TAREA COLABORATIVA BLOQUE III

1)    Cuéntanos algún problema que a título personal (o familiar o de conocidos) te haya sucedido. Describe que medidas de seguridad han fallado (física, lógica, activa o pasiva) y que alternativas existen para que no se repita.

En mi cuenta de Facebook, hace unos meses vi dos publicaciones que yo no había realizado y tenía nuevos amigos a los que ni yo había aceptado, ni había solicitado amistad. Me sentí bastante mal puesto que en mi Facebook tengo fotos, fechas e informaciones que no lo hago público, pero lo tengo almacenado (solo para mí). Que alguien pudiera acceder a eso no me gustó. Pienso que no he sido víctima de un hackeo sino que alguien malintencionado ha sido capaz de visualizar mi clave cuando yo he accedido, fallando así mi seguridad activa.

Me informé de los pasos a dar para recuperar mi cuenta, pero lo primero que hice fue cambiar mi contraseña haciéndola más segura y siendo más cauto con las miradas a la hora de entrar. El problema se solucionó así y quité las publicaciones que no correspondían y eliminé amigos. Tuve suerte de que la persona que entraba en mi perfil no cambiase el correo electrónico y/o la contraseña, puesto que hubiera sido más complicado. Sí que me acuerdo que había tomado la precaución de haber respondido a unas preguntas para que en caso de robo, poder solo yo recuperarla. También tengo activada la verificación de 2 pasos, que te obliga a confirmar cualquier cambio a través del móvil.

En fin, esta situación me ha hecho estar más alerta y seguro.

2)    Localiza alguna noticia en la que el fallo lo haya cometido o sufrido una empresa. Indícanos que ha pasado, que daños ha habido, cuáles han sido las consecuencias para la empresa o los trabajadores, y que medidas de seguridad crees que han fallado.

A veces salen noticias sobre el robo de exámenes en los institutos y universidades, no de forma física. La que he seleccionado se refiere al robo de exámenes entrando en los correos corporativos de los profesores y hasta el uso de alguna tarjeta de los profesores afectados para compras por parte del grupo organizado.

El robo masivo de exámenes podía tener el fin de aprobar con buena nota y ser vendidos al alumnado interesado a través de las redes sociales y grupos de WhatsApp.

Lograban el hackeo de las cuentas instalando un software ilegal que se encargaba de registrar las pulsacionesque se realizaban en el teclado de los equipos de 1º y 2º de Bachillerato, 4º de ESO y aulas informáticas del instituto. De esta forma, memorizaban un fichero de texto con todo el contenido y consiguieron las contraseñas de las cuentas de los correos electrónicoscorporativos de, al menos, 27 profesores del centro. El fallo ha sido de seguridad activa.

Los afectados han sido el instituto y la mayoría de su profesorado, el alumnado que realmente estudia que se ha visto con similares oportunidades que otros que han conseguido o comprado los exámenes.

El instituto podría aumentar su seguridad poniendo contraseñas en los equipos  de uso exclusivo del profesorado y “obligando” a los profesores a un cambio rutinario de las claves de acceso a sus correos corporativos. Aunque una medida ya adoptada le enviaba información de los equipos en los que se abría su correo.

El enlace de la noticia es: http://www.elmundo.es/sociedad/2017/06/22/594b9f62468aebe52f8b468b.html

3)    Detalla al menos 5 medidas de seguridad distintas que has implementado (o que deberías hacer si no lo has hecho ya)  para los equipos tuyos o de tu familia, recuerda que la seguridad informática no es solo el ordenador. Tablets, wifi, router o móvil también forman parte de la "familia". Especifica problema, tipo de seguridad involucrada y solución preventiva.

Estos son algunas de las medidas que ya tomamos y algunas la implementaremos próximamente:

1. Contraseñas débiles. Seguridad activa. Contraseñas combinando  números, letras, signos,… y que nunca sean fechas o nombre intuitivos.

2. Predisposición al phishing. Seguridad lógica. No contestar correos electrónicos en donde te solicitan “información de tu cuenta” que pueden suplantar tu identidad.

3. Falta de respaldo de información ante un virus oeliminación accidental de un archivo,... Seguridad pasiva. El problema es que no estamos a hacer copias de seguridad.

4. Uso de software pirata. Pueden ser utilizados para sembrar troyanos y virus en los equipos y dado que el software carece de respaldo puesto que es pirata, el usuario es privado de soporte técnico quedando a expensas del ataque sin ayuda. Seguridad lógica. Usar software original.

5. Mal uso de dispositivos de almacenamiento portátil.El uso de dispositivos de almacenamiento portátil debe ser controlado, para usuarios selectos y con dispositivos predeterminados. Seguridad activa. Contraseñas, certificado digital, huella.

6. Uso de conexiones Wireless.A veces realizamos conexiones a redes gratuitas en cafés.. Aunque su acceso es rápido, fácil y gratuito, estas pueden no ser seguras y acceder a ellas puede abrir las puertas a amenazas con mayor facilidad. Seguridad lógica. No conectarse a estas redes y menos para realizar transacciones relevantes por internet como transferencias y acceso a cuentas bancarias o compra de servicios en línea.

7. Buena ubicación de los equipos. Seguridad física. Tomar precauciones de que no haya facilidad de que se mojen los equipos por cercanía a grifos o tuberías, ni muy cercanos a fuentes de calor. Sería bueno utilizar SAI.