**Seguridad OWASP**

Anteriormente, usted aprendió que los analistas de ciberseguridad ayudan a mantener los datos seguros y reducir el riesgo para una organización mediante el uso de una variedad de marcos de seguridad, controles y principios de seguridad. En esta lectura, aprenderá más sobre el Proyecto Abierto de Seguridad en Aplicaciones Web, recientemente renombrado Open Worldwide Application Security Project® (OWASP), los principios de seguridad y cómo los utilizan los analistas de nivel básico.

* **Principios de seguridad**

En el lugar de trabajo, los principios de seguridad están integrados en las tareas diarias. Ya sea analizando registros, supervisando un panel de administración de información y eventos de seguridad (SIEM) o utilizando un escáner de vulnerabilidades, utilizará estos principios de alguna manera.

Anteriormente, se le presentaron varios principios de seguridad OWASP. Estos incluyen:

* **Minimizar la superficie de ataque**: La superficie de ataque se refiere a todas las vulnerabilidades potenciales que un Agente de amenaza podría explotar.
* **Principio de privilegio mínimo**: Los usuarios tienen la menor cantidad de acceso necesario para realizar sus tareas cotidianas.
* **Defensa en profundidad**: Las organizaciones deben disponer de diversos controles de seguridad que mitiguen los riesgos y amenazas.
* **Separación de funciones**: Las acciones críticas deben depender de varias personas, cada una de las cuales debe seguir el principio de privilegio mínimo.
* **Seguridad sencilla**: Evite las soluciones innecesariamente complicadas. La complejidad dificulta la seguridad.
* Solucione **correctamente** los problemas de seguridad: Cuando se produzcan incidentes de seguridad, identifique la causa raíz, contenga el impacto, identifique las vulnerabilidades y lleve a cabo pruebas para garantizar que la corrección se realiza correctamente.
* **Principios de seguridad OWASP adicionales**

A continuación, usted aprenderá acerca de cuatro principios de seguridad OWASP adicionales que los analistas de ciberseguridad y sus equipos utilizan para mantener las operaciones de la organización y las personas a salvo.

1. **Establecer valores predeterminados seguros**

Este principio significa que el estado de seguridad óptimo de una aplicación es también su estado por defecto para los usuarios; debería costar un trabajo extra hacer que la aplicación sea insegura.

1. **Fallar con seguridad**

Fallar de forma segura significa que cuando un control falla o se detiene, debe hacerlo pasando por defecto a su opción más segura. Por ejemplo, cuando un cortafuegos falla, debería simplemente cerrar todas las conexiones y bloquear todas las nuevas, en lugar de empezar a aceptarlo todo.

1. **No confíes en los servicios**

Muchas organizaciones trabajan con socios externos. Estos socios externos suelen tener políticas de seguridad diferentes a las de la organización. Y la organización no debe confiar explícitamente en que los sistemas de sus socios sean seguros. Por ejemplo, si un proveedor externo realiza el seguimiento de los puntos de recompensa de los clientes de una aerolínea, ésta debería asegurarse de que el saldo es exacto antes de compartir esa información con sus clientes.

1. **Evitar la seguridad por oscuridad**

La seguridad de los sistemas clave no debe basarse en mantener ocultos los detalles. Considere el siguiente ejemplo FROM OWASP (2016): OWASP Mobile Top 10

La seguridad de una aplicación no debería basarse en mantener en secreto el código fuente. Su seguridad debe basarse en muchos otros factores, incluidas políticas de contraseñas razonables, defensa en profundidad, límites de transacciones comerciales, arquitectura de red sólida y controles de fraude y auditoría.

* **Puntos clave**

Los profesionales de la Ciberseguridad aplican constantemente principios de seguridad para salvaguardar a las organizaciones y a las personas a las que sirven. Como analista de seguridad principiante, puede utilizar estos principios de seguridad para promover prácticas de desarrollo seguras que reduzcan los riesgos tanto para las empresas como para los usuarios.

**Más información sobre auditorías de seguridad**

Anteriormente, se le presentó cómo planificar y completar una auditoría interna de Seguridad. En esta lectura, aprenderá más sobre las auditorías de Seguridad, incluyendo las metas y objetivos de las auditorías.

* **Auditorías de seguridad**

Una **Auditoría** de seguridad es una revisión de los Controles de seguridad, políticas y Procedimientos de una organización contra un conjunto de expectativas. Las auditorías son revisiones independientes que evalúan si una organización cumple los criterios internos y externos. Los criterios internos incluyen las políticas, los procedimientos y las mejores prácticas descritas. Los criterios externos incluyen el cumplimiento normativo, las leyes y las regulaciones federales.

Además, una Auditoría de seguridad puede utilizarse para evaluar los Controles de seguridad establecidos por una organización. Como recordatorio, los **Controles de seguridad** son salvaguardas diseñadas para reducir riesgos de Seguridad específicos.

Las auditorías ayudan a garantizar que se realizan controles de seguridad (es decir, el seguimiento diario de la información de seguridad y los paneles de gestión de eventos), para identificar amenazas, riesgos y vulnerabilidades. Esto ayuda a mantener la postura de seguridad de una organización. Y, si hay Problemas de Seguridad, debe existir un proceso de remediación.

* **Metas y objetivos de una auditoría**

El objetivo de una auditoría es garantizar que las prácticas de tecnología de la información (TI) de una organización cumplen las normas del sector y de la organización. El Objetivo es identificar y abordar las áreas de remediación y crecimiento. Las auditorías proporcionan dirección y claridad al identificar cuáles son los fallos actuales y desarrollar un plan para corregirlos.

Deben realizarse auditorías de seguridad para salvaguardar los Datos y evitar sanciones y multas de las agencias gubernamentales. La frecuencia de las auditorías depende de las leyes locales y de las regulaciones federales de cumplimiento.

* **Factores que afectan a las auditorías**

Los factores que determinan los tipos de auditorías que implementa una organización incluyen:

* Tipo de industria
* Tamaño de la organización
* Vínculos con las regulaciones gubernamentales aplicables
* La ubicación geográfica de un negocio (Business-to-Business)
* Una decisión empresarial de adherirse a un cumplimiento normativo específico
* **Función de los marcos y controles en las auditorías**

Junto con el cumplimiento, es importante mencionar el papel de los marcos y controles en las auditorías de Seguridad. Marcos como el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF) y la serie de normas internacionales para la seguridad de la información (ISO 27000) están diseñados para ayudar a las organizaciones a prepararse para las auditorías de seguridad de cumplimiento normativo. Al adherirse a estos y otros marcos relevantes, las organizaciones pueden ahorrar tiempo a la hora de realizar auditorías externas e internas. Además, los marcos, cuando se utilizan junto con los controles, pueden apoyar la capacidad de las organizaciones para alinearse con los Requisitos y Estándares de cumplimiento normativo.

Existen tres categorías principales de controles a revisar durante una auditoría, que son los controles administrativos y/o de gestión, técnicos y físicos.

* **Lista de control de auditoría**

Es necesario crear una lista de comprobación de la auditoría antes de llevarla a cabo. Por lo general, una lista de comprobación se compone de las siguientes áreas de atención:

**Identificar el alcance de la auditoría**

* La auditoría debe:
  + Lista de los recursos que se evaluarán (por ejemplo, los firewalls están configurados correctamente, la PII está segura, los recursos físicos están bloqueados, etc.)
  + Indicar cómo la auditoría ayudará a la organización a alcanzar sus objetivos deseados
  + Indique con qué frecuencia debe realizarse una auditoría
  + Incluya una evaluación de las políticas, protocolos y procedimientos de la organización para asegurarse de que funcionan según lo previsto y de que los empleados los implementan

**Completar una evaluación de riesgos**

* Se utiliza una Evaluación de riesgos para valorar los riesgos organizativos identificados en relación con el Presupuesto, los controles, los procesos internos y los Estándares externos (es decir, las Regulaciones).

**Realizar la auditoría**

* Al realizar una auditoría interna, evaluará la seguridad de los recursos identificados

**Cree un plan de mitigación**

* Un plan de mitigación es una estrategia establecida para reducir el nivel de riesgo y los posibles costes, sanciones u otros problemas que puedan afectar negativamente a la postura de seguridad de la organización.

**Comunicar los resultados a las partes interesadas**

* El resultado final de este proceso es la presentación de un informe detallado de los resultados, las mejoras sugeridas necesarias para reducir el nivel de riesgo de la organización y las Regulaciones y Estándares a los que la organización debe adherirse.
* **Puntos clave**

En esta lectura ha aprendido más sobre las auditorías de Seguridad, incluyendo qué son; por qué se llevan a cabo; y el papel de los frameworks, controles y cumplimiento en las auditorías.

Aunque hay mucho más que aprender acerca de las auditorías de Seguridad, esta introducción está destinada a apoyar su capacidad para completar una auditoría propia para una actividad de auto-reflexión del portafolio más adelante en este curso.