DOCUMENTO BASE PARA EL MODELADO DE AMENAZAS DE APLICACIONES DE SOFTWARE Y ANÁLISIS DE RIESGOS

(V0.1.0)

ÍNDICE

1. Marco Referencial y Definiciones

El presente documento tendrá como bases las siguientes definiciones y marco referencial:

1.1. Seguridad de Software

La seguridad del software se relaciona por completo con la calidad. Debe pensarse en seguridad, confiabilidad, disponibilidad desde la fase de diseño y durante todo el ciclo de vida del software

1.2. ¿Por qué es necesario realizar un modelado de amenazas?

El modelado de amenazas es un proceso estructurado a través del cual se pueden identificar posibles amenazas y vulnerabilidades de seguridad, cuantificar la gravedad de cada una, y priorizar los controles para mitigar los ataques.

1.3. ISO/IEC 27001

El presente documento cumple con los controles 8.2.1 (Clasificación de la información) y 14.2.1 (Política de desarrollo seguro) de la norma ISO/IEC 27001.

1.3. ISO/IEC 27034

El presente documento cumple con el control 3.20 (Threat Risk Modelling) de la norma ISO/IEC 27034.

2. Metodología

El Instituto SANS (SysAdmin Audit, Networking and Security Institute) ofrece un procedimiento práctico de siete pasos para realizar el modelado de amenazas y análisis de riesgos de aplicaciones:

Paso 1: Hacer una lista de lo que estás tratando de proteger.

- Clasificar los datos (que es público, que es privado)
- Identificar los procesos críticos de la aplicación (del cual se requiere logs detallados)

Paso 2: Elaborar un diagrama de aplicación

- Elaborar un diagrama que muestre todas las redes, servidores, máquinas virtuales, clientes, firewalls, enrutadores, conmutadores, Microservicios, API gateways y otros componentes importantes. Se debe especificar el nombres de protocolo y números de puerto que se usarán

Paso 3: Elaborar la lista de agentes de amenaza

- Realizar lista de agentes de amenazas (Usuario logeado, hacktivistas, bots, insiders, ataque dirigido) y sus motivaciones

Paso 4: Realizar una lista de amenazas

- Realizar una lista de amenazas de los actores anteriormente descritos. Para identificar estas amenazas se usará la técnica STRIDE. Esta clasifica las amenazas de seguridad en seis categorías:

  - ➢ **S**poofing: cuando un atacante finge ser alguien que no es
  - ➢ **T**ampering: ocurren cuando el atacante modifica datos en tránsito
  - ➢ **R**epudiation: Cuando alguien realiza una acción y luego afirma que en realidad no la realizó
  - ➢ **I**nformation disclosure: El atacante accede a datos sensibles
  - ➢ **D**enial of service: El atacante puede degradar o negar el servicio a los usuarios.
  - ➢ **E**levation of privilege: El atacante tiene la capacidad de obtener privilegios que normalmente no tiene

  Ejemplo de amenazas:

- ➔ Fuga de información
- ➔ Modificar fecha de un registro
- ➔ Ataques automatizados
- ➔ Saltar la validación del SEGIP
- ➔ Registro de múltiples cuentas (uso de correos descartables)

Paso 5: Estimar la probabilidad y el daño potencial

Para determinar el riesgo general se usará el modelo de evaluación de riesgos DREAD que tiene las categorías:

- ➢ **D**amage (Daño): ¿qué tan grave sería un ataque?
- ➢ **R**eproducibility (Reproducibilidad): ¿qué tan fácil es reproducir el ataque?
- ➢ **E**xploitability (Explotabilidad): ¿cuánto trabajo cuesta lanzar el ataque?
- ➢ **A**ffected users (Usuarios afectados): ¿cuántas personas se verán afectadas?
- ➢ **D**iscoverability (Descubrimiento): ¿qué tan fácil es descubrir la amenaza?

Para la evaluación de riesgo se dio énfasis al impacto que pueda producir la materialización de un riesgo.

DAÑO POTENCIAL (1-5):

1 = Sin daño

2 = Divulgación de información

3 = Datos de usuarios no confidenciales individuales / empleadores comprometidos

4 = Datos administrativos no sensibles comprometidos

5 = Destrucción de datos o aplicación no disponible

REPRODUCIBILIDAD (0-10):

0 = Difícil o Imposible

5 = Complejo

7 = Fácil para usuarios autenticados

10 = Muy fácil a través del navegador web, sin autenticación

EXPLOTABILIDAD (0-10):

1 = Incluso con el conocimiento directo de la vulnerabilidad, no existe una manera de explotarlo

2 = Se requieren técnicas avanzadas, herramientas a medida. Solo explotable por usuarios autenticados.

5 = La explotación está disponible y utilizable con una habilidad moderada por usuarios autenticados.

7 = La explotación está disponible y utilizable por usuarios no autenticados.

10 = Trivial: sólo se requiere un navegador web.

USUARIOS AFECTADOS (0-10):

0 = No hay usuarios afectados

2.5 = Usuario individual

6 = Pocos usuarios

8 = Usuarios administrativos

10 = Todos los usuarios

DESCUBRIMIENTO (0-10):

0 = Muy difícil o imposible de detectar incluso con acceso al código fuente y acceso privilegiado a los sistemas en ejecución.

5 = Puede averiguarlo mediante solicitudes HTTP

9 = Los detalles de fallas como esta ya son de dominio público y pueden se descubre fácilmente mediante un motor de búsqueda.

10 = La información está visible en la barra de direcciones del navegador web o en un formulario

Para determinar el riesgo general usaremos la siguiente fórmula:

Riesgo general = DAÑO POTENCIAL * (REPRODUCIBILIDAD + EXPLOTABILIDAD + USUARIOS AFECTADOS + DESCUBRIMIENTO)

Nivel de riesgo	Puntuación DREAD	Tratamiento
Crítico	160-200	Se debe considerar de inmediato para su revisión y resolución
Alto	100-159	Se debe considerar para revisión y resolución en un corto período de tiempo
Medio	41-99	Se deben gestionar estos riesgos una vez que se hayan abordado los riesgos críticos y altos
Bajo	1-40	No representa un riesgo significativo para la aplicación y se puede aceptar el riesgo si implementar el control consumiría muchos recursos

Paso 6: Elaborar las contramedidas

- Piense en las contramedidas para mitigar las amenazas identificadas y sus posibles problemas que su implementación

Paso 7: Revisar el documento

- Revisar el documento por al menos un desarrollador del equipo asignado, un QA y el responsable de área.

3. Bibliografía

1. Secure, Resilient, And Agile Software Development
2. https://www.sans.org/blog/practical-risk-analysis-and-threat-modeling-spreadsheet/
3. https://blog.eccouncil.org/dread-threat-modeling-an-introduction-to-qualitative-and-quantitative-risk-analysis/