Certified Tech Developer
The Ultimate Degree

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:** La empresa a pesar de que es pequeña se nota que el mecanismo de seguridad es deficiente debido a que la información sensible está muy

expuesta, se deberían implementar mecanismos de control más eficientes, un mecanismo de copias de respaldo, control de acceso a los usuarios mediante perfiles, implementar algún mecanismo preventivo de posibles ataques DoS, implementar mecanismo para detección de errores y de seguridad, y una vez detectados iniciar un plan de corrección.

2. **Para cada escenario planteado, crear un plan de seguridad**

Escenario 1: Información expuesta.
Implementar perfiles de acceso para cada usuario, con el objetivo de limitar el acceso a la información que actualmente se encuentra publica para todos.

Utilizar mecanismos de cifrado de la información en reposo y en tránsito.

Escenario 2: Copias de Respaldo.

Es necesario crear copias de seguridad, backup de los datos completos e incrementales con el tiempo, con el objetivo de tener un respaldo en caso de producirse un ataque o la pérdida de los mismos.

Adicional, se recomienda un mecanismo de respaldo de información en el caso de recuperación de datos ante desastres naturales.

Escenario 3: Ataques DoS:
Implementar reglas de Firewall que permitan el acceso seguro a los

servidores mediante el bloqueo de puertos descubiertos, implementar black list de ips, usar proxys inversos para evitar el acceso directo al servidor.

Escenario 4: implementar mecanismo para detección de errores y seguridad. La detección de errores se logra mediante la implementación de monitoreo en los servidores, donde se detecta la cantidad de tráfico entrante y tráfico saliente y donde se vigila que las respuestas entregadas sean exitosas.

La detección de seguridad se logra mediante la implementación de antivirus, firewall.

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**.

Paso 1(Seguridad física): Realizar backup programados sobre áreas que manejan información sensible o de alta demanda.

Paso 2 (Seguridad lógica): Realizar control de acceso creando perfiles de usuarios mediante el uso de contraseñas que tengan que ser actualizadas periódicamente.

Paso 3: (Seguridad lógica): Implementar seguridad mediante el cifrado de información utilizando certificados digitales y protocolos seguros como el

https. Implementar un sistema de detección y prevención de intrusiones que monitoriza las conexiones y alerta de intentos de acceso no autorizados.

Paso 4: La detección de seguridad se logra mediante la implementación de antivirus, firewall.

Paso 5: Implementar estándares de seguridad como ISO/IEC 27001

Paso 6: Fijar políticas de Seguridad y manejo de información, acompañado de capacitación al personal.

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.