Práctica de auditoría y búsqueda de vulnerabilidades- Equipo 4

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.

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.

1- SEGURIDAD LÓGICA:
Chequear control de acceso, cifrado de datos, actualización de antivirus y firewalls para asegurar que se aplique de manera correcta la seguridad lógica a través de su intranet.

2-SEGURIDAD FÍSICA:
Recomendamos la instalación de pararrayos y alarmas contra intrusos
Además recomendamos la revisión periódica de extintores de incendio y detectores de humo para cumplir la reglamentación.

Instalación de UPS en servidores importantes, para evitar pérdidas de información ante cortes de suministro.

Recomendamos un sistema de respaldo de datos periodico y la utilización de sistemas redundantes para información más valiosa para la empresa.

3-SEGURIDAD PASIVA
Recomendamos tener un procedimiento actualizado de realización de copias de seguridad, actualización de antivirus
Adicionalmente un plan de acción y simulacro de emergencia ante ataque de malware.

4-SEGURIDAD ACTIVA
Comenzar a capacitar de inmediato a los colaboradores acerca de las buenas prácticas en seguridad para evitar ataques.
Instalación de sotfware de seguridad informática

5-CONTROLES DE MEDIDAS DE SEGURIDAD Y DE VULNERABILIDADES.
Realizar simulacros de ataques de malware (por ejemplo a través de phishing) para generar conciencia de la gravedad e importancia de la ciberseguridad.

Auditoría del grupo 5 al grupo 4

Como equipo de trabajo auditor, nuestro objetivo es analizar de manera exhaustiva y profunda las distintas características y áreas de esta empresa. Por lo que, en este informe, nos encargaremos de analizar y determinar que esta red de seguridad sea eficiente.

El primer paso de la auditoría será formar un equipo de trabajo que conste de dos personas externas y dos personas internas con el objetivo de conocer el estado de la seguridad informática actual, según el equipo de IT de la compañía.

Luego, deberíamos realizar testeos generales con preguntas tipo examen para entender el nivel de conocimiento en seguridad informática que tienen los empleados en la actualidad. Una vez los conozcamos, seguirán los simulacros de phishing como en el plan original, pero especializados en los empleados más vulnerables y en los temas que mayor riesgo impliquen.

Los empleados internos de IT deberían detallar todos los procesos informáticos de manejo de información, redes, y accesos que tengan los empleados de la compañía, a fin de poder hacer una investigación detallada y encontrar potenciales riesgos.

Los softwares anti-malware y firewalls tienen que estar actualizados en todo momento, por lo que se harán revisiones periódicas para garantizarlo y se obligarán a los empleados a hacerlo y forzar el reboot del sistema, con algunas advertencias previas para que puedan guardar su trabajo.

Revisar el vencimiento de extintores y mantener el edificio en condiciones en todo momento. De ser posible, tercerizar el servicio de higiene y seguridad.