Dominios de ciberseguridad

Dominio 1: Seguridad y gestión de riesgos

Todas las organizaciones deben desarrollar su postura de seguridad, es decir, su capacidad para gestionar la defensa de sus activos y datos críticos así como para reaccionar frente a los cambios. Algunos de los elementos del dominio de seguridad y gestión de riesgos que impactan en la postura de seguridad de una organización son:

- Metas y objetivos de seguridad.
- Procesos de mitigación de riesgos.
- Cumplimiento normativo (compliance).
- Planes para la continuidad del negocio.
- Normativa.
- Ética profesional y organizacional.

La seguridad de la información, o InfoSec, también está relacionada con este dominio y se refiere a un conjunto de procesos establecidos para proteger la información. Una

organización puede usar guías o manuales de estrategias (o procedimientos) e implementar la formación como parte de su programa de seguridad y gestión de riesgos, en función de sus necesidades y de los riesgos percibidos. Existen muchos procesos de diseño de InfoSec, como:

- Respuesta a incidencias.
- Gestión de las vulnerabilidades.
- Seguridad en la aplicación.
- Seguridad en la nube.
- Seguridad de la infraestructura.

Por ejemplo, un equipo de seguridad puede tener que modificar el tratamiento de la información de identificación personal (PII) para cumplir el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Dominio 2: Seguridad de los activos

La seguridad de los activos implica gestionar los procesos de ciberseguridad de los activos organizacionales, lo cual incluye almacenamiento, mantenimiento, conservación y destrucción de datos físicos y virtuales. Dado que la pérdida o el robo de activos puede exponer a una compañía y aumentar el nivel de riesgo, es esencial hacer un seguimiento de los activos y los datos que contienen. Realizar 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. Las/los analistas de seguridad pueden necesitar almacenar, mantener y conservar datos mediante la creación de copias de seguridad, para asegurarse de poder restaurar el entorno en caso de que un incidente de seguridad ponga en riesgo los datos de la organización.

Dominio 3: Arquitectura y diseño de seguridad

Este dominio se enfoca en la gestión de la seguridad de los datos. Garantizar la existencia de herramientas, sistemas y procesos eficaces ayuda a proteger los activos y datos de una organización. Estos procesos son creados por quienes se dedican a la arquitectura e ingeniería de seguridad.

Un aspecto importante de este dominio es el concepto de responsabilidad compartida, que implica que todas las personas involucradas asuman un papel activo en la reducción del riesgo durante el diseño de un sistema de seguridad. Los principios de diseño adicionales relacionados con este dominio, que se tratarán más adelante en el programa, son:

- Simulación de amenazas.
- Principio de privilegio mínimo.
- Defensa en profundidad.

- Fallar de forma segura.
- Separación de funciones.
- Simplicidad.
- Confianza cero.
- Confianza tras verificación.

Un ejemplo de administración de datos es el uso de una herramienta de gestión de eventos e información de seguridad (SIEM) para monitorear los indicadores relacionados, ante un inicio de sesión o una actividad de usuario inusuales, que podrían indicar que un agente de amenaza está intentando acceder a datos privados.

Dominio 4: Seguridad de las comunicaciones y de redes

Este dominio se centra en la gestión y la seguridad de las redes físicas y las comunicaciones inalámbricas, incluidas las que son en el mismo lugar, remotas y en la nube.

Las organizaciones que cuentan con entornos de trabajo remotos, híbridos y presenciales (en el lugar) deben asegurarse de que los datos permanezcan seguros y, a la vez, gestionar las conexiones externas y garantizar que quienes trabajan a distancia accedan de forma segura a las redes. Diseñar controles de seguridad de red, como el acceso restringido, puede ayudar a proteger a los/las usuarios/as y garantizar que la red de una empresa permanezca segura cuando sus empleados/as viajan o trabajan fuera de la oficina principal.

Dominio 5: Gestión de identidades y accesos

El dominio de gestión de identidades y accesos (IAM) se centra en mantener la seguridad de los datos, asegurándose de que las identidades de los/las usuarios/as sean confiables y estén autenticadas, y que el acceso a los activos físicos y lógicos esté autorizado. Esto ayuda a prevenir el acceso de usuarios/as no autorizados/as, al tiempo que permite que quienes están autorizados/as realicen sus tareas.

Básicamente, el IAM utiliza lo que se conoce como el principio de privilegio mínimo, que es el concepto de otorgar solo el acceso y la autorización mínimos necesarios para completar una tarea. Por ejemplo, a un/a analista de ciberseguridad se le puede pedir que se asegure de que las/los representantes del servicio de atención al cliente solo puedan ver los datos privados de un/a cliente, como su número de teléfono, mientras trabajan en la resolución de un problema. Una vez resuelto el inconveniente, se deberá eliminar el acceso.

Dominio 6: Evaluación y pruebas de seguridad

El dominio de evaluación y pruebas de seguridad se enfoca en identificar y mitigar riesgos, amenazas y vulnerabilidades. Las evaluaciones de seguridad ayudan a las empresas a determinar si sus sistemas internos son seguros o están en riesgo. Las organizaciones

pueden emplear pruebas de penetración, un proceso conocido como pentesting, para encontrar vulnerabilidades que podría aprovechar un agente de amenaza.

Este dominio sugiere que las organizaciones realicen pruebas de control de la seguridad, y que recopilen y analicen datos. Además, se enfatiza la importancia de realizar auditorías de seguridad para monitorear y reducir la probabilidad de que se produzca una filtración de datos. Para contribuir a este tipo de tareas, las y los profesionales de la ciberseguridad pueden encargarse de auditar los permisos de usuarios/as, a fin de confirmar si tienen los niveles correctos de acceso a los sistemas internos.

Dominio 7: Operaciones de seguridad

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

- Entrenamiento y concientización.
- Informes y documentación.
- Detección y prevención de intrusiones.
- Herramientas SIEM.
- Gestión de registros.
- Gestión de incidentes.
- Manuales de estrategias (playbooks).
- Análisis forense posterior a una filtración.
- Reflexión sobre las lecciones aprendidas.

Los y las profesionales de ciberseguridad involucrados/as en este dominio trabajan en equipo para gestionar, prevenir e investigar amenazas, riesgos y vulnerabilidades. Están entrenados/as para hacer frente a ataques activos, como el acceso a grandes cantidades de datos desde la red interna de una organización, fuera del horario normal de trabajo. Una vez identificada una amenaza, el equipo trabaja para mantener a salvo los datos y la información privada.

Dominio 8: Seguridad en el desarrollo de software

El dominio de seguridad en el desarrollo de software se enfoca en el uso de prácticas y políticas de programación para crear aplicaciones seguras. Contar con ellas ayuda a ofrecer servicios seguros y fiables, y a proteger a las organizaciones y sus usuarios/as.

La seguridad debe incorporarse en cada elemento del ciclo de vida del desarrollo de software, desde el diseño y el desarrollo hasta las pruebas y el lanzamiento. Para lograr la

seguridad efectiva, es necesario tener en mente la seguridad en cada paso del proceso de desarrollo de software. No se la puede considerar como un aspecto secundario o posterior.

Realizar pruebas de seguridad de las aplicaciones puede ayudar a garantizar que las vulnerabilidades sean identificadas y mitigadas adecuadamente. Además, es necesario disponer de un sistema que permita evaluar las convenciones de programación, los ejecutables de software y las medidas de seguridad incorporadas en el mismo. También, es clave contar con profesionales de control de calidad y de pruebas de penetración que se encarguen de verificar que el software cumpla con los estándares de seguridad y rendimiento establecidos. Por ejemplo, un/a analista de nivel inicial que trabaje para una empresa farmacéutica podría tener la responsabilidad de asegurarse de que el cifrado, o encriptación, esté configurado correctamente en un nuevo dispositivo médico que almacenará datos privados de pacientes.