Ingeniería de la Ciberseguridad
Curso 2023/2024

Caso Práctico 2

Gestión de la cadena de suministro

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

ÍNDICE

1. Acuerdos de nivel de servicio (SLAs)

Introducción

Los acuerdos de nivel de servicio (SLAs) son acuerdos contractuales que definen los niveles de calidad esperados de cada proveedor, abarcando elementos vinculados a la seguridad y privacidad de la información.

En el contexto de ChaseMyCash, los fundadores deben garantizar que los acuerdos de nivel de servicios con proveedores como Amazon, GitHub, Office365 y Zoho incorporen disposiciones referentes a la seguridad y privacidad de la información.

Pasos a seguir

Para formalizar un SLA con un proveedor, resulta crucial especificar indicadores clave de rendimiento (KPIs) que permitan evaluar el cumplimiento de los requisitos de seguridad acordados. Algunos ejemplos de KPIs que podrían ser definidos son:

- Intervalo de respuesta ante incidentes de seguridad.
- Tiempo de solución de incidentes de seguridad.
- Frecuencia de actualización de sistemas de seguridad.
- Frecuencia de auditorías de seguridad.
- Disponibilidad del servicio.
- Rendimiento del servicio.

Por ejemplo, podría acordarse una cláusula que obligue al proveedor a notificar inmediatamente a ChaseMyCash en caso de una violación de seguridad que afecte a los datos de la empresa o sus clientes. Igualmente, pueden establecerse cláusulas relacionadas con el cumplimiento de estándares y regulaciones de seguridad, como ISO 27001 o el Reglamento General de Protección de Datos (RGPD).

Responsabilidad

El fundador B (CTO) podría desempeñar un rol particularmente relevante en la gestión de los SLAs vinculados a proveedores de servicios tecnológicos. Como encargado de las TIC de la empresa y del desarrollo de productos, es probable que posea más pericia y conocimientos técnicos para fijar los KPIs y niveles de servicio apropiados para cada proveedor. Además, su equipo de desarrolladores y arquitectos en la nube podría estar a cargo de implementar y supervisar los controles necesarios para garantizar el cumplimiento de los SLAs.

El fundador A (CEO) también tendría una función destacada en la gestión de los SLAs, especialmente en lo relativo a proveedores de servicios de atención al cliente y ventas. En su calidad de encargado del desarrollo de negocio y del marketing estratégico, es probable que cuente con mayor experiencia en establecer KPIs y niveles de servicio relacionados con la satisfacción del cliente y la calidad del servicio.

El fundador C (COO) podría jugar un papel clave en la gestión de los SLAs vinculados a proveedores de servicios financieros y legales. Como responsable de finanzas y asuntos legales de la empresa, es probable que posea más experiencia en establecer KPIs y niveles de servicio relacionados con el cumplimiento de normativas y estándares financieros y legales. Además, su equipo de recursos humanos podría estar encargado de capacitar y sensibilizar a los empleados de ChaseMyCash sobre los requisitos de seguridad y privacidad de los SLAs.

2. Monitoreo continuo

Introducción

Es esencial llevar a cabo una supervisión constante de los servicios y aplicaciones que se apoyan en proveedores para detectar cualquier incidencia o vulnerabilidad de seguridad. Para ello, se pueden emplear herramientas como AWS CloudWatch o AWS Config, que posibilitan un monitoreo continuo de los servicios de Amazon Web Services. En el caso de GitHub, herramientas de análisis de código como SonarQube pueden ser útiles para identificar vulnerabilidades en el código.

Procedimiento a seguir

Para instaurar el control de supervisión continua en ChaseMyCash, se pueden seguir los pasos siguientes:

- **Identificar los sistemas y aplicaciones que dependen de los servicios de los proveedores críticos,** tales como Amazon, GitHub, Oce365 y Zoho. Esto implica revisar la arquitectura de la aplicación y los acuerdos con los proveedores.

- **Seleccionar las herramientas de supervisión de seguridad adecuadas.** En este caso, herramientas de AWS como AWS CloudWatch y AWS Security Hub pueden ser empleadas. Estas permiten detectar amenazas y debilidades en tiempo real, y generar alertas al identificar eventos de seguridad.

- **Configurar las herramientas de supervisión de seguridad conforme a las políticas de seguridad de ChaseMyCash.** Por ejemplo, AWS CloudWatch podría configurarse para generar alertas ante eventos de seguridad críticos en los sistemas y aplicaciones dependientes de los servicios de los proveedores. Además, considerar el uso de servicios de inteligencia de amenazas, los cuales monitorean la dark web en busca de información relevante y potenciales amenazas, utilizando técnicas avanzadas de recolección de datos y análisis para identificar actividades maliciosas y alertar a las organizaciones oportunamente.

- **Establecer métricas de monitoreo continuo**. Se deben definir métricas que permitan evaluar la efectividad del sistema de supervisión de seguridad y su capacidad para detectar amenazas y debilidades.

Responsable

Dado que el control de supervisión continua está vinculado a la seguridad de sistemas y aplicaciones, el fundador B (CTO) asumiría una mayor responsabilidad en su implementación.

Como CTO, está a cargo de las TIC de la empresa y del desarrollo de productos, lo que incluye garantizar la seguridad de los sistemas y aplicaciones de ChaseMyCash. Además, cuenta con un equipo dedicado a estas tareas, lo que le otorga la capacidad y el conocimiento técnico para implementar y administrar el sistema de monitoreo continuo.

Métricas

Número de incidentes atribuidos a sistemas de terceros: Este indicador contempla varios tipos de incidentes de seguridad, como explotación de vulnerabilidades conocidas, desbordamiento de memoria, ataques de día cero, así como problemas de disponibilidad. Al analizar estos incidentes, el CTO puede determinar si los servicios contratados a terceros cumplen con los intereses de la empresa. Este indicador se considera un Indicador Clave de Rendimiento (KRI) debido a que ChaseMyCash no posee su propia infraestructura y depende en gran medida de los servicios y la infraestructura de terceros. Por lo tanto, cualquier incidente que ocurra en estos sistemas de terceros afectará directamente el producto que ChaseMyCash ofrece.

Este Indicador Clave de Rendimiento (KRI) evalúa la cantidad de incidentes de seguridad ocurridos en 2022 en los servicios contratados por ChaseMyCash, basándose en información obtenida de las publicaciones oficiales de los proveedores y registros internos de la empresa. Este indicador está directamente vinculado al riesgo y refleja la confiabilidad y madurez de los proveedores en términos de seguridad de la infraestructura.

En el gráfico presentado, se muestra que Oce 365 experimentó 4 incidentes durante el último año, seguido de Amazon con 3, Github con 2 y Zoho con 1. ChaseMyCash establecerá un límite máximo de incidentes por año para cada uno de sus proveedores contratados. Por ejemplo, si se supera el nivel máximo establecido por alguno de ellos, ChaseMyCash consideraría buscar servicios similares ofrecidos por otro proveedor que inspire una mayor confianza y fiabilidad.

3. Pruebas de continuidad del negocio

Introducción

Las pruebas de continuidad del negocio son fundamentales para evaluar la capacidad de una empresa para recuperarse ante una interrupción del servicio. En el caso de ChaseMyCash, es crucial realizar pruebas de continuidad del negocio para los proveedores críticos, lo que implica identificar alternativas en caso de interrupciones y establecer planes de contingencia para cada uno de ellos.

Procedimiento a seguir

Para implementar el control de pruebas de continuidad del negocio en ChaseMyCash, se pueden seguir los siguientes pasos:

- **Identificación de proveedores críticos:** Se debe identificar aquellos proveedores cuyos servicios son esenciales para el funcionamiento de ChaseMyCash, como Amazon, GitHub, Oce365 y Zoho, entre otros.

- **Establecimiento de un plan de contingencia:** Para cada proveedor crítico, se debe establecer un plan de contingencia que permita a ChaseMyCash recuperarse ante una interrupción del servicio. Esto incluye identificar alternativas, realizar backups y adoptar medidas de seguridad adicionales.

- **Realización de pruebas de continuidad del negocio:** Es crucial llevar a cabo pruebas para verificar la efectividad del plan de contingencia y la capacidad de ChaseMyCash para recuperarse ante una interrupción del servicio. Estas pruebas pueden simular interrupciones y poner en práctica el plan de contingencia correspondiente.

- **Análisis de resultados y mejora continua:** Una vez realizadas las pruebas, es importante analizar los resultados y realizar mejoras en el plan de contingencia y las medidas de seguridad. Métricas como el tiempo de recuperación y el porcentaje de pérdida de datos pueden ser útiles para este propósito.

Herramientas y tecnología

Para implementar este control, se pueden considerar diversas herramientas y tecnologías, como:

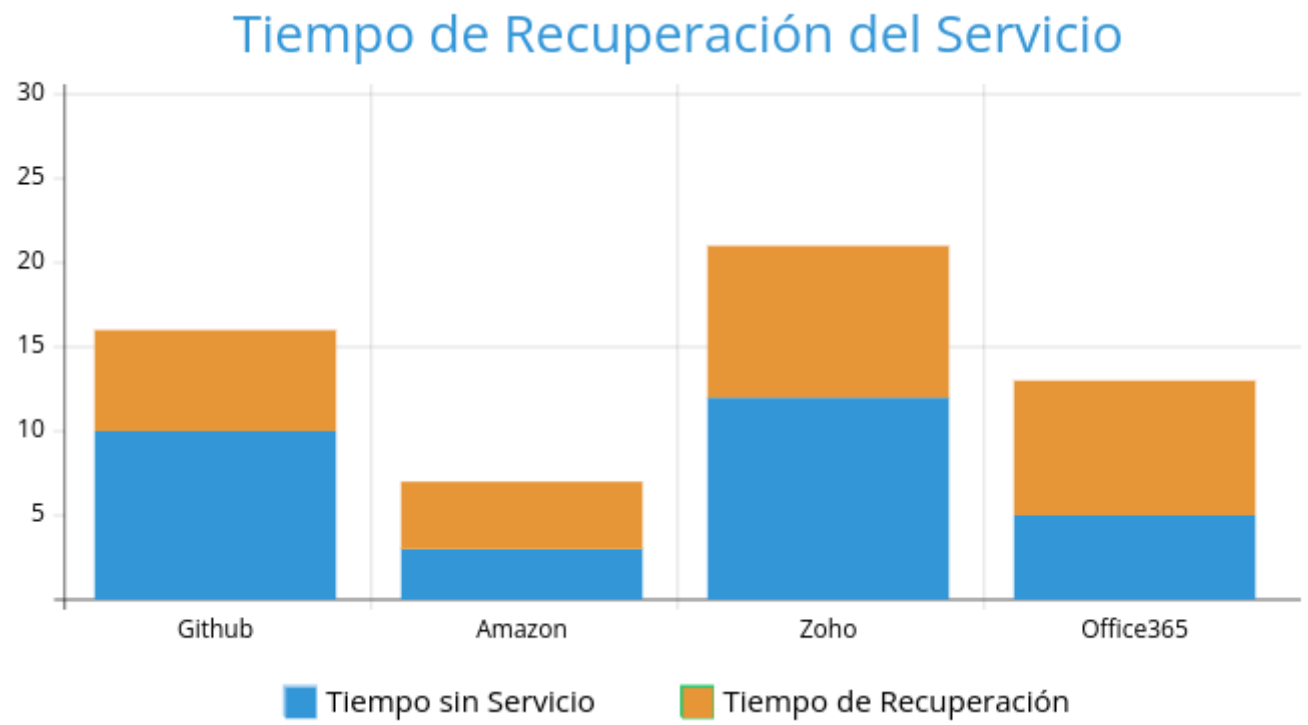
- Soluciones de backup y recuperación, como AWS Backup y AWS Disaster Recovery.
- Herramientas de gestión de riesgos, como AWS Security Hub y AWS Config.
- Plataformas de comunicación en caso de interrupciones del servicio, como AWS SNS y AWS Chime.

Responsable

En cuanto a la responsabilidad, el fundador B (CTO) tendría la mayor implicación en la implementación del control de pruebas de continuidad del negocio. Sin embargo, es relevante destacar que esta tarea requiere la colaboración de toda la organización, dado que se trata de asegurar la continuidad del servicio en caso de interrupciones. Por ende, todos los fundadores y sus respectivos equipos deberían participar en este proceso, contribuyendo según sus responsabilidades y conocimientos.

Métricas

Tiempo de respuesta o recuperación del servicio tras una caída: Esta métrica, similar a la anterior, permite al CTO evaluar si un servicio contratado satisface las necesidades de la empresa. Se mide el tiempo transcurrido desde que se produce una interrupción en un servicio de terceros hasta que este se restablece por completo. A través de esta métrica, se puede evaluar la calidad del servicio ofrecido por el proveedor. Por ejemplo, si ChaseMyCash utiliza Amazon Web Services (AWS) como su proveedor de infraestructura de TI y ha establecido un Acuerdo de Nivel de Servicio (SLA) que garantiza una disponibilidad del servicio del 99.9%, monitorear el tiempo de respuesta o recuperación del servicio permitiría al CTO determinar si el proveedor cumple con el SLA establecido. Si se observan períodos de inactividad prolongados o tiempos de recuperación excesivos, podría indicar deficiencias en el servicio proporcionado. Por lo tanto, esta métrica resulta útil para evaluar la calidad y confiabilidad de los servicios de terceros, así como para tomar medidas destinadas a mejorar la continuidad del servicio.



Este Indicador Clave de Rendimiento (KRI) mide el tiempo en horas anuales que los servicios contratados por ChaseMyCash han estado fuera de servicio. Se ha elaborado un gráfico recopilando datos del equipo de IT y de las publicaciones de los proveedores. ChaseMyCash ha acordado con sus proveedores un tiempo de restablecimiento esperado de 525,6 minutos (22 horas) al año, basado en el estándar de alta disponibilidad del 99,9% en un año. Se generarán alertas cuando se supere este tiempo establecido. Sin embargo, según el gráfico, ninguno de los proveedores contratados por ChaseMyCash supera este tiempo establecido como máximo, aunque Zoho se acerca bastante.

4. Inventario activo de las dependencias

Introducción

Es esencial mantener un inventario actualizado de las dependencias y componentes de los proveedores utilizados en los sistemas de ChaseMyCash.

Para ello, se pueden emplear herramientas de gestión de la configuración como AWS Systems Manager o Puppet, que facilitan el mantenimiento de un registro actualizado de las dependencias y componentes utilizados en los sistemas.

Procedimiento a seguir

Para implementar un inventario activo de las dependencias en ChaseMyCash, se pueden seguir los siguientes pasos:

- **Establecer un registro de dependencias:** Se debe establecer un registro que contenga información sobre los proveedores críticos, los sistemas y aplicaciones que dependen de ellos, y los requisitos de seguridad establecidos en los contratos. Este registro debe actualizarse regularmente y estar accesible para los miembros del equipo de gestión de la cadena de suministro y seguridad de la información.
- **Establecer requisitos de seguridad para cada proveedor:** Es importante establecer requisitos de seguridad para cada proveedor con el fin de garantizar la seguridad de la información de ChaseMyCash. Estos requisitos deben basarse en estándares reconocidos, como ISO 27001.
- **Establecer métricas para el inventario de dependencias:** Deben definirse métricas para medir la efectividad del inventario de dependencias. Algunas métricas pueden incluir la actualización regular del registro de dependencias, la identificación temprana de proveedores con problemas de seguridad, y la capacidad de la empresa para responder a interrupciones del servicio.

Para llevar a cabo estas tareas, se pueden utilizar herramientas de gestión de proveedores y seguridad de la información, como AWS Security Hub para centralizar y automatizar la gestión de la seguridad de los servicios de Amazon, o herramientas de gestión de riesgos como FAIR (Factor Analysis of Information Risk) para cuantificar los riesgos asociados a las dependencias y establecer prioridades en su gestión. También pueden ser útiles herramientas de gestión de activos, como JIRA, para realizar un seguimiento de las tareas relacionadas con la gestión de proveedores y la seguridad de la información.

Responsable

El fundador B (CTO) tendría mayor responsabilidad en la implementación del control de inventario activo de dependencias, dado que está a cargo de las TIC de la compañía y del desarrollo del producto.

Métricas

Mantenimiento regular del registro de dependencias: Una métrica para el mantenimiento periódico del registro de dependencias podría ser el "Tiempo Medio entre Actualizaciones de Dependencias" (TMAAD). Esta métrica cuantifica el tiempo que transcurre entre las actualizaciones de las dependencias de software que ChaseMyCash utiliza.

Para calcular el TMAAD, se suman todos los intervalos de tiempo entre las actualizaciones y se dividen por el número total de actualizaciones.

Este TMAAD proporciona una idea de la frecuencia con la que ChaseMyCash actualiza sus dependencias de software. Un TMAAD más bajo indicaría que la empresa se mantiene al día con las actualizaciones, lo que podría ser un indicador de un menor riesgo en la cadena de suministro de software. Por otro lado, un TMAAD más alto podría indicar un mayor riesgo, ya que las dependencias desactualizadas pueden contener vulnerabilidades de seguridad o ser incompatibles con otras partes del sistema.

ChaseMyCash puede solicitar a cada uno de los proveedores el tiempo transcurrido entre cada actualización de dependencias. Por ejemplo, si Amazon realizó actualizaciones en las siguientes fechas: 2023-04-01, 2023-04-15 y 2023-05-01, tendríamos dos intervalos de tiempo: 14 días entre la primera y segunda actualización, y 16 días entre la segunda y tercera actualización.

Para calcular el TMAAD en este ejemplo, sumaríamos todos los períodos de tiempo registrados (en este caso, 14 + 16 = 30 días) y dividiríamos la suma total de días por el número de actualizaciones realizadas. Si hubo tres actualizaciones, dividiríamos 30 días entre 3 actualizaciones, lo que resultaría en un TMAAD de 10 días.

5. Capacitación y concienciación de los empleados

Introducción

Es esencial capacitar a los empleados sobre los riesgos de seguridad asociados a los proveedores y las mejores prácticas de seguridad de la información. Para este fin, se pueden utilizar herramientas como PhishingBox o KnowBe4, que facilitan la realización de simulaciones de ataques de phishing y la capacitación de los empleados en la detección de estos ataques.

Procedimiento a seguir

Para implementar el control de capacitación y concienciación de los empleados, se pueden seguir los siguientes pasos:

- **Identificación de los riesgos de seguridad asociados a los proveedores:** El primer paso es identificar los riesgos de seguridad relacionados con los proveedores críticos de ChaseMyCash. Esto se puede lograr mediante el uso de herramientas de análisis de riesgos y evaluación de proveedores. Una vez identificados los riesgos, se deben elaborar planes de capacitación y concienciación para los empleados.

- **Desarrollo del programa de capacitación y concienciación:** El segundo paso implica la creación de un programa integral de capacitación y concienciación para los empleados. Este programa debe abordar los siguientes elementos:
    - Riesgos de seguridad asociados a los proveedores, como interrupciones del servicio, violaciones de datos y fallos de seguridad.
    - Mejores prácticas de seguridad de la información, incluyendo el uso de contraseñas seguras, autenticación de dos factores, encriptación de datos y el uso de VPN para acceder a los sistemas de la empresa
    - Políticas y procedimientos de seguridad de la información de ChaseMyCash, como la política de uso aceptable de sistemas y la política de gestión de contraseñas.
    - Normativas y regulaciones de seguridad de la información aplicables a la empresa y a los proveedores, como el RGPD y la Ley de Protección de Datos.

- **Implementación del programa de capacitación y concienciación:** Para llevar a cabo este programa, se pueden utilizar diversas herramientas, como presentaciones, videos, cursos en línea y charlas. Además, es crucial establecer un sistema de seguimiento y evaluación del programa para asegurar que los empleados reciban la capacitación necesaria y comprendan los riesgos y las mejores prácticas de seguridad de la información.

- **Establecimiento de métricas:** Es fundamental establecer métricas para evaluar la efectividad del programa de capacitación y concienciación de los empleados. Algunas métricas útiles podrían incluir:

    - La tasa de incidentes de seguridad antes y después de la implementación del programa.
    - El nivel de comprensión de los empleados sobre los riesgos y las mejores prácticas de seguridad de la información, medido mediante pruebas o encuestas.
    - El porcentaje de empleados que han completado la capacitación.

Uso de tecnologías: Para facilitar la implementación del programa de capacitación y concienciación de los empleados, se pueden aprovechar diversas tecnologías, como plataformas de aprendizaje en línea, herramientas de gestión de contenido y herramientas de seguimiento y evaluación. Por ejemplo, plataformas como Coursera o Udemy pueden utilizarse para ofrecer cursos de seguridad de la información, mientras que herramientas como Google Forms o SurveyMonkey pueden emplearse para medir la comprensión de los empleados sobre los riesgos y las mejores prácticas de seguridad de la información.

Responsable

En lo que respecta a la responsabilidad de llevar a cabo el control de capacitación y concienciación de los empleados, todos los fundadores tienen cierta responsabilidad, dado que es un control fundamental para la seguridad de la empresa.

No obstante, el fundador C, en su rol de COO, podría asumir un papel más destacado en este control. Dada su responsabilidad sobre las finanzas y los recursos humanos, posee una mayor experiencia y conocimientos en la implementación de políticas y programas de capacitación y concientización. Esto podría ser de gran ayuda para garantizar una implementación efectiva del control. Además, en su calidad de responsable financiero, el fundador C podría ser quien apruebe el presupuesto destinado a la capacitación y concientización de los empleados, así como quien supervise el uso eficiente de los recursos financieros asignados a este fin.

Métricas

Tiempo transcurrido desde el último taller de ciberseguridad: El departamento de Recursos Humanos de ChaseMyCash es responsable de organizar talleres de ciberseguridad, y este indicador es relevante para el Director de Operaciones (COO).

Este indicador muestra la cantidad de días que han pasado desde la última vez que se llevó a cabo un taller de ciberseguridad. También incluye umbrales que indican cuándo existe un mayor riesgo de que los empleados "olviden" lo que han aprendido en el curso. Este indicador se considera un Indicador Clave de Rendimiento (KRI) debido a que la falta de conciencia en ciberseguridad aumenta la probabilidad de que un ataque de ingeniería social tenga éxito. Cuando han pasado demasiados días desde el último taller, existe un mayor riesgo de que los empleados no estén al tanto de las últimas prácticas y técnicas de seguridad, lo que puede comprometer la seguridad de ChaseMyCash. La formación y concienciación del personal pueden ser controles importantes en la gestión del ciberriesgo en la cadena de suministro, por tanto se ha establecido como umbral mínimo, la necesidad de una formación de cualquier tipo (taller, charla, certificación, ...) que aborde este tema cada dos años y un umbral máximo, de una cada año.

Número de empleados afectados por campañas de phishing realizadas por la empresa: Este indicador también es relevante para el COO, ya que está relacionado con la efectividad de los cursos impartidos por Recursos Humanos. Mide el porcentaje de empleados de ChaseMyCash que caen en las campañas de phishing diseñadas por el equipo de IT para evaluar la respuesta de los empleados ante un ataque real de phishing. Este indicador se considera un KRI, ya que está directamente relacionado con la probabilidad de que la empresa sea víctima de ataques de phishing. Valores altos en este indicador serían motivo de preocupación, ya que indicarían una mayor vulnerabilidad y una falta de conciencia en ciberseguridad entre los empleados. Es importante que los cursos de capacitación y concientización aborden de manera efectiva la detección y prevención de ataques de phishing para proteger los activos y la información de ChaseMyCash.

Por ejemplo, un atacante que está al tanto de los proveedores de ChaseMyCash podría utilizar esa información para ejecutar un ataque de Spear-Phishing, fingiendo ser uno de los proveedores. Esto haría que un empleado de ChaseMyCash, que no ha sido informado sobre esta posibilidad en alguna sesión formativa, no desconfíe.