Ingeniería de la Ciberseguridad
Curso 2023/2024

Sesión práctica 1:

Informe ejecutivo. CORAS

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

El propósito de este informe es exponer los hallazgos del análisis de riesgos realizado para la empresa ChaseMyCash.

Activos Críticos

Para el análisis de riesgos se identificaron los activos críticos de ChaseMyCash que son:

- **Reputación de la compañía**: Es esencial para mantenerse competitivos en el mercado, y puede verse afectada negativamente por incidentes de seguridad.
- **Imagen proporcionada a los clientes**: Una percepción negativa puede afectar adversamente la lealtad de los clientes y, por ende, la viabilidad económica de la empresa.
- **Información sensible de los usuarios:** Una gestión ineficaz, o una brecha de seguridad que comprometa estos datos, podría tener consecuencias devastadoras, no sólo en términos de pérdida de confianza y credibilidad entre los usuarios, sino también en posibles sanciones legales y financieras para la empresa.
- **Código fuente del software:** La eventual pérdida o vulneración de la seguridad del código podría dar a los atacantes la posibilidad de acceder a información sensible y manipular la aplicación.

Incidentes no deseados

El equipo de análisis descubrió diversos eventos no deseados que podrían comprometer la seguridad de la información y la continuidad operativa de ChaseMyCash. Estos incidentes abarcan:

- La **descarga e instalación de malware,** en el equipo de un trabajador podría comprometer los sistemas y establecer una puerta trasera haciendo que los atacantes pudieran manipular el código fuente de la aplicación.
- La **eliminación accidental de información de la base de datos**, podría ocasionar una denegación de servicio.
- La **propagación de ransomware a través de la red corporativa**, lo que podría comprometer los sistemas y datos críticos de la empresa.
- Una **brecha de datos de clientes,** ocasionaría la pérdida de información confidencial y, por lo tanto, pérdidas económicas y de reputación.

Estableciendo un orden de criticidad, el riesgo más crítico sería la brecha de datos de clientes, seguido de la propagación del ransomware y de la denegación del servicio. Estos riesgos requieren una atención inmediata para reducir su impacto en la privacidad y seguridad de los clientes, así como en la reputación de la empresa. En cuanto a la brecha de datos del código, es un riesgo asumible y la empresa puede implementar medidas para mitigarlo, aunque no es necesario actuar con urgencia.