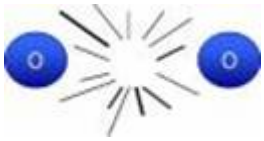
Diez preguntas que ponen a prueba la seguridad informática de una empresa

- Noticias TIC -

Publicado: 11 de septiembre de 2017



Aula TIC PYMEs de la USC

El reciente ataque informático WannaCry ha demostrado que la seguridad juega un papel muy importante en las empresas. En este ámbito, hay que adoptar las medidas defensivas más apropiadas y, para ello, nada mejor que empezar comprobando si una empresa es segura. Para ello, se plantean las siguientes diez preguntas.

¿Utilizan los empleados una contraseña fuerte?

Más de la mitad de los datos que se pierden en la empresa tienen su origen en el uso de contraseñas débiles y sin embargo, menos del 25% de las empresas aseguran que su organización cuenta con una buena política de gestión de identidades.

¿Se solicita a los empleados que cambien de contraseña con regularidad?

Una contraseña, aunque sea segura, pierde su efectividad con el transcurso del tiempo. Una buena política de empresa para reforzar la seguridad es cambiarlas con regularidad.

¿Se utiliza un sistema de autenticación de doble factor?

Esto significa que no solo basta con introducir nombre y contraseña, sino un código adicional que se genera de forma aleatoria y que el usuario percibe por otro canal, como puede ser un SMS en el teléfono.

¿Cómo se integran los smartphones de tus empleados en la red de tu empresa?

Ofrecer a los empleados teléfonos corporativos es una buena forma de evitar que un teléfono móvil personal se integre en la red de una empresa, algo que incrementa las opciones de ser víctima de un ataque malware.

¿Se realiza periódicamente una copia de seguridad de los datos?

Un ataque de ransomware podría secuestrar la totalidad de los datos de una empresa haciéndolos inaccesibles. De ahí la extrema importancia de mantener una política activa de backup.

¿Se cuenta con las soluciones de seguridad adecuadas?

Cada dispositivo que se conecta a la red de tu empresa debería contar con una solución de seguridad apropiada y actualizada. Servidores, ordenadores, teléfonos, tablets e incluso impresoras pueden convertirse en un vector de ataque.

¿Limitas el número de empleados que tienen privilegios de administrador en la infraestructura IT de tu empresa?

Muchos de los problemas de seguridad informática que sufren las empresas se podrían evitar si se limitase al máximo, el número de usuarios que pueden acceder a los privilegios que tiene un administrador de sistemas (como permiso para instalar nuevo software).

¿Saben los empleados reconocer un e-mail sospechoso?

Los ataques de phishing son cada vez más sofisticados. No sólo son capaces de hacerse pasar por una entidad bancaria, sino también por compañías o incluso hasta por organismos oficiales como la propia Hacienda. Es muy importante que se reconozcan este tipo de envíos, identificando el remitente y la dirección web para mantener a raya a los cibercriminales.

¿Se encripta de alguna forma las bases de datos y la información sobre los clientes?

Si un cibercriminal pone en el punto de mira en una organización, la probabilidad de que finalmente consiga introducirse en la infraestructura IT de la misma es bastante alta.

No obstante, si además de tener una buena política de copias de seguridad, se encripta adecuadamente la información más sensible de la empresa, se conseguirá mantener a salvo.

¿Están los sitios web de la empresa protegidos?

El origen de muchos ciberataques puede estar en algo tan "sencillo" como una infección a un site WordPress que no ha sido actualizado.

Si tenemos una web corporativa, conviene asegurarse que esté aislada del resto de nuestra estructura IT y por supuesto, actualizada con los últimos parches de seguridad que se hayan lanzado.

Fuente: Muy Pymes [http://www.muypymes.com/2017/09/05/preguntas-prueba-seguridad-informatica-empresa], 05 de septiembre de 2017