Práctica Nº1 / Tema 1

Fecha de realización: 10 - 10 - 22

Indice

1. Trabajas en una auditoría de seguridad informática. Llega un nuevo cliente que desea conocer la situación de su empresa y si es aceptable o podría mejorar. Durante la entrevista tomas las siguientes notas:

2. Al día siguiente continúa la entrevista. Tus nuevas notas son:

3. Tus notas del tercer y último día son las siguientes:

1. Trabajas en una auditoría de seguridad informática. Llega un nuevo cliente que desea conocer la situación de su empresa y si es aceptable o podría mejorar. Durante la entrevista tomas las siguientes notas:

1.1 | El edificio tiene un servicio de vigilancia a través de una empresa externa. Por reducción del presupuesto, ahora solo hay un vigilante que también atiende el edificio del otro lado de la calle.

1.2 | El CPD tiene otro vigilante, de otra compañía, que también atiende el teléfono de la centralita a partir de las 3, cuando termina el turno del recepcionista.

1.3 | Para entrar al CPD, cada informático tiene una tarjeta particular, si bien hay una en el cajón de la mesa del vigilante para el personal de limpieza o por si ocurre una emergencia.

1.4 | Una vez a la semana se hace la copia de seguridad. Como solo disponen de un dispositivo de cinta, los cuatro servidores se reparten cada semana del mes.

1.5 | Dado que solo hay un vigilante para el CPD, las cintas se dejan dentro de la sala, cada una encima de su servidor (cada servidor tiene una cinta en exclusiva).

1.6 | El edificio pertenece al patrimonio histórico y no admite reformas en la fachada. Por tanto, no ha sido posible instalar equipos de aire acondicionado en el CPD. Para combatir el calor que desprenden los ordenadores, las ventanas están siempre abiertas.

1.7 | Cada servidor tiene un disco duro de alta gama, que no ha fallado nunca.

1.8 | Los servidores tienen doble fuente de alimentación, por si se estropea alguna.

1.9 | El presidente y el contable tienen cada uno un portátil de la empresa. El disco duro de estas máquinas no está cifrado porque no se arriesgan al desastre que supondría olvidar la contraseña.

1.10 | Los ordenadores tienen dos usuarios: uno para las tareas normales y otro cuando necesitan realizar alguna instalación o modificar un parámetro del sistema operativo. Los empleados saben cuándo deben usar cada uno.

- **Terminái hoy la entrevista porque ha sido una reunión muy larga. Todavía no has redactado el informe final, pero ¿encuentras algo que mejorar? ¿Qué alternativa le puedes proponer?**

La primera vulnerabilidad que podemos encontrar es en el punto 4, compraría más dispositivos de cinta para poder hacer la copia de los 4 servidores a la misma vez, el tiempo con el que se hacen las copias de seguridad yo lo reduciría a diariamente por la noche. También, el punto 5 lo veo muy mala idea, lo que haría las copias de seguridad en la nube, y las cintas las llevaría a un edificio o almacén distinto para conservar su integridad y disponibilidad, ya que si hubiera un incendio o algo parecido, las copias de seguridad estarían en lugares distintos. El punto 6, al tener las ventanas abiertas, podrían entrar fácilmente por hay, por eso lo más lógico y prudente sería reforzar la seguridad poniendo unos barrotes en estas ventanas. En el punto 1, es una mala idea. Lo mejor sería que ese único vigilante, solo vigilara nuestro propio edificio, ya que si se va al otro, tendríamos una vulnerabilidad bastante grande. Conforme al punto 3, es necesario no utilizar tarjetas generales, y tener bastante controladas las entradas y salidas por si algún día pasa algo, todo sea fácilmente identificable. Si nos fijamos en el punto 7, lo mejor sería tener dos discos duros, ya que aunque no le haya fallado hasta el día de hoy, lo mejor sería tener otro por si algo ocurre. También si vemos el punto 9, lo más lógico es que aunque de pereza, esos ordenadores son los más importantes, y por lo tanto, si salen de la empresa, tenemos que tenerlos cifrados y seguros, y el jefe de administración, que tuviera esas contraseñas bajo llave. Por último, viendo el último punto diría que aunque el empleado sepa qué hacer con los ordenadores, fuera el administrador el que gestionara todo lo que tuviera que ver con el sistema operativo, y antes de hacer cualquier cambio en los parámetros, hacer copia de seguridad de esta configuración.

2. Al día siguiente continúa la entrevista. Tus nuevas notas son:

2.1 | Hay una red wifi en la oficina que permite entrar en la red de ordenadores y salir a Internet. No tiene contraseña para que los clientes puedan utilizarla con total comodidad.

2.2 | La mayoría de los ordenadores utilizan Windows XP, pero algunos empleados necesitan Windows 7. Como la empresa no puede afrontar la compra de nuevas licencias, están utilizando software pirata.

2.3 | En cuanto al antivirus, cada empleado pone el que más le gusta y se los pasan entre ellos mediante discos USB.

2.4 | Los ordenadores que hacen de servidores tienen activadas las actualizaciones automáticas de todas las aplicaciones y el sistema operativo, pero en los ordenadores de empleados no se hace porque han visto que se satura la conexión a Internet.

2.5 | La mayoría de los equipos de red son switch y routers, pero algunos despachos todavía tienen hubs porque son fiables y el ancho de banda es suficiente.

2.6 | Para entrar a la red desde Internet utilizan Hamachi, un servicio gratuito y muy sencillo de instalar.

2.7 | El servidor web está instalado sobre una máquina con sistema operativo Linux Ubuntu Server 9.0

- **Termina la entrevista del segundo día porque tiene otro compromiso. De nuevo, ¿encuentras algo que mejorar? ¿Qué le puedes proponer?**

En el primer punto, vemos que es muy mala opción ya que lo mejor sería crear dos redes WIFI, la primera sería para los ordenadores que van a trabajar, este tendría una contraseña larga y difícil para que no se pueda adivinar ni usar fuerza bruta y activaría un protocolo como WPA2 y la otra red sería sin contraseña pero estaría limitada para que no pueda conectarse con el área de trabajo que previamente creamos en la otra red. También tenemos que tener en cuenta que utilizar software pirata, como vemos en el punto 2 es una mala opción. Al no ser oficial puede tener muchas vulnerabilidades y arriesgarnos de que contengan algún virus o archivo expiatorio. Y además nos arriesgamos a que si vienen a hacernos alguna inspección, nos pongan una multa por usar estas licencias de manera ilegal. Lo mejor es invertir en licencias legales, ya que a la larga nos saldrá más barato.

Una de las principales causas de infección en empresas es a causa de virus por USB, sabiendo este dato y mirando el punto 3, lo mejor sería instalar el mismo antivirus para todos, y añadir que al insertar un USB pida contraseña de administrador, si no, desactivar este puerto si no es esencial. Conforme el punto 4, descargar actualizaciones está bien, pero lo que yo haría sería descargar estas actualizaciones pero no instalarlas hasta que el administrador lo requiera necesario y si es posible hacerlo por la noche, para no cortar el tráfico ni el trabajo. Si vemos el punto 5, lo mejor sería usar switch ya que el hub puede tener más problemas de sniffs.

Si miramos el punto 6, esta empresa hace uso de Hamachi, la cual es una VPN disponible pública y gratuita, conectarse a una red de este servicio es muy parecido a conectarte a tu propia LAN; exceptuando el hecho de que todos los equipos existentes en la red de Hamachi a la que está conectado son desconocidos y pueden ser una verdadera amenaza para cualquiera en la red. Contando que esencialmente está proporcionando una entrada a su propia red sin algunas de las precauciones de seguridad más importantes, es casi seguro que esta empresa podría recibir algún tipo de ataque por esto

Por último, y no menos importante, recomendaría que lo actualizaran a una versión de Ubuntu más actualizada en este caso la 22.04, ya que según el punto 7, esta empresa usa una versión deprecated de este sistema operativo.

3. Tus notas del tercer y último día son las siguientes:

- **Los clientes rellenan una ficha con su nombre, dirección, teléfono, correo electrónico y la medicación que están tomando en este momento. ¿Tienes algo que aportar sobre la seguridad que necesitan estos datos?**

- **Después, una secretaria introduce la ficha en una hoja Excel de su ordenador.**

Finalmente, ¿tienes algo que aportar sobre la seguridad que necesitan estos datos?

Tendrá que solicitar a la agencia de protección de datos para poder crear un fichero y sea legal, por supuesto, tendrá que tener una seguridad alta. La secretaria deberá tener su ordenador cifrado, con una contraseña robusta y bien vigilada, con una copia de seguridad diaria.