Benyahir Y. Martínez Hermina R00624824

Asignación 2 - Análisis de Riesgo Cuantitativo y Cualitativo y Métodos de Ataques Cibernéticos

Parte 1: Casos de Uso Prácticos (12 puntos)

Caso 1 – Análisis de Riesgo Cuantitativo (6 puntos)

Una empresa de e-commerce identifica que su servidor de pagos (valor: $1,200,000) está expuesto a un ataque de ransomware.

- Se estima que, si ocurre un ataque exitoso, la pérdida sería del 50% del valor del activo.

- La probabilidad de ocurrencia es de 0.3 incidentes por año (un ataque exitoso cada ~3 años).

SLE = $1,200,000 × 50% = $600,000

ARO = 0.3/año

ALE = $600,000 × 0.3 = $180,000 por año

Interpretación: si la compañía invierte en un control de seguridad de $50,000 anuales y reduce la probabilidad a 0.1.

SLE = ($1,200,000 - $50,000) × 50% = $1,150,000 × 50% = $575,000

ARO = 0.1/año

ALE = $575,000 × 0.1 = $57,000 por año

Caso de Uso 2 – Análisis de Riesgo Cualitativo (6 puntos)

Un hospital universitario teme un ataque de Denegación de Servicio Distribuido (DDoS) contra su portal web de citas médicas en línea.

- Se estima que la probabilidad de ocurrencia es Alta.

- El impacto sería Medio (pérdida de citas y quejas de pacientes, pero sin riesgo directo a vidas humanas).

		Impacto	
Probabilidad	**Bajo**	**Medio**	**Alto**
Bajo	Bajo	Bajo	Medio
Medio	Bajo	Medio	Alto
Alto	Medio	Alto	Crítico

- La razón por la cual el nivel de riesgo seria alto se debe a que los atacantes podrían recolectar la información personal de los pacientes que estaban utilizando el portal.

Contra medidas iniciales:

Técnico: Aplicar un parche al portal que limita la velocidad de este haciendo que limite la cantidad de solicitudes que se pueden enviar en un plazo determinado de tiempo. Haciendo que este no se sobrecargue de recursos que puedan provocar un ataque DDoS.

Parte 2: Preguntar Teóricas (8 puntos)

1. **Menciona** las tres dimensiones usadas para clasificar los riesgos según la Lección 1. (2pts)
   - Clasificación por origen
   - Clasificación por intención
   - Clasificación por foco

2. **Menciona** las cuatro categorías de ataques vistas en la Lección 2. (2pts)
   - Intercepción – El atacante espía sin modificar el contenido en tránsito.

   - Modificación – El atacante altera datos legítimos a lo que estos están en tránsito para cambiar su efecto.

- Fabricación – El atacante diseña paquetes o mensajes falsos que son aceptados como validos por el sistema.

- Interrupción – El atacante impide que el acceso legítimo de a recursos o destruirlos.

3. **Define** qué es SLE (Single Loss Expectancy) en análisis de riesgo cuantitativo. **DEFINICIÓN COMPLETA.** (1pts)

   SLE – La pérdida monetaria estimada o el impacto de una sola ocurrencia de una amenaza y se puede calcular de esta manera, valor activo × porciento de la perdida esperada.

4. **Explica** qué significa "**probabilidad alta**" en un análisis cualitativo y cómo se representa en una matriz de probabilidad-impacto. (1.5pts)

   Para clasificar que el riesgo de probabilidad alta este se asocia con el color rojo. También el significado de esta implica que el impacto de algo como esto suceda puede ser bastante grave para el tipo de situación que se está lidiando.

5. **Define** Interrupción como modelo de ataque y **da un ejemplo práctico**. (1.5pts)

   Interrupción – El atacante impide que el acceso legítimo de a recursos o destruirlos.

   Ejemplo: Digamos que dos doctores están discutiendo un caso que es de suma importancia, pero de repente el mensaje que discutía información importante para un nuevo desarrollo es interceptando por un atacante que sostiene esta información hasta que el doctor que iba recibirlo cumpla por las demandas de este.