Dominios de Seguridad que los analistas de Ciberseguridad deben conocer

Como analista, puede explorar diversas áreas de la ciberseguridad que le interesen. Una forma de explorar esas áreas es comprendiendo los diferentes dominios de Seguridad y cómo se utilizan para organizar el trabajo de los profesionales de la Seguridad. En esta lectura aprenderá más sobre los ocho dominios de Seguridad del CISSP y cómo se relacionan con el trabajo que realizará como analista de seguridad.

Primer dominio: Seguridad y Gestión de riesgos

Todas las organizaciones deben desarrollar su Postura de seguridad. Postura de seguridad es la capacidad de una organización para gestionar su defensa de los activos y datos críticos y reaccionar ante los cambios. Entre los elementos del dominio de la Gestión de riesgos y seguridad que repercuten en la postura de seguridad de una organización se incluyen:

- Metas y objetivos de Seguridad
- Procesos de mitigación de riesgos
- Cumplimiento normativo
- Planes de continuidad del negocio (Business-to-Business)
- Regulaciones legales
- Ética profesional y organizativa

La Seguridad de la información, o InfoSec, también está relacionada con este dominio y se refiere a un conjunto de procesos establecidos para asegurar la información. Una organización puede utilizar manuales de procedimientos e implementar el Entrenamiento como parte de su programa de Seguridad y Gestión

de Riesgos, basándose en sus necesidades y en el riesgo percibido. Existen muchos procesos de diseño de InfoSec, tales como:

- Respuesta ante incidentes
- Gestión de vulnerabilidades
- Seguridad de las aplicaciones
- Seguridad de la nube
- Seguridad de las infraestructuras

A modo de ejemplo, es posible que un Equipo de seguridad necesite modificar el tratamiento de la información de identificación personal (PII) para cumplir el Reglamento General de Protección de Datos de la Unión Europea (RGPD).

Segundo dominio: Seguridad de los recursos

La seguridad de los activos implica gestionar los procesos de ciberseguridad de los activos de la organización, incluido el almacenamiento, el mantenimiento, la retención y la destrucción de datos físicos y virtuales. Dado que la pérdida o el robo de activos puede exponer a una organización y aumentar el nivel de riesgo, es esencial llevar un registro de los recursos y de los datos que contienen. Llevar a cabo un análisis del impacto en la seguridad, establecer un plan de recuperación y gestionar la exposición de los datos dependerá del nivel de riesgo asociado a cada activo. Los analistas de seguridad pueden necesitar almacenar, mantener y conservar los datos creando copias de seguridad para asegurarse de que son capaces de restaurar el entorno si un incidente de seguridad pone en peligro los datos de la organización.

Tercer dominio: Arquitectura de seguridad e ingeniería

Este dominio se centra en la gestión de la Seguridad de los datos. Garantizar la existencia de herramientas, sistemas y procesos eficaces ayuda a proteger los recursos y los Datos de una organización. Los arquitectos e ingenieros de Seguridad crean estos procesos.

Un aspecto importante de este dominio es el concepto de Responsabilidad compartida. Responsabilidad compartida significa que todas las personas implicadas asumen un papel activo en la reducción del Riesgo durante el diseño de un sistema de Seguridad. Entre los principios de diseño adicionales relacionados con este dominio, que se tratan más adelante en el programa, se incluyen:

- Modelado de amenazas
- Mínimo privilegio
- Defensa en profundidad
- Fallar con seguridad

- Separación de funciones
- Mantenga la sencillez
- Confianza cero
- Confiar pero verificar

Un ejemplo de gestión de datos es el uso de una herramienta de administración de información y eventos de seguridad (SIEM) para monitorizar las señales relacionadas con un inicio de sesión o una actividad de usuario inusuales que podrían indicar que un Agente de Amenaza está intentando acceder a datos privados.

Cuarto dominio: Comunicación y Seguridad de red

Este dominio se centra en gestionar y proteger las redes físicas y las comunicaciones inalámbricas. Esto incluye las comunicaciones in situ, remotas y en la Nube.

Las organizaciones con entornos de trabajo remotos, híbridos e in situ deben garantizar que los datos permanecen seguros, pero gestionar las conexiones externas para asegurarse de que los trabajadores remotos acceden de forma segura a las redes de una organización es todo un reto. El diseño de controles de seguridad de la red -como el acceso restringido a la red- puede ayudar a proteger a los usuarios y garantizar que la red de una organización permanece segura cuando los empleados viajan o trabajan fuera de la oficina principal.

Quinto dominio: Gestión de identidad y acceso

El dominio de Gestión de identidad y acceso (IAM) se centra en mantener la seguridad de los datos. Para ello, garantiza que las identidades de los usuarios sean fiables y estén autenticadas y que el acceso a los recursos físicos y lógicos esté autorizado. Esto ayuda a evitar usuarios no autorizados, al tiempo que permite a los usuarios autorizados realizar sus tareas.

Esencialmente, IAM utiliza lo que se conoce como el principio de privilegio mínimo, que es el concepto de conceder sólo el acceso y la autorización mínimos necesarios para completar una tarea. Como ejemplo, se podría pedir a un analista de ciberseguridad que se asegure de que los representantes del servicio de atención al cliente sólo puedan ver los datos privados de un cliente, como su número de teléfono, mientras trabajan para resolver el problema del cliente; después, que elimine el acceso cuando el problema del cliente esté resuelto.

Sexto dominio: Evaluación y pruebas de seguridad

El dominio de la evaluación y las pruebas de seguridad se centra en identificar y mitigar los riesgos, las amenazas y las vulnerabilidades. Las evaluaciones de la Seguridad ayudan a las organizaciones a determinar si sus sistemas internos son seguros o están en riesgo. Las organizaciones podrían emplear probadores de penetración, a menudo denominados "pen testers", para encontrar vulnerabilidades que podrían ser explotadas por un agente de amenaza.

Este dominio sugiere que las organizaciones lleven a cabo pruebas de control de la seguridad, así como que recopilen y analicen datos. Además, hace hincapié en la importancia de realizar auditorías de seguridad para monitorear y reducir la probabilidad de una violación de datos. Para contribuir a este tipo de tareas, los profesionales de la ciberseguridad pueden encargarse de auditar los permisos de los usuarios para validar que éstos tienen los niveles correctos de acceso a los sistemas internos.

Séptimo dominio: Operaciones de seguridad

El dominio de las operaciones de seguridad se centra en la investigación de una posible violación de datos y en la implementación de medidas preventivas después de que se haya producido un incidente de seguridad. Esto incluye el uso de estrategias, procesos y herramientas como:

- Entrenamiento y concienciación
- Informes y documentación
- Detección y prevención de intrusiones
- Herramientas SIEM
- Gestión de registros
- Administración de incidentes
- Manuales de estrategias
- Análisis forense posterior a la violación
- Reflexión sobre las lecciones aprendidas

Los profesionales de la ciberseguridad implicados en este dominio trabajan en equipo para gestionar, prevenir e investigar amenazas, riesgos y vulnerabilidades. Estas personas están formadas para hacer frente a ataques activos, como el acceso a grandes cantidades de datos desde la red interna de una organización, fuera de las horas normales de trabajo. Una vez que se identifica una amenaza, el Equipo trabaja diligentemente para mantener los datos privados y la Información a salvo de los actores de la amenaza.

Dominio ocho: Seguridad en el desarrollo de software

El dominio de la Seguridad en el desarrollo de software se centra en el uso de prácticas y directrices de programación seguras para crear aplicaciones seguras. Having secure applications helps deliver secure and reliable services, which helps protect organizations and their users.

La Seguridad debe incorporarse a cada elemento del ciclo de vida del desarrollo de software, desde el diseño y el desarrollo hasta las pruebas y la publicación. Para lograr la seguridad, el proceso de desarrollo de software debe tener la seguridad en mente en cada paso. La Seguridad no puede ser una ocurrencia tardía.

Realizar pruebas de Seguridad de la aplicación puede ayudar a garantizar que se identifican las vulnerabilidades y se mitigan en consecuencia. Es necesario disponer de un sistema para probar las convenciones de programación, los ejecutables de software y las medidas de seguridad integradas en el software. Contar con profesionales de la garantía de calidad y de las pruebas de penetración que garanticen que el software cumple las normas de seguridad y rendimiento es también una parte esencial del proceso de desarrollo del software. Por ejemplo, a un analista principiante que trabaje para una empresa farmacéutica se le puede pedir que se asegure de que la encriptación está correctamente configurada para un nuevo dispositivo médico que almacenará datos privados de los pacientes.

Puntos clave

En esta lectura, usted aprendió más sobre las áreas de enfoque de los ocho dominios de Seguridad CISSP. Además, aprendió sobre InfoSec y el principio de privilegio mínimo. Estar familiarizado con estos dominios de seguridad y los conceptos relacionados le ayudará a obtener una visión del dominio de la Ciberseguridad.