DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Fundamentos de ciberseguridad

Seguridad en el desarrollo de software

Profesor

Mg. Juan Ignacio Iturbe A.

Introducción

- El software usualmente es desarrollado teniendo en cuenta la funcionalidad, no la seguridad del mismo.
- La seguridad y la funcionalidad deberían estar integrados en cada fase del ciclo de vida del desarrollo.
- La seguridad debería estar entretejida dentro del corazón del producto y proveer protección a las capas necesarias.

¿Dónde colocar la seguridad?

- Hoy en día muchos de los esfuerzos para solucionar los problemas de seguridad son a través de:
  - Firewalls
  - IDS
  - Filtro de contenidos
  - Software Antivirus
  - Escaner de vulnerabilidad
  - Etc.

¿Dónde colocar la seguridad?

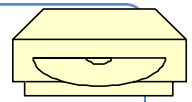
- Todo esto por que el software contiene muchas vulnerabilidades.
- En general el perímetro se encuentra fortificado y solido, pero el ambiente interno y el software es fácilmente explotable para obtener algún acceso.
- Los defectos de software causan la mayoría de las vulnerabilidades.

¿Dónde colocar la seguridad?

- Esto se explica por diversos factores:
  - En el pasado no era crucial implementar la seguridad durante las etapas de desarrollo.
  - La mayoría de los profesionales de la seguridad no son desarrolladores de software, y no tienen una visión completa
  - Funcionalidad ante la seguridad.
  - Vendedores de software tratando de posicionar en el mercado sus productos lo antes posible.
  - Instalar software con defectos y aplicar parches posteriormente se ha vuelto una práctica habitual.

Tendencia habitual al tratar con seguridad en las aplicaciones

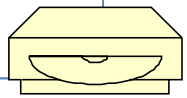
1. • Software defectuoso es lanzado al mercado para vencer a la competencia.



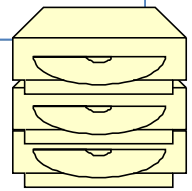
2. • Hacker buscan nuevas vulnerabilidades y debilidades en el nuevo software.

3. • Algún sitio web “postea” estas vulnerabilidades y como explotarlas

4. • El vendedor desarrolla y lanza parches para arreglar las vulnerabilidades.



5. • El nuevo parche va la pila de parches de software que todos los administradores de red y sistema necesitan probar e instalar.



Ambiente versus aplicación

- Los controles de software pueden ser implementados:
  - Por el sistema operativo (S.O.)
  - Por la aplicación
  - Ó una combinación de ambos.
- Por un lado el S.O. no se puede conocer todos los tipos de vulnerabilidades internas que puede tener una aplicación. Por ej:
  - Es difícil para el S.O predecir que vulnerabilidades tiene la aplicación instalada y el control adecuado.
- La aplicación se puede ocupar de protegerse, pero no puede hacer nada ante vulnerabilidad es del S.O. Por ej:
  - Si se insertan entradas ARP maliciosas, esto es responsabilidad de la pila de red y del S.O., no de la aplicación.

Funcionalidad versus seguridad

- Programar código es complejo
- Muchas veces tratando de programar con precaución y realizando todos los “que tal si…”, se reduce la funcionalidad de la aplicación.
- Se debe encontrar un punto medio entre:
  - la necesaria funcionalidad del programa
  - y los mecanismos que deben ser implementados para proveer seguridad
  - (mas complejidad a lo ya por sí complejo).

Ciclo de vida del desarrollo de sistemas (SDLC)

- Un ciclo de vida es una representación de cambios en el desarrollo.
- Un sistema tiene su propio ciclo de vida:
  - Iniciación: Necesidad para que un nuevo sistema sea definido.
  - Adquisición/Desarrollo: Nuevo sistema es creado o comprado.
  - Implementación: Nuevo sistema es instalado en ambiente de producción.
  - Operación/Mantención: El sistema es utilizado y cuidado.
  - Eliminación: El sistema es removido desde el ambiente de producción.

SDLC

Necesitará determinación:
•Percepción de una necesidad
•Link de la necesidad a la misión y objetivos de rendimiento
•Evaluación de alternativas a los activos actuales
•Preparación para la revisión de la inversión y presupuesto

•Investigación de mercado
•Estudio de factibilidad
•Análisis de requerimientos
•Análisis costo-beneficio
•Análisis de costos
•Plan de RM
•Planeamiento de adquisición.

•Instalación
•Inspección
•Pruebas de aceptación
•Entrenamiento inicial de usuarios
•Documentación

•Medición de rendimiento
•Modificación de contratos
•Operación
•Mantenimiento

•Aprobación de la eliminación
•Intercambio o venta
•Detección de la organización interna
•Transferencia y donación
•Cierre de contratos

Consideraciones de seguridad

•Categorización de seguridad
•Evaluación de riesgo preliminar

•Evaluación de riesgo
•Análisis de requerimientos funcionales de seguridad
•Aseguramiento de la seguridad
•Análisis de requerimientos
•Consideraciones de costos y reportería
•Desarrollo de controles de seguridad.
•Pruebas de seguridad y evaluaciones
•Otros planeamientos.

•Inspección y aceptación
•Integración de sistema
•Certificación de seguridad
•Acreditación de seguridad

•Gestión de la configuración y controles
•Monitoreo continuo

•Preservación de la información
•Sanitización de medios
•Eliminación de software y hardware

Nota: la ISO/IEC 27002 ISMS tiene una porción específica enfocado a esto.

Iniciación

- Se establecen las necesidades específicas del sistema
  - Se establece un problema o función que debe ser resuelta a través de tecnología.
  - ¿Qué es lo que necesitamos y para qué lo necesitamos?
    - esto no se debe tomar a la ligera.
    - No queremos que la compañía compre una solución equivocada por las razones equivocadas.
  - Una evaluación preliminar del riesgo debe ser realizada.
    - Una descripción inicial de los requerimientos de CIA.
    - Se debe definir el ambiente de producción en que va a operar e identificar potenciales vulnerabilidades.
    - Esto ayuda al equipo a identificar los controles de seguridad requeridos que el sistema puede necesitar.

Iniciación

- Desde un punto de vista de la seguridad, el tipo de preguntas son:
  - ¿Qué nivel de protección este sistema necesita proveer?
  - ¿Se debe proteger datos sensibles en descanso y en transito?
  - ¿Se debe proveer una autenticación de dos factores?
  - ¿Se debe proveer capacidades de monitoreo continuo?

Adquisición/Desarrollo

- Antes de que el sistema sea desarrollado o comprado, se debe cumplir:
  - Análisis de requerimientos (funciones necesarias)
  - Evaluación formal de riesgos
    - Se construye sobre la evaluación inicial
    - Identifica vulnerabilidades y amenazas
    - Los niveles potenciales de riesgos asociados a CIA.
    - Su resultado ayuda a construir el plan de seguridad

Adquisición/Desarrollo

- Análisis de los requerimientos funcionales de seguridad
  - Identifica los niveles de protección que deben ser proveídos por el sistema para cumplir toda la regulación, req. Legales, políticas.
- Análisis de los requerimientos que garantizan la seguridad.
  - Identifica todos los niveles de garantía que el sistema debe proveer.
  - Las actividades que se necesitan llevar a cabo para determinar el nivel deseado de confianza en el sistema.
    - Estas son tipos específicos de pruebas y evaluaciones.

Adquisición/Desarrollo

- Evaluaciones de terceras partes
  - Si el sistema va a ser comprado, una buena idea es revisar el nivel de servicio y calidad del proveedor específico.
- Plan de seguridad
  - El sistema debe contener controles de seguridad documentados para asegurar el cumplimiento de las necesidades de seguridad de la compañía.
  - Provee una completa descripción del sistema y los links a documentos claves de la compañía. Por ej:
    - Gestión de la configuración
    - Planes de pruebas y evaluación
    - Acuerdos de interconexión de sistemas
    - Acreditaciones de seguridad, etc.

Adquisición/Desarrollo

  - Pruebas de seguridad y plan de evaluación
    - Delinea como los controles de seguridad deben ser evaluados antes que el sistema sea aprobado y desplegado.
- Una vez hecho esto, la compañía puede desarrollar o comprar la solución.

Implementación

- Puede ser necesario llevar a cabo un proceso de certificación y acreditación (C&A), antes que el sistema pueda ser instalado formalmente en el ambiente de producción.
  - *Certificación:*
    - son las pruebas técnicas de un sistema.
    - Establece que los procedimientos de verificación son seguidos para asegurar la efectividad del sistema y sus controles de seguridad.

Implementación

- Acreditación:
  - es la autorización formal dada por la gerencia para permitir que el sistema opere en un ambiente específico.
  - La acreditación es basada en los resultados del proceso de certificación.
- Incluso si la organización no requiere de un proceso C&A, el sistema debe ser probado en un ambiente aparte.

Implementación

- Por ejemplo: un oficial de seguridad de una compañía que comprará un nuevo sistema para procesar datos confidenciales.
  - El oficial busca saber si este sistema es apropiado para estas tareas y si este va a proveer el nivel de protección necesario.
  - También busca saber si es compatible con su ambiente actual, que no reduzca la productividad y no abra nuevas puertas y nuevas amenazas.
  - El oficial puede pagar para que se realicen los procedimientos necesarios para certificar los sistemas o puede hacerlo internamente.
  - El equipo de evaluación puede realizar pruebas en: configuraciones de software, Hardware, Firmware, Diseño, Implementación, Procedimientos de sistemas, Controles físicos y de comunicación.

Operación/Mantención

- Un sistema debe tener una línea base establecida, relacionado con el hardware, software y la configuración de firmware definida durante la fase de implementación.
- En la fase de operación y mantención el monitoreo continuo debe ser restablecido para estar seguro que la línea base es cumplida.

Operación/Mantención

- Por ejemplo, una configuración de línea base para Windows 2008 puede dictar que:
  - Los logs de auditoría deben estar activos.
  - La configuración de registros debe tener ciertos valores.
  - Y que IPv6 debe estar deshabilitado.
- Muchas cosas pueden afectar las configuraciones con el tiempo, por ejemplo:
  - Instalación de nuevo software
  - Actividad de usuario
  - Software malicioso.
- Entonces estas configuraciones deben ser continuamente monitoreadas.

Operación/Mantención

- La gestión de la configuración y los procedimientos de control de cambios ayudan a cumplir que la línea base de los sistemas siempre se cumpla.
- Y si el sistema requiere cambios, deben ser probados y aprobados antes de ser implementados.
- La evaluación de vulnerabilidades y pruebas de penetración deben realizarse en esta fase. Este tipo de pruebas permiten reconocer nuevas vulnerabilidades y remediarlas.

Eliminación

- Cuando una organización no provee mas una función antes necesaria, se debe planear una transición del sistema y sus datos.
- Se puede necesitar mover los datos a un sistema diferente, archivarlos, descartarlos o destruirlos.
- Si los pasos adecuados no son realizados, un acceso no autorizado a información sensible puede ser llevado a cabo.
- Por ej. Los medios de almacenamiento de un sistema deben ser desmagnetizados, puestos a través de un proceso de zeroización o físicamente destruidos

FIN