Auditoria en Seguridad de sistemas

Beneficios

- Proteger la integridad de la información del sistema.
- Proteger de filtraciones de información y espionaje.
- Garantizar a la empresa y sus clientes un nivel de seguridad aceptable al momento de realizar sus trámites.

Cuando se realiza

Durante las fases de análisis, diseño o codificación de un proyecto de desarrollo.
Idealmente entre las fases de diseño y codificación.

Factores a estudiar:

- Nivel de seguridad de la empresa

  La información de una empresa es uno de los recursos de mayor valor, si bien los equipos y capitales tienen un valor muy significativo, la información de una empresa es la que permite que las funciones de la misma se desarrollen de manera apropiada y constituye a su vez el vínculo entre el cliente, la empresa y cada uno de los departamentos que la conforman.

  De acuerdo al nivel empresarial cada empresa necesita manejar un determinado volumen de información relacionada a las actividades de la misma. En correspondencia existe un nivel de seguridad informática necesario para garantizar la protección e integridad de dicha información. Este nivel viene dado por una serie de tecnologías y técnicas de programación creador para dicho fin.

  Preguntas a realizarse:

  ¿Qué volumen de información maneja la empresa?
  De acuerdo al tipo de actividades desarrolladas por la empresa, ¿Maneja la empresa información clasificada? ¿De qué tipo?
  ¿Los sistemas informáticos de la empresa tienen conexión con sistemas exteriores a la misma?
  ¿Existe dentro del departamento IT una división o especialista encargado de la seguridad?

- Zona Desmilitarizada (DMZ).

  La zona militarizada hace referencia a una arquitectura de sistemas en la cual se esquematizan las conexiones dentro del mismo en tres zonas
  Una red externa, normalmente internet
  Una red interna que contiene toda la información privada y confidencial de la empresa
  Una DMZ (Zona Desmilitarizada) que contiene información de la empresa que puede ser compartida y accesada desde el exterior
  Normalmente esta arquitectura se establece con un firewall que regula el funcionamiento de estas tres zonas y la comunicación entre ellas.

  Preguntas a realizarse:

  ¿La empresa implementa esquema de DMZ?
  ¿Es necesaria la implementación de este esquema?
  ¿Cómo están distribuidos los elementos del sistema dentro del esquema DMZ?
  ¿Esta distribución es la más apropiada?

- Criptología y Encriptamiento

  La criptologia consiste en la implementación de distintas funciones y procedimientos matemáticos y lingüísticos para codificar un segmento de información de tal forma que de ser interceptado no pueda ser interpretado sin la aplicación del procedimiento de desencriptacion.

  Existen muchas tecnologías y algoritmos de encriptación de hecho normalmente cada empresa se encarga de desarrollar su propio algoritmo para garantizar un buen nivel de seguridad.

  Preguntas a realizarse:

  ¿Se maneja algún esquema de encriptamiento?

  ¿Qué esquema de cifrado se maneja? ¿Se implementa el método de cifrado por llave privada y llave publica?

  ¿Es desarrollado por la empresa? ¿Quiénes dentro de la empresa tienen acceso al modelo?

  ¿El funcionamiento del método de encriptamiento funciona apropiadamente o presenta algún fallo?

- Medios de Respaldo

  Los medios de respaldo constituyen los diversos dispositivos y algoritmos con los cuales un sistema puede mantener una copia de la información que maneja en caso de un evento indeseado que pueda comprometer el funcionamiento del mismo o provocar la pérdida del registro original de información del mismo.

  Preguntas a realizarse:

  ¿Existe algún medio de respaldo de información? ¿Qué esquema de replicación de información maneja? ¿Es el más apropiado?

  ¿Sino existen los medios de respaldo es posible instalarlos?

  ¿Se manejan esquemas de redundancia?

  ¿La información respaldada cubre todos los registros de relevancia para la empresa?

- Procedimiento antes, Durante y Después de la contingencia

  Ante una contingencia existen preparaciones que deben estar presentes para cada fase de la situación, estas son:

  Antes de la contingencia: Se refiere al conjunto de medidas que buscan evitar que el evento ocurra. a nivel de software se refiere al conjunto de mecanismos que pueden medir niveles de tráfico, solicitudes o procesos anormales que pueden indicar el funcionamiento anormal del sistema y dar solución antes de que este se presente.

  Durante la contingencia: Otros mecanismos entran en juego a nivel de software, normalmente ante un funcionamiento irregular de un sistema, existen mecanismos que buscan ubicar y aislar la problemática en determinado modulo para no inhabilitar totalmente el sistema. En el peor de los casos debe existir un mecanismo que suspenda la utilización del sistema y realice automáticamente un respaldo de la información y transacciones realizadas para su posterior análisis por los desarrolladores.

  Después de la contingencia: Una contingencia es un evento pasajero, aun si causa la inhabilitación total del sistema eventualmente terminara y entonces entran en juego una serie de procesos para la recuperación y futura prevención de eventos similares.

  En esta fase se realiza una recolección de información, se realiza un diagnostico al sistema, equipos, registros y bases de datos para evaluar los daños. Posteriormente se debe analizar las posibles causas de dicho evento indeseado, basándose en el registro de transacciones realizado durante la contingencia, este análisis permitirá a futuro plantear una serie de medidas para evitar situaciones similares.