Análisis y gestión del riesgo

Práctica 1: Análisis de riesgos en ChaseMyCash

Marta Beltrán Pardo

Contenidos

1. Introducción

Para la realización de esta práctica los miembros del equipo iréis rotando entre diferentes roles que os indicaremos para cada sesión.

En total realizaremos 5 sesiones en el aula relacionadas con esta práctica, las fechas se indicarán con antelación suficiente en el calendario de la asignatura en Aula Virtual.

Al final de esta práctica habréis realizado un proceso de análisis de riesgos para la empresa ChaseMyCash, tanto desde el punto de vista de la seguridad corporativa como de la seguridad de producto y de la protección de datos. Y lo habréis hecho combinando diferentes metodologías para completar los resultados de unas con los de otras.

2. Material para la realización del caso

A continuación, se enumeran los materiales necesarios para la realización de esta práctica, que pueden descargarse desde el Aula Virtual:

- **Práctica1_Guion.pdf**: este documento.
- **Dossier ChaseMyCash.pdf**: información sobre la empresa con la que vamos a trabajar en los casos y las prácticas.
- **Material de apoyo sobre las metodologías proporcionado en Aula Virtual para cada sesión.**

3. Normativa y evaluación

En este apartado se detalla el formato de entrega de la práctica y la forma en la que se evaluará la misma:

- El porcentaje de la nota final de la asignatura al que corresponde esta práctica puede consultarse en la Guía docente de la propia asignatura.
- El caso deberá realizarse, de forma obligatoria en el aula los días indicados en el calendario de la asignatura en Aula Virtual, en grupos de cuatro personas. Para la asignación de los grupos se deberán seguir las indicaciones del profesor. Será necesario trabajar fuera del aula para terminar las tareas propuestas.
- Cada grupo deberá entregar una única copia de la memoria (entregables de las sesiones) a través de Aula Virtual. La fecha límite para cada entrega se avisará con tiempo suficiente.
- Los entregables deben ser, como mínimo, los propuestos en el siguiente apartado.

4. Enunciado de la práctica

Como ya se ha comentado en el apartado de Introducción, en esta práctica vais a realizar un proceso de análisis de riesgos completo.

Para ello se proponen las siguientes tareas y entregables asociados a cada una de las sesiones de trabajo. Los entregables tienen que generarse de manera profesional, como se haría en un proceso de análisis de riesgos real.

SESIÓN 1 – Análisis de riesgos con CORAS

En esta sesión se trabajará con la metodología CORAS. Se pide realizar un proceso de análisis de riesgos que incluya todos los pasos excepto el último (Risk Treatment, que dejaremos para la práctica 2 de la asignatura).

Se deben incluir en el análisis al menos, dos riesgos relacionados con la seguridad corporativa (brecha de datos que afecta al código de la aplicación y ransomware) y dos riesgos relacionados con la seguridad de producto (brecha de datos de clientes y denegación de servicio).

Para el análisis de riesgos para la seguridad corporativa, los roles en el equipo serán los siguientes:

> Responsable de seguridad corporativa, fundadores A, B y C.

Para el análisis de riesgos para la seguridad de producto, los roles en el equipo serán los siguientes:

> Responsable de seguridad de producto, fundador B, miembro del equipo de desarrollo, arquitecto cloud (responsable del despliegue en Amazon).

Entregable 1 – Fichero .zip o .rar que incluya la documentación, diagramas, escalas, tablas, etc. asociadas al proceso de análisis de riesgos realizado con la metodología CORAS. Es muy importante justificar las decisiones tomadas así como documentar las discusiones que se haya producido en el equipo y todo el material preparado para la realización del análisis.

Se incluirá un documento maestro en formato pdf con un resumen ejecutivo al principio y tantos anexos o ficheros adicionales como se estime necesario.

SESIÓN 2 – Análisis de riesgos con FAIR – Value at Risk

En esta sesión se trabajará con la metodología FAIR – Value at Risk. Se pide realizar un proceso de análisis de riesgos que incluya todos los pasos hasta llegar al tratamiento o gestión de los riesgos (que se excluye ya que será el objetivo de la práctica 2).

Se deben incluir en el análisis al menos, los mismos riesgos que se hayan analizado en la sesión 1 utilizando CORAS.

El reparto de roles entre los miembros del equipo será el mismo que en la sesión de trabajo 1.

Entregable 2 – Fichero .zip o .rar que incluya la documentación, diagramas, escalas, tablas, etc. asociadas al proceso de análisis de riesgos realizado con la metodología FAIR. Es muy importante justificar las decisiones tomadas (por qué esos riesgos en concreto, por ejemplo) así como documentar las discusiones que se haya producido en el equipo y todo el material preparado para la realización del análisis.

Se incluirá un documento maestro en formato pdf con un resumen ejecutivo al principio y tantos anexos o ficheros adicionales como se estime necesario.

SESIÓN 3 – Trabajo con las probabilidades y los impactos

En esta sesión se revisitarán los análisis realizados en las sesiones 1 y 2 intentando mejorar las estimaciones realizadas para probabilidades e impactos con las técnicas estudiadas en la unidad 6 de la asignatura. Probablemente esto implique desviarse un poco de las metodologías que se habían empleado, CORAS y FAIR y buscar nuevas fuentes de datos e inteligencia. Se deben usar métodos indirectos para la estimación de la probabilidad, al menos una vez el teorema de Bayes y al menos una vez la distribución Beta.

Además de intentar mejorar el trabajo realizado en las sesiones previas, se compararán los resultados obtenidos con ambos enfoques, cualitativo y cuantitativo, y se combinarán los resultados de ambos intentando llegar a conclusiones de interés.

El reparto de roles entre los miembros del equipo será el mismo que en las sesiones 1 y 2.

Entregable 3 – Documento maestro en formato pdf con un resumen ejecutivo al principio que explique los cambios realizados y las mejoras introducidas en los análisis que se habían realizado en las sesiones 1 y 2. Anexos y ficheros adicionales que se estimen oportunos.

Entregable 4 – Documento maestro en formato pdf que combine los resultados del enfoque cualitativo (CORAS) y cuantitativo (FAIR) explicando cómo se complementan, en qué se diferencian. Debe incluir unas conclusiones del proceso de análisis a la vista de todos los resultados obtenidos. También una discusión de limitaciones y posibilidades de mejora.

SESIÓN 4 – Modelado de amenazas

En esta sesión se jugará una partida de cartas con el juego Cornucopia de OWASP para obtener un primer modelo de amenazas de la aplicación ChaseMyCash. Al ser un primer modelo, tiene que centrarse en el subconjunto de amenazas más obvias/críticas. Se irá completando este modelo en el futuro.

Para esta partida, los roles en el equipo serán los siguientes:

> Responsable de seguridad de producto, fundador B, miembro del equipo de desarrollo, arquitecto cloud (responsable del despliegue en Amazon).

Entregable 5 – Ficheros y documentación asociados a la partida (tablas, comentarios y discusiones, puntuaciones).

Entregable 6 – Documento maestro en formato pdf con el modelo de amenazas formalizado y preparado para ser publicado internamente (y ser utilizado como guía en diferentes procesos).

SESIÓN 5 – Evaluación de impacto para la protección de datos

En esta sesión se tratará el tema de los riesgos para la protección de datos ya que la aplicación que comercializa ChaseMyCash recopila y almacena datos personales. Para ello se seguirán las indicaciones de la Agencia Española de Protección de Datos, ya que es la autoridad de control ante la que hay que responder. No se incluirá en esta sesión la parte de gestión de los riesgos, sólo la de análisis.

Se deben incluir en el análisis, al menos, los cinco riesgos que se consideren más significativos, atendiendo especialmente a los impactos que las brechas de datos podrían tener en los derechos y libertades de los clientes.

Para esta partida, los roles en el equipo serán los siguientes:

> Responsable de seguridad de producto, fundadores A, B y C.

Entregable 7 – Documentación asociada a la evaluación de impacto realizada (excepto lo relativo a mitigaciones y gestión) como si se fuera a presentar a la AEPD.