino también sus procesos internos, como el correo electrónico, el intercambio de archivos y otras herramientas de colaboración. Esto puede conducir a la interrupción de la comunicación entre los empleados y a la desaceleración de los procesos internos, lo que a su vez puede afectar la productividad en general. Se estima un costo promedio asociado a esta pérdida de productividad de 15.000€

Reemplazo

Este tipo de ataque no suele ocasionar la necesidad de reemplazo de ningún equipo. En caso de que el borrado haya sido producido de manera intencional por parte de un empleado será necesario su despido, añadiendo a los gastos el finiquito además de la contratación de un nuevo empleado. Por lo tanto el coste medio será de unos 30.000€, el coste mínimo de 20.000€ y el coste máximo de 40.000€.

Respuesta

Es crucial que la empresa tome medidas adecuadas para mejorar la seguridad de sus sistemas y garantizar su disponibilidad. Para mitigar el riesgo de sufrir una denegación de servicio, la empresa ya ha implementado medidas de seguridad adicionales. Sin embargo, podría considerar contratar el servicio de AWS Shield, con un costo medio anual estimado de unos 37.200€, para obtener una solución aún más completa. En consecuencia, el costo total promedio sería de 30.000€, con un mínimo de 40.000€ y un máximo de 55.000€.

PÉRDIDAS SECUNDARIAS

Probabilidad de pérdida secundaria:

Cuando una empresa experimenta una denegación de servicio, las pérdidas secundarias pueden ser significativas. Además de la interrupción temporal de los servicios y la pérdida de productividad, la empresa puede enfrentar costos de recuperación. Esto implica invertir en tecnología y recursos adicionales para recuperarse del ataque, lo que conlleva costos adicionales.

Además, podría producirse la interrupción de operaciones críticas. Dado que la empresa depende de tecnología y sistemas críticos para sus operaciones diarias, una denegación de servicio podría interrumpir estos sistemas y causar problemas significativos.

Debido a estos factores, hemos calculado que dichas pérdidas secundarias se producirán, en promedio, el 35% de las veces.

Respuesta:

En cuanto a las respuestas secundarias después de una denegación de servicio, estas incluyen la actualización de software y sistemas, la implementación de medidas de seguridad adicionales y la capacitación del personal en seguridad informática. Por lo tanto, calculamos que el costo promedio de estas acciones sería de alrededor de 3.000€.

Reputación:

Consideramos que un deterioro significativo en el prestigio de la compañía podría ocurrir, ya que si la empresa emite una declaración para aclarar el incidente, es probable que muchos consumidores perciban a la organización como débil y poco confiable en términos de seguridad, lo que podría llevarlos a abandonarla.

Ante este escenario, será necesario asignar recursos adicionales para la captación de nuevos consumidores. Esto podría implicar la creación de estrategias de publicidad específicas destinadas a atraer a nuevos clientes y restaurar la confianza en el mercado. Se estima que el costo promedio de estas acciones sería de 5.000€.

Ventaja competitiva:

Una denegación de servicio puede impactar significativamente la capacidad de la empresa para cumplir con sus compromisos adquiridos con los clientes. El tiempo de inactividad resultante puede afectar la percepción de la empresa por parte de los clientes y disminuir su confianza en la misma. Esto podría resultar en la pérdida de clientes y una reducción en las ventas. Además, si la empresa no logra recuperarse del ataque de manera efectiva, podría perder su ventaja competitiva en el mercado, ya que los clientes podrían optar por competidores que puedan ofrecer servicios similares sin interrupciones. Se estima que el costo promedio de estos impactos sería de 20.000€.

Juicios:

Si se logra identificar la fuente de la denegación de servicio, es posible emprender acciones

legales. Se estima que el costo medio aproximado de tales acciones legales sería de 4.000€.

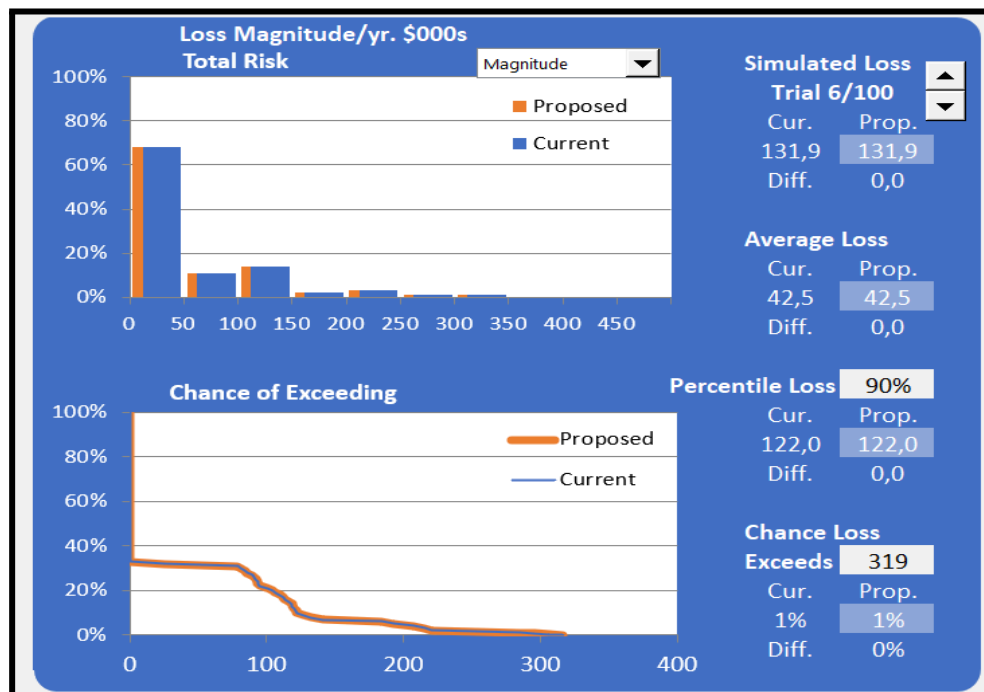
RESUMEN DE LOS VALORES UTILIZADOS

Primary Loss Magnitude			
Current	Min	ML	Max
Productivity	5	15	25
Replacement	20	30	40
Response	30	40	55
Reputation			
Competitive Adv.			
Judgments			
Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Secondary Loss Magnitude				
SLEF		Min	ML	Max
	Current	25%	35%	55%
	Proposed			
Current		Min	ML	Max
Productivity				
Replacement				
Response		2	3	5
Reputation		3	5	8
Competitive Adv.		10	20	30
Judgments		2	4	7
Proposed		Min	ML	Max
Productivity				
Replacement				
Response				
Reputation				
Competitive Adv.				
Judgments				

Copyright © 2018 The Open Group®. All Rights Reserved.

ANÁLISIS COSTE ESTIMADO



Conclusiones

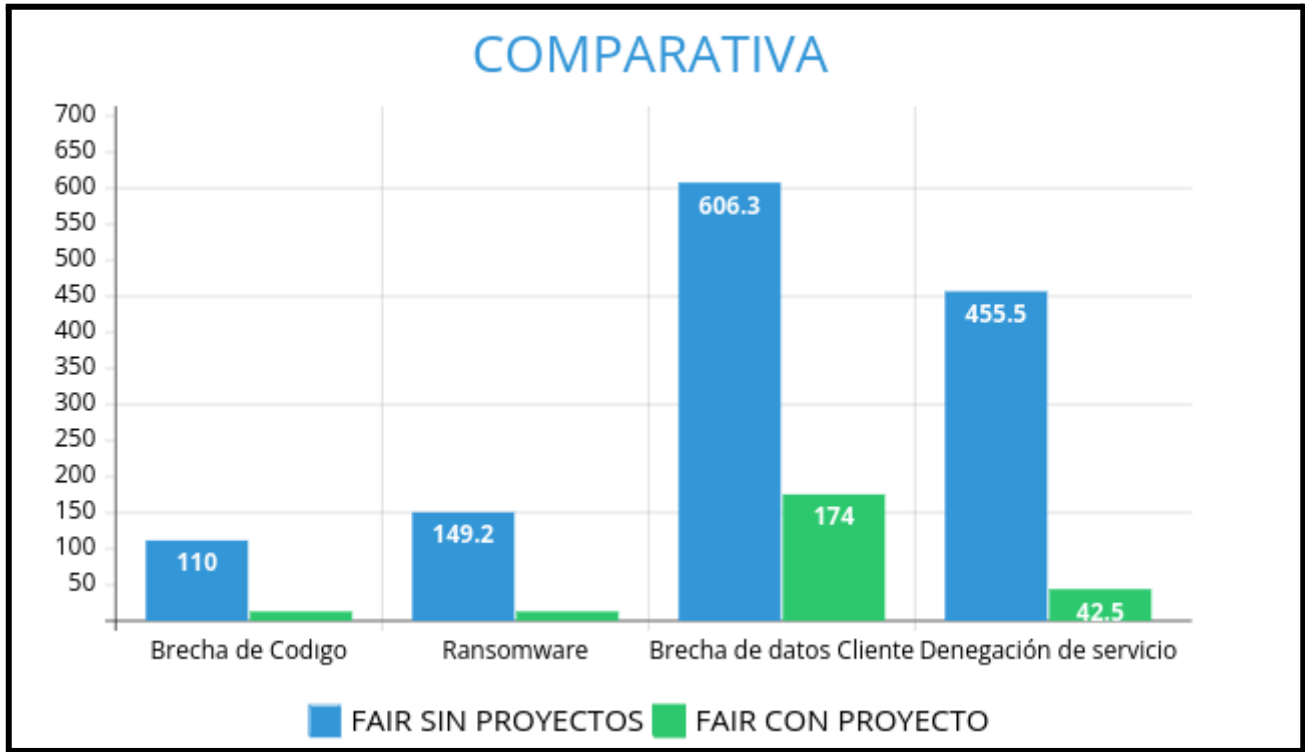
- El coste medio que va a suponer para las arcas de ChaseMyCash es de 42.500€ al año
- La probabilidad de que en un año este incidente genere pérdidas de más de 215.000€ es del 4%.
- A la vista de los datos, el coste máximo que puede tener al cabo del año ronda los 319.000€.

2. Comparación del riesgo

Los proyectos llevados a cabo se centraron en reducir al máximo posible los cuatro riesgos principales que preocupaban a ChaseMyCash en un período de 12 meses. Se implementaron medidas para mitigar estos riesgos y se espera que estas acciones reduzcan las pérdidas totales que la empresa podría sufrir debido a estos riesgos.

En la siguiente imagen se reflejan las pérdidas totales que supondrían a la empresa cada uno de estos riesgo antes y después de las proyectos implementados

	FAIR	PROYECTOS IMPLEMENTADOS
Brecha de código	110.000	11.500
Ransomware	149.200	11.600
brecha de datos cliente	606.300	174.000
DDoS	455.500	42.500



El cambio más notable observado es la significativa reducción en las pérdidas potenciales que cada riesgo podría ocasionar a la empresa después de la implementación de los proyectos. Esto ha resultado en un cambio significativo en el ranking de pérdidas asociadas a estos riesgos.

Antes de las mejoras, el riesgo de brecha de datos de clientes ocupaba el primer lugar en pérdidas, seguido por el de denegación de servicio, ransomware y brecha de datos de código, respectivamente. Sin embargo, después de los proyectos, la brecha de datos de clientes continúa siendo el riesgo que más pérdidas supone, seguido por ransomware, brecha de datos de código y denegación de servicio, en ese orden.

Por lo tanto, se concluye que ransomware y brecha de datos de código han avanzado un puesto en el ranking, superando a la denegación de servicio, que ahora es el riesgo con menos pérdidas, descendido dos puestos.

Es importante destacar que este análisis se basa en supuestos donde no se consideran los presupuestos de ChaseMyCash ni posibles imprevistos, lo que podría aumentar significativamente los costos en caso de incidentes. Sin embargo, la diferencia con respecto al primer análisis seguiría siendo notable.