CONSEJOS DE SEGURIDAD INFORMÁTICA PARA EMPRESAS

Cuando se habla de seguridad, aplicada a cualquier aspecto, se deben tener las mismas precauciones. Es decir, seguro que a nadie se le dejarían las llaves de casa, o la cartilla del banco. Siempre se desconfía, y esa misma actitud es la que se debe adoptar cuando se trata con elementos informáticos.

Medidas de seguridad básicas

Cumpliendo los siguientes 7 consejos reducirás las probabilidades de que tu empresa se vea afectada por un ataque informático:

1. No dar nunca datos personales a menos que se esté seguro de quién los solicita.
2. Disponer de más de una cuenta de correo, estando muy diferenciadas las de trabajo con la personal.
3. Rechazar los correos *spam* y no abrir nunca los ficheros desconocidos.
4. No dar con facilidad el correo personal.
5. Mantener en secreto las contraseñas y nunca dejarlas escritas a la vista.
6. Las contraseñas se deben cambiar frecuentemente y alternar mayúsculas, minúsculas y números.
7. Nunca confiar en ofertas exageradas o regalos desorbitados en Internet, pues pueden tratarse de webs falsas, cuya única misión es copiar los datos personales y financieros para posibles estafas.

Reforzar las medidas de seguridad

Cuando hablamos de seguridad informática no solo se trata de mantener la información segura, sino también de cómo se van a mantener esos datos y es importante conocer los distintos métodos para tratarlos.

Cifrar las bases de datos

Uno de esos procedimientos es cifrar las bases de datos que contengan información de clientes y proveedores. En la actualidad existen muchos formatos de cifrado y básicamente se trata de aplicar un algoritmo asociado con una o varias contraseñas para poder ser descifrado, pues todo es poco a cambio de mantener los datos protegidos.

Protocolo SSL

Para el intercambio de información con la página web es importante usar un protocolo encriptado del tipo SSL, que no garantiza un cifrado de extremo a extremo, es decir, desde el servidor hasta el equipo cliente y viceversa.

Contraseñas seguras

Otro de método es la implementación de contraseñas seguras, que parece lo más obvio. Pero actualmente se siguen utilizando contraseñas muy débiles como fechas de nacimiento, nombres o apodos. Se deben hacer uso de contraseñas complejas, utilizando mayúsculas, minúsculas y números o caracteres especiales como ‘*EstaEsMicontr4seña*‘.

Software actualizado
Es importante utilizar siempre la última versión del *software* instalado, el sistema operativo más reciente, antivirus y *software* empresarial. No hay que explicar que las últimas versiones de *software* incorporan parches de seguridad y bloquear vulnerabilidades que pueden ser aprovechados por ciberdelincuentes.

Capcha
Utilizar utilidades de tipo Capcha, que incorpora imágenes para detectar que quienes están accediendo a las páginas web no son robots. De esta manera se filtran los usuarios que acceden.

Cumplimiento de la legalidad
Otro aspecto importante es mantenerse al día en cuanto a la legislación para estar informado sobre los requerimientos legales, y así saber a dónde acogerse cuando se sufra un ataque.

Correos electrónicos
Por último, es importante gestionar los correos electrónicos de una forma eficiente, aplicando reglas de *spam* y bloqueos de cuentas extrañas, además de no abrir archivos adjuntos que sean sospechosos.

diarios ataques informáticos.

Teniendo en cuenta lo mencionado anteriormente, las empresas se han dado cuenta de que dada la gran cantidad de dinero solicitada por los ciberdelincuentes y lo mucho que se juegan, ya sea en prestigio o reputación, la seguridad informática es fundamental.

Es muy importante para las empresas tener una imagen solida frente a los ataques, ya que sus clientes van a confiar en ellos y tener clientes se representa en dinero para ellas. Por eso, las compañías deben invertir dinero en seguridad informática, que según los costes no dista mucho de las cifras que solicitan los ciberdelincuentes.

Es tal el incremento en la actualidad de los ciberataques, que muchas otras empresas han tenido que adaptarse a los tiempos modernos, como son las empresas de seguros. Estas empresas han adaptado sus productos para dar confianza incorporando seguros de responsabilidad en caso de pérdida o robo de información.

HERRAMIENTAS GRATUITAS

Hackend

Existen muchas herramientas en el mercado para verificar la seguridad de las pymes, como es el caso del juego creado por el Instituto Nacional de Ciberseguridad (INCIBE) llamado *Hackend, (*se acabó el juego) que es muy adecuado para empresas que están en proceso de desarrollo para la protección de su web.

Scan My Server

La herramienta mas utilizada y solvente utilizada por las pymes es Scan My Server, puesto que es una herramienta gratuita. Entre algunas acciones que llevan a cabo se encuentran la comprobación de *malware* existente en la página web de los servidores.

Observatory

Otra herramienta similar es Observatory de Mozilla, que es un *software* muy potente, que además también es gratuito.