Unidad 3 / Escenario 5

Lectura fundamental

Seguridad en el ciclo de desarrollo de *software*

Contenido

Palabras clave: implementación, seguridad, ciclo, desarrollo, consejos, sensibilización, motivación.

1. Introducción

En la Unidad 2 comprendimos cuáles son los las actividades de seguridad que se deben implementar en cada una de las fases o etapas de desarrollo del modelo en cascada. Si bien esta teoría es básica y fundamental, la implementación de la misma no es tan fácil en la práctica.

La implementación de seguridad en el ciclo de desarrollo, como cualquier implementación de seguridad de la información, debe ser justificada de manera adecuada, esto con el objetivo de evitar que sea visto como un gasto más para las compañías, llegando inclusive a ser señalado como una actividad sin ningún tipo de valor.

En este escenario revisaremos una serie de consejos orientados a facilitar la implementación de la seguridad en el ciclo de desarrollo dentro de una empresa, información que le será muy útil si es usted el encargado de llevar a cabo dicho objetivo.

Antes de entrar en materia, recordemos cuáles son las actividades de seguridad que se implementan a lo largo de las etapas del ciclo de desarrollo en el modelo en cascada, información a recordar para entender esta lectura:

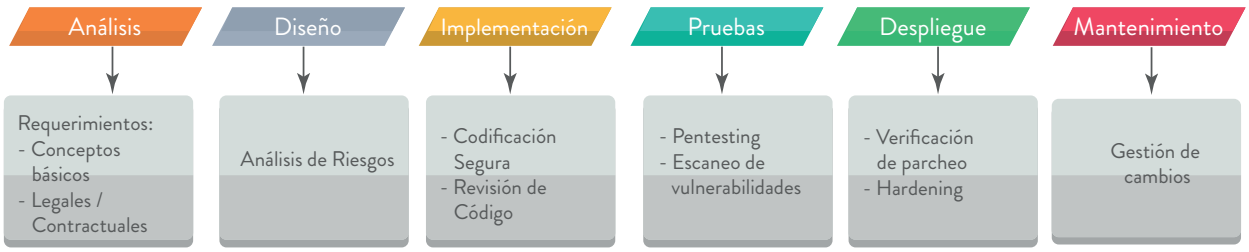

Figura 1. Actividades de seguridad para cada una de las etapas del modelo en cascada

Fuente: elaboración propia

2. Obtener el apoyo de la alta gerencia

La seguridad en el ciclo de desarrollo es un control vital que hace parte de la seguridad de la información de una compañía, pues muchos productos y/o servicios se soportan en aplicaciones WEB, por lo cual una falla de seguridad en la aplicación se puede ver reflejado en afectaciones de tipo:

- **Financiero:** los atacantes generalmente buscan vulnerar las aplicaciones con objetivos económicos, es decir buscan lucrarse a costa de la información que almacenan las aplicaciones. Adicionalmente cuando ocurre un incidente, el solo hecho de gestionarlo para mitigar su impacto, requiere de horas hombre de trabajo y herramientas especializadas (en algunos casos aplicar procesos de informática forense), elementos que representan costos que se pudieron haber evitado si se hubiese implementado seguridad en la aplicación desde un principio, confirmando que es mejor tomar una postura de seguridad preventiva que correctiva.
- **Reputacional o de imagen:** una falla de seguridad puede tener a nivel de imagen resultados devastadores. Suponga que usted tiene sus ahorros en una institución financiera y la aplicación WEB transaccional ha sido atacada y vulnerada, lo más probable es que esta situación lo "motive" a retirar su dinero cuanto antes de dicha entidad. Adicionalmente en la memoria del mercado, al menos por una buena cantidad de años, quedará la imagen de que la institución no protege el dinero y la información de los clientes, lo que fácilmente puede desencadenar en que la compañía no logre sus objetivos o inclusive quiebre por falta de clientes.
- **Legal:** una compañía que sufre una brecha de seguridad en una de sus aplicaciones puede tener complicaciones de tipo legal por demandas de los directamente afectados. Por ejemplo, si se tiene una aplicación que maneja historias médicas y durante un incidente de seguridad información sensible de pacientes (por ejemplo enfermedades de transmisión sexual o contagiosas) ha sido revelada, esos pacientes podrán demandar a la entidad de salud por una cantidad de dinero que "compense" que su información ha sido accedida por personal no autorizado.
- **Ambiental:** algunas aplicaciones se utilizan para controlar sistemas de control industrial, los cuales sirven para controlar válvulas, apertura y cierre de compuertas, sistemas de refrigeración, etc. Si se llega a presentar un incidente de seguridad sobre una de esas aplicaciones, podría generarse una afectación de tipo ambiental, por ejemplo un atacante podría abrir intencionalmente las compuertas de una represa de agua, generando inundaciones a los sectores aledaños, afectando la naturaleza, animales, fauna e inclusive la vida humana.

En todas las empresas, la palabra de la dirección es irrefutable, por lo que una orden debe ser cumplida a cabalidad. En línea con esto, la mejor estrategia para implementar seguridad en el ciclo de desarrollo es obtener el apoyo de la gerencia, de manera que sea una directriz de obligatorio cumplimiento.

Pero para que esa directriz se haga realidad, claramente es necesario convencer a la dirección, lo

cual se logra exponiéndole los potenciales impactos que puede tener una falla de seguridad en la aplicación WEB.

Su reto como especialista, será identificar los posibles impactos que tiene para la compañía una falla de seguridad en su o sus aplicaciones WEB, de manera que le pueda hablar en un lenguaje entendible cuál es el impacto de la falla, al menos en los aspectos financiero, de imagen, legal y ambiental.

Si es usted directamente quien debe exponer o sustentar el por qué se debe implementar seguridad en el ciclo de desarrollo, recuerde lo siguiente:

- Sea muy concreto, las direcciones normalmente no disponen de grandes cantidades de tiempo, por lo que los minutos que le sean dados deben ser aprovechados al máximo.
- Lleve un estimado de los costos que representa implementar todas las actividades de seguridad para cada una de las etapas del ciclo de desarrollo, idealmente demostrando que la inversión será varias veces menor que lo que le cuesta financieramente a la empresa una brecha o falla de seguridad.
- Lleve gráficas y números, este es el lenguaje que más se acomoda y gusta a las altas direcciones de las empresas.
- Si han ocurrido incidentes en empresas de la competencia o del sector, relacionados con fallas en sus aplicaciones WEB, preséntelos y demuestre que efectivamente esos eventos acontecen, demostrando que no es paranoia.

Si en su compañía existen áreas de riesgo o auditoría, es posible que tengan información que le ayude a alimentar y fortalecer su sustentación. Adicionalmente propóngales apoyar su iniciativa, entre más existan áreas que respalden su idea, mejor será visto por la dirección

¿Sabía qué...?

es de vital importancia obtener apoyo de la alta dirección para implementar seguridad en el ciclo de desarrollo.

3. Identifique si hace parte de un compromiso contractual o legal

Este consejo está directamente relacionado con la actividad "Requerimientos Legales/Contractuales" que veíamos en la etapa de análisis del modelo en cascada. Básicamente lo que se busca establecer son esos requisitos que las leyes del país o los contractos con los clientes hacen que sea obligatorio implementar seguridad en el ciclo de desarrollo.

Si usted tiene identificados estos tipos de requerimientos, la tarea de implementar seguridad en el ciclo de desarrollo va a ser mucho más fácil, pues no es un tema opcional, es una obligación. De incumplir con esta obligación, la compañía de igual manera se puede exponer a:

- Afectaciones económicas: cobrando multas o sanciones por un porcentaje del valor del contrato.
- Finalización o cancelación del contrato, en especial cuando el cliente ha establecido un plazo de cumplimiento y este no ha sido cumplido.
- Otras sanciones, siempre de carácter negativo.

Usted puede identificar estas sanciones para "motivar" a aquellas personas que no están cumpliendo con el requisito legal/contractual, escalándolo a nivel de empresa al nivel que sea necesario, inclusive a la alta dirección.

Recordemos algunos ejemplos de este tipo de requisitos:

- Circular 042 de 2012 (Superintendencia Financiera de Colombia, 2012)
- SOX Ley Sarbanes-Oaxley (107th United States Congress, 2002)
- Ley de protección de datos personales 1581 de 2012 (Congreso de Colombia, 2012)
- PCI DSS (PCI Security Standards Council, 2016)
- SO/IEC 27001 (International Organization for Standardization, 2013)

¿Sabía qué...?

algunas leyes y contractos obligan la implementación de seguridad en el ciclo de desarrollo.

4. Sensibilización y capacitación

La seguridad en el ciclo de desarrollo, como parte integral de la seguridad de la información, debe garantizar un adecuado nivel de sensibilización y capacitación que motive a los involucrados a implementar las actividades y controles de seguridad que tengan a su cargo.

A muy pocas personas les agrada la idea de tener que ejecutar una actividad que probablemente no saben hacer, o peor aún, que ni siquiera entienden. Por lo anterior, es necesario establecer un programa de sensibilización y capacitación que desarrolle las competencias necesarias para llevar a cabo la implementación de las actividades de seguridad en el ciclo de desarrollo de software.

A continuación se establece un ejemplo de los temas que debe podría ese plan de sensibilización y capacitación, para cada una de las áreas que normalmente intervienen en el proceso:

Desarrollo:

- Conceptos básicos de seguridad
- Identificación de requerimientos
- Codificación segura
- Revisión estática y dinámica de código
- Gestión de cambios

Seguridad de la información o informática:

- Identificación de requerimientos
- Análisis de riesgos
- Pentesting
- Escaneo de vulnerabilidades

Administradores de infraestructura:

- Hardening
- Parcheo

Esta sensibilización y capacitación puede ser contratada o desarrollada al interior de la compañía, en cualquier caso se recomienda entregar a los participantes un certificado de asistencia, pues es algo que le cae muy bien a sus respectivas hojas de vida.

Como parte de la sensibilización, recuérdeles a los participantes que ellos serán al final los principales beneficiados, pues se "ahorrarán" el trabajo de realizar investigaciones, elaboración de informes y demás actividades propias de la gestión de incidentes, pues como ya lo hemos dicho anteriormente, la implementación de seguridad es una actividad principalmente preventiva.

¿Sabía qué...?

La formación es una excelente técnica de motivación en pro de la implementación de seguridad en el ciclo de desarrollo.

5. Implementación progresiva

Cuando se busca implementar seguridad en el ciclo de desarrollo, una de las prácticas más comunes (pero poco efectivas) consiste en pretender implementar todas las actividades de seguridad en paralelo. En realidad es poco efectivo porque varios motivos:

- Representa una elevada carga que puede desmotivar al equipo de trabajo.
- Por la falta de experiencia o de madurez, al final no se ejecuta ninguna actividad con el suficiente nivel de calidad.
- Puede interpretarse como una falta de orden.

Por lo anterior, en la práctica se recomienda implementar las actividades de manera progresiva. Con el objetivo de demostrar las implicaciones que tiene una aplicación insegura, es recomendable iniciar con una prueba de Pentesting, pues esta permitirá entre otras cosas:

- Evidenciar que las vulnerabilidades existen y pueden ser explotadas.
- Explicar el riesgo a nivel de compañía que se tiene, lo cual se recomienda llevar al novel más alto de la compañía, preferiblemente a la dirección.
- Demostrar que no se trata de una idea aislada de los especialistas de seguridad.
- Es una prueba "tangible" y evitamos que el tema se encasille como "teórico" o "académico"

Esta es una recomendación aplicada cuando la aplicación ya ha sido desarrollada. Cada empresa deberá definir el orden en el cuál se implementarán las actividades, pero es claro que se deben implementar todas para lograr un nivel de seguridad adecuado. Para establecer el orden de las actividades, se deben tener en cuenta los siguientes aspectos:

- Recursos humanos
- Recursos técnicos
- Objetivos del área de desarrollo
- Conocimientos
- Otros proyectos en curso que impidan o afecten la implementación de la seguridad en el ciclo de desarrollo

Una vez revisados estos aspectos, se construye el proyecto de implementación, el cuál como ya lo hemos visto, deberá tener el apoyo de la alta dirección para obtener los resultados esperados.

En síntesis...

existen una serie de consejos que deben ser aplicados para facilitar la implementación de seguridad en el ciclo de desarrollo de software.

Referencias

Superintendencia Financiera de Colombia. (2012). *Circular Externa 042 de 2012*. Recuperado de https://m.superfinanciera.gov.co/descargas?com=institucional&name=pubFile31164&downloadname=ce042_12.doc

107th United States Congress. (2002). *Sarbanes–Oxley Act of 2002*. Recuperado de https://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf

Congreso de Colombia. (2012). *Ley estatutaria 1581 de 2012.* Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

PCI Security Standards Council. (2016). *Requisitos y procedimientos de evaluación de seguridad.* Recuperado de https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_3_es-LA.pdf?agreement=true&time=1512747614564

International Organization for Standardization. (2013). *Sistemas de Gestión de Seguridad de la Información*. Recuperado de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Seguridad en el Ciclo de Desarrollo

Unidad 3: Integración de la seguridad con modelos de desarrollo de *software* existentes

Escenario 5: Consejos para integrar seguridad en el ciclo de desarrollo de *software*

Autor: Miguel Ángel Zambrano Puentes

Asesor Pedagógico: Edwin Mojica Quintero

Diseñador Gráfico: Brandon Steven Ramírez Carrero

Asistente: Ginna Quiroga