GRUPO DE SEGURIDAD INFORMÁTICA

Fundamentos de la Seguridad Informática

Gestión de Riesgos

Marco de políticas

- Las aplicaciones seguras, no solamente “suceden”
- Son el resultado de una organización decidiendo que van a producir aplicaciones de esa forma
- Para una aplicación segura, se requiere al menos:
  - Una gerencia organizacional que conoce bien los problemas de seguridad que puedan tener

Marco de políticas (2)

- Una política de seguridad escrita derivada de estándares nacionales
- Una metodología de desarrollo con adecuados checkpoints y actividades de seguridad
- Procesos de *Secure release* y *configuration management*

- La mayoría de las organizaciones producen políticas de information security derivadas de la ISO 17799, o si es en USA, de COBIT, u ocasionalmente de ambos

LA pregunta

- Si les pregunto: ¿cómo defiendo mi aplicación?

.... ¿de qué?

Gestión de riesgos

- Al iniciar el diseño de una aplicación, es esencial aplicar análisis de riesgo
- El método usado no es tan importante como realmente hacer un modelo estructurando el análisis de las posibles amenazas

Terminología de análisis de riesgos tradicional

- Activo: el objeto de los esfuerzos de protección.
  - Puede ser definido como un componente del sistema, datos, etc.
- Riesgo: la probabilidad de que un activo sufra un evento con un impacto negativo
- Amenaza: el actor o agente que es el origen del peligro.
  - En general es un agente malicioso
  - Efectúan ataques sobre la seguridad del sistema

Terminología de análisis de riesgos tradicional (2)

- Vulnerabilidad: para que una amenaza sea efectiva, debe actuar sobre una vuln.
  - Es un defecto o debilidad en la seguridad de un sistema, su diseño, implementación, o controles internos
  - En el software, surgen de los defectos, y están en dos "sabores":
    - Fallas: problemas a nivel de diseño
    - Bugs: problemas a nivel de código fuente

Terminología de análisis de riesgos tradicional (3)

- Contramedidas o salvaguardas: los controles operacionales, de gestión, o técnicos realizados a un sistema de información
  - Tomados en conjunto protegen adecuadamente la confidencialidad, integridad, y disponibilidad del sistema
  - Para cada riesgo, pueden ponerse controles que previenen o detectan cuando se dispara el riesgo

Terminología de análisis de riesgos tradicional (4)

- Impacto: en la organización que usa el software, si el riesgo se materializara
  - Puede ser monetario, de imagen
  - Violación de alguna ley, o de un SLA
  - Sin cuantificar un riesgo es difícil de mitigar
- Probabilidad: posibilidad que un evento dado se genere
  - Usualmente expresado como un porcentaje o simplemente Alto/Medio/Bajo

Grupo de Seguridad Informática

¿Para qué calculo el riesgo?

- Para crear estrategias de mitigación

... en definitiva, dónde poner los controles

... y, cómo testearlos!

Cálculo de riesgo

- Descomponer la aplicación
  - encontrar sus activos, funcionalidad y conectividad
- Definir y clasificar los activos - clasificar los activos en activos tangibles e intangibles, y ponderarlos de acuerdo a su criticidad para el negocio.
- Explorar vulnerabilidades potenciales (técnicas, operacionales y de gestión)

Cálculo de riesgo (2)

- Explorar amenazas potenciales
  - a través de un proceso de desarrollo de escenarios de amenaza o árboles de ataque
- Desarrollan una visión realista de potenciales vectores de ataque desde la perspectiva del atacante

Referencias

- NIST SP 800, Risk Management Framework for Information Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- https://csrc.nist.gov/Projects/risk-management/rmf-quick-start-guides
- CVSS, https://www.first.org/cvss/ (Mide Severidad, no riesgo)