DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Ejemplo:

Ejemplo de aplicación de DREAD

Fundamentos de Ciberseguridad

Profesor

Juan Ignacio Iturbe A.

DREAD

- DREAD se utiliza principalmente para evaluar el riesgo asociado con amenazas específicas que podrían explotar vulnerabilidades. Por lo tanto, al aplicar DREAD, necesitas tener en cuenta varios de estos componentes. Específicamente:
  1. Amenaza: Necesitas identificar la amenaza específica que estás evaluando. Esto podría ser, por ejemplo, un atacante que intenta obtener acceso no autorizado a una base de datos.
  2. Vulnerabilidad: Es esencial conocer la vulnerabilidad o debilidad específica que la amenaza podría explotar. Esta vulnerabilidad podría ser un error de configuración, una deficiencia en el software, etc.
  3. Activo: Aunque DREAD no se centra específicamente en el activo, es útil conocer cuál es el activo en riesgo para entender el potencial "Daño" si la amenaza se materializa. Un activo podría ser información confidencial, un sistema crítico, entre otros.
  4. Agente de Amenaza (opcional): Si bien DREAD no requiere específicamente la identificación del agente de amenaza, tener una idea de quién podría ser el agente (por ejemplo, un hacker novato, un insider malicioso, un actor patrocinado por un estado) puede ayudarte a evaluar mejor la "Explotabilidad" y "Reproducibilidad" de la amenaza.

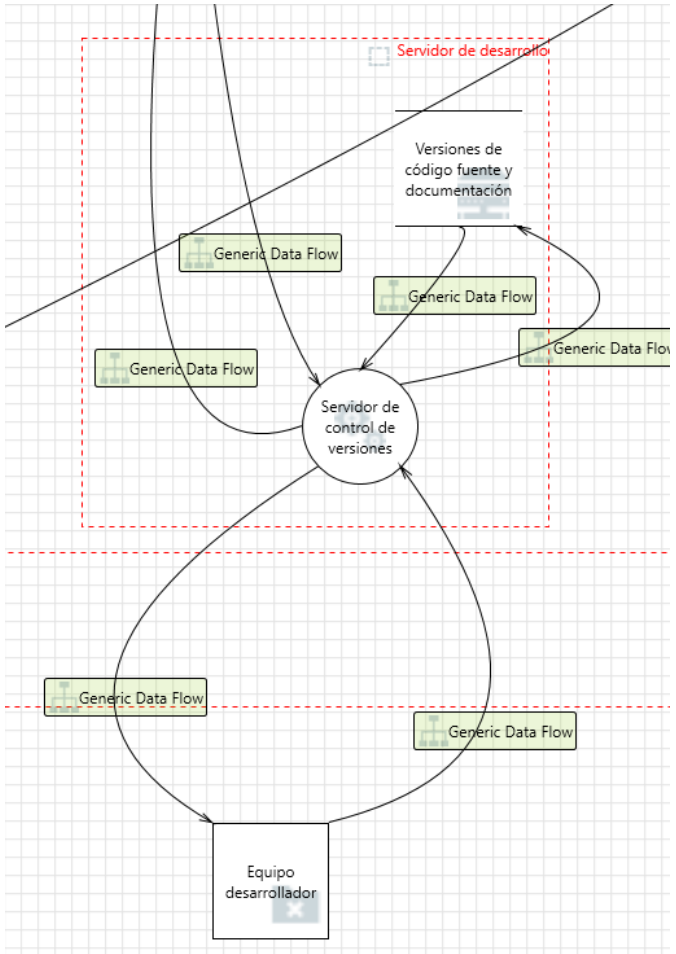
DREAD

Dicho esto, para aplicar DREAD de manera efectiva:

- **Damage (Daño):** Evalúa el impacto potencial en el activo si la amenaza se materializa aprovechando la vulnerabilidad.
- **Reproducibility (Reproducibilidad):** Estima qué tan fácil es para un agente de amenaza reproducir el ataque que explota la vulnerabilidad.
- **Exploitability (Explotabilidad):** Considera qué tan fácil es para el agente de amenaza llevar a cabo el ataque que explota la vulnerabilidad.
- **Affected Users (Usuarios Afectados):** Evalúa cuántos usuarios podrían verse afectados si la amenaza se materializa. Aunque esta métrica tiene un enfoque en los "usuarios", puede adaptarse para referirse a cuántos "activos" o "sistemas" se verían afectados.
- Discoverability (Descubribilidad): Considera qué tan fácil es para el agente de amenaza descubrir y luego explotar la vulnerabilidad.

Ejemplo: Contexto

- **Amenaza:** Un desarrollador de software malicioso quiere introducir un bug en el software de producción.
- **Vulnerabilidad:** A pesar de los controles en el sistema de control de versiones (Revisión por el equipo de QA y aprobación del Jefe de informática), un desarrollador podría introducir cambios maliciosos en su propia rama de desarrollo.
- **Activo:** El software en producción que es esencial para las operaciones.
- **Agente de Amenaza:** El desarrollador malicioso con acceso al sistema de control de versiones.



Ejemplo: Aplicación de DREAD

Damage (Daño):

- Si el desarrollador malicioso introduce un bug que pasa desapercibido a través de QA y se implementa en producción, el daño podría ser significativo. Esto depende de la naturaleza del bug, pero podría causar interrupciones en el servicio, pérdida de datos o incluso la exposición de información confidencial.
- Valor asignado: 8 (en una escala del 1 al 10, siendo 10 el daño máximo posible).

Ejemplo: Aplicación de DREAD

Reproducibility (Reproducibilidad):

- Dado que el desarrollador tiene acceso regular al sistema de control de versiones y puede hacer cambios en su propia rama, la reproducibilidad es alta.
- Valor asignado: 9.

Ejemplo: Aplicación de DREAD

Exploitability (Explotabilidad):

1. Si bien el desarrollador puede introducir cambios maliciosos, el código aún debe pasar por el equipo de QA y ser autorizado por el jefe de informática. Estos controles adicionales reducen la facilidad de explotación.
2. Valor asignado: 6.

Ejemplo: Aplicación de DREAD

Affected Users (Usuarios Afectados):

1. Si el bug es introducido en producción, podría afectar a todos los usuarios del software. Dependiendo de la base de usuarios, esto podría ser significativo.
2. Valor asignado: 8.

Ejemplo: Aplicación de DREAD

Discoverability (Descubribilidad):

- Aunque el desarrollador pueda introducir un bug, la revisión del equipo de QA y la aprobación del jefe de informática actúan como controles que podrían descubrir el cambio malicioso antes de que llegue a producción. Sin embargo, no hay garantía de que estos controles siempre detecten el bug.
- Valor asignado: 5.

Ejemplo: Resumen aplicación de DREAD

- Daño: 8
- Reproducibilidad: 9
- Explotabilidad: 6
- Usuarios Afectados: 8
- Descubribilidad: 5

Recursos bibliográficos

- Stallings W. (2019). Effective Cybersecurity: A guide to using Best Practices and Standards. Addison-Wesley
- Threat Modeling: A practical Guide for Development Teams, O'Reilly