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.
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.

Escenario para grupos 2, 4, 6, 8, 10 , 12

- Empresa ya consolidada que se dedica a brindar servicios informáticos. La mayoría de sus empleados trabajan de forma remota, pero hay algunos que lo hacen on site. Necesitan una intranet más segura. La información confidencial de la empresa tiene buena seguridad lógica, pero muy poca física, aunque igualmente desean tener asesoramiento en seguridad lógica. No tienen problemas en invertir dinero, pero sus empleados se resisten al cambio de nuevas restricciones. Poseen una página web donde brindan sus servicios y los clientes pueden contactarse a través de la misma.

Mesa 6: PLAN DE SEGURIDAD

1- Seguridad lógica: Solicitud de cambio de contraseña cada n cantidad de tiempo, Validacion estado de antivirus y actualización del mismo,control sobre envío de archivos e información confidencial a externos, Firewalls

2- Seguridad física: Implementación de UPS en las casas de los empleados y la oficina física ya que ante una eventual pérdida de energía, es importante poder tener unos minutos para poder guardar el trabajo que se estaba realizando. Además, en la oficina también hay que colocar extintores, ya que cualquier dispositivo funcionando de una forma defectuosa podría generar una chispa y poner en peligro no solo la información, sino también a las personas. Para terminar, es necesario realizar backups tanto de manera local como remota, de esta forma, si algún sistema de almacenamiento falla, siempre se puede acceder al backup para recuperar la mayor cantidad de datos posibles

3- Seguridad pasiva: Realizar copias de seguridad en al menos 1 dispositivo ubicado fuera de la oficina. Escanear los equipos 2 veces a la semana en busca de malware. En caso de un ataque, desconectar inmediatamente el equipo de la red.

4- Seguridad activa: Uso y empleo adecuado de contraseñas. Encriptar los datos importantes, mediante un algoritmo de cifrado con una clave. Uso obligatorio de antivirus actualizado.

5- Controles de medida de seguridad: Implementar medidas de seguridad proactivas como Monitorear la actividad del usuario y el acceso a los recursos y reactivas Apoyo a la respuesta a incidentes.

6- Vulnerabilidades que podrían explotar los atacantes: Contraseñas poco robustas que puedan generar inseguridad y acceso de terceros a información delicada