5 acciones PARA PREVENIR brechas DE SEGURIDAD en tu EMPRESA

por juan martos*

La seguridad informática ya no es cosa de los profesionales del sector tecnológico. De hecho, se trata de un problema global que nos afecta a todos: desde las grandes empresas hasta los usuarios particulares. Los ataques cibernéticos son cada vez más sofisticados. Las posibilidades de éxito son relativamente altas para los delincuentes y los beneficios potenciales son altamente lucrativos. Por otro lado, las mafias son conscientes de que las posibilidades de que los culpables sean descubiertos y puestos a disposición de la Justicia son escasas.

A pesar de todo, con sentido común y una buena dosis de autodisciplina es posible evitar caer en las redes de quienes quieren hacerse con nuestros datos y/o con nuestro dinero. Veamos cuáles son las 5 acciones esenciales para prevenir brechas de seguridad en tu empresa:

1. Realización regular de copias de seguridad

No por ser el más antiguo de los clásicos de la seguridad ha perdido efectividad. En la actualidad, existen innumerables sistemas, ya sea locales o basados en la nube, que realizan copia de nuestros datos. Disponer de un sistema de copia de seguridad efectivo nos librará de los efectos de algunos de los ciberataques más frecuentes como el secuestro de datos o "ransomware".

2. Mantener el sistema operativo actualizado

Mantener los equipos informáticos y los dispositivos de telefonía móvil actualizados es una parte fundamental del proceso preventivo. Las actualizaciones no solamente incorporan nuevas funcionalidades o mejoras en el manejo de los dispositivos. Una buena parte de ellas incluye, además, nuevos parches que solucionan agujeros de seguridad que se van descubriendo con el tiempo y que ponen en riesgo la seguridad de la información.

3. Cambiar regularmente las contraseñas

En un mundo ideal, deberíamos tener contraseñas diferentes para cada una de nuestras cuentas. Si esto no es posible, al menos deberíamos utilizar contraseñas con un mínimo de longitud y de dificultad. Nada de datos personales como nuestra fecha de nacimiento o el nombre de nuestros hijos. Lo primero que hará un hacker es buscar información sobre nosotros en Internet: LinkedIn, redes sociales, etc. De modo que si utilizamos como contraseña un dato relacionado con nosotros

mismos se lo estaremos poniendo en bandeja. Actualmente, existen diversos sistemas tanto a nivel de sistema operativo como de los propios navegadores de Internet, que generan contraseñas seguras y las guardan cifradas para que no tengamos que recordarlas. Sin embargo, mucho ojo. Porque dichos sistemas suelen depender de una única contraseña maestra que da acceso al resto. Por lo que conviene recordar lo que indicábamos al comienzo de este punto.

En este caso, no debemos olvidar activar los sistemas de verificación de doble factor. Estos evitarán que un tercero no autorizado pueda acceder a nuestros datos incluso aunque conozca la contraseña.

4. Cifrado de la información

En ocasiones, el acceso a nuestros datos puede producirse por contacto físico con el equipo que los contiene. Por ejemplo, nos pueden robar el portátil mientras tomamos café y lo descuidamos un segundo. En estos casos, es esencial que el disco duro del equipo esté protegido mediante un sistema de cifrado que impedirá que los datos puedan ser leídos si no se dispone de la clave oportuna. Ni siquiera en el caso de que el disco sea desmontado físicamente y conectado en otro ordenador.

5. Concienciación sobre ciberseguridad

El eslabón más débil de la cadena de la seguridad informática es el usuario. Un hacker, por muchos conocimientos técnicos que tenga, necesitará siempre la colaboración de la víctima que, sin saberlo, será quien le facilite el acceso a los datos que necesita el hacker para acceder a su botín. Por tanto, conviene realizar charlas y cursos de concienciación sobre ciberseguridad para que todos los miembros de la empresa estén atentos a cualquier intento de ataque por parte de un tercero.

*Socio director de Forensic Tecnológico de Grupo Paradell.