Certified Tech Developer
The Ultimate Degree

Práctica integradora

Seguridad Informática - Equipo 9

Integrantes:

Santiago Chacon
Sebastian Marello
Sanctiago Arciniegas
Jhonathan barrera
Camilo Sanchez
Yerson Arboleda

Práctica de diseño de plan de seguridad

Práctica integradora

Objetivo

Para empezar a poner en práctica los conocimientos adquiridos, realizaremos la siguiente actividad. Se crearán grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.

Microdesafío 📌

La empresa que se les haya asignado los contrata como asesores de seguridad, ya que creen que es una parte fundamental para resguardar sus activos. En base a lo visto en clase y clases anteriores deben hacer:

1. Un análisis de la situación actual de cada empresa que se les haya asignado.
2. Para cada escenario planteado, crear un plan de seguridad

3. Este plan debe ser de 6 pasos e incluir: seguridad lógica, física, pasiva, activa y controles de medida de seguridad y de vulnerabilidades que podrían explotar los atacantes.

Esta serie de pasos y sugerencias debe ser presentada en un documento que pueda ser compartido con otras personas, especificando el grupo que son y el escenario que les tocó.

Escenarios para grupos 1, 3, 5, 7, 9, 11

- Empresa emergente dedicada a la venta de productos fertilizantes para campos con una capacidad financiera acotada. Todos sus empleados trabajan on site y están dispuestos a recibir capacitación. Poseen actualmente dos personas encargadas de sistemas, las cuales manejan información sensible, pero que todos los usuarios pueden ver (no es política de la empresa). No realizan copias de información porque no las creen convenientes. Poseen una página web donde hay catálogos y los clientes pueden hacer compras a través de la misma.

RESPUESTAS

1.Análisis: Notamos que esta empresa no cuenta con dispositivos físicos de protección, además, existe información sensible que puede ser vulnerada, así como tampoco realizan copias de seguridad de la información en general.

Vemos que en la página web es necesario verificar que no hayan vulnerabilidades en la pasarela de pagos.

Analizando la situación y conociendo la predisposición del personal vemos oportuno capacitar a los empleados para implementar buenas prácticas en seguridad informática.

2.Plan de seguridad:

Seguridad Física;

Agregar dispositivos de protección física como, pararrayos, extintores, detectores de humo, alarma contra intrusos, UPS. Realizar copias de seguridad o backups de los datos completos e incrementales al igual que sistemas redundantes.

Vulnerabilidades: Revisar los últimos CVE relacionados con el framework, cms, y otras tecnologías utilizadas en la creación del sistema informático. Hacer periódicamente un pentesting ya sea a nivel interno o por medio de un externo, para revisar las nuevas brechas de seguridad que podrían estar presentes en el sistema.

Seguridad Pasiva

- Realizar periódicamente copias de seguridad en diferentes dispositivos físicos y/o en particiones de discos.
- Verificar que los antivirus estén actualizados
- Capacitar al personal para que se habitúe a escanear y limpiar los equipos y evitar los ataques de Malware.
- Instruir también al personal para que en caso de responder de manera rápida desconectando al equipo de la red hasta que pueda solucionarse.
- Analizar la máquina periódicamente en busca de malware. Puede que los tengas dentro pero que no estén activos

Seguridad activa:

- Emplear contraseñas seguras: Las cuales deben contar mínimo con ocho caracteres,mezclando letras mayúsculas con letras minúsculas,números y otros caracteres.No se deben emplear como contraseñas la fecha de nacimiento o nombre de la mascota.

- Encriptar los datos importantes: O lo que es lo mismo, cifrar los datos para que sólo puedan ser leídos si se conoce la clave de cifrado. La encriptación se hace con programas especiales.

- Usar software de seguridad: como antivirus, antiespías, cortafuegos.

- Tener un antivirus actualizado. No ignores sus peticiones de actualización.

- Realizar copias de seguridad. Deben ser constantes y de todo lo que consideremos que tiene un cierto valor.

Seguridad Lógica:

- Opciones de login a sistemas de información y bases de datos:
- La autenticación de tokens de seguridad proporciona a los usuarios un número que cambia en una línea de tiempo determinada, generalmente cada minuto. Como parte de un proceso de inicio de sesión
- La autenticación de dos factores (2FA). Además de un nombre de usuario y contraseña, los usuarios pueden proporcionar respuestas a preguntas de seguridad o confirmar un PIN enviado a un dispositivo o aplicación por separado.
- Configuraciones biometricas - por voz - retina
- La segmentación de usuarios permite a los administradores del sistema controlar las áreas de la red de la organización a las que pueden acceder los usuarios individuales. Esto garantiza que, en caso de que la cuenta de un usuario se vea comprometida de alguna manera, el atacante no podrá causar estragos en toda la red de la organización.

- Agregar control de acceso, no permitir que todos lo empleados tengan acceso a toda la información.
- Cifrado de datos: Cifrar los datos del equipo para la protección de los mismos.
- Antivirus: Instalar antivirus para la protección de los datos.
- Firewalls: instalar para prevenir nuestra red privada.

Auditoría: Por último es importante la realización de una auditoría haciendo énfasis en los siguientes aspectos.

- Entrevistas al personal para saber si son conscientes de las prácticas de seguridad y si están siendo aplicadas.
- Análisis de código de software.
- Verificación del sistema de encriptación de datos de la página web.