Ataques ransomware, ninguna empresa ni profesional está a salvo del ciber riesgo (ARTICULOS)

30, mayo

Todas las empresas están a merced de los **ciberataques de ransomware**. El pasado 12 de mayo de 2017 empresas de todo el mundo sufrieron un ciberataque masivo, incluyendo una de las gigantes como Telefonica, que pidió a sus empleados que apagaran sus ordenadores. El virus utilizado no era demasiado complejo ni sofisticado, pero encontró la manera de expandirse, propagándose de un ordenador a otro a través de la red común de la empresa.

El cibercrimen está cada vez más extendido, actúa de una forma sencilla, a través de correos electrónicos que reciben los usuarios diariamente, o a través de anuncios en páginas webs conocidas. Una vez ha entrado el virus en el ordenador, una pantalla informa de que los archivos están encriptados y que si quiere recuperarlos es necesario pagar un rescate. En definitiva, lo que hacen es **“secuestrar” datos y archivos**, aunque los ransomware más evolucionados también amenazan con publicar información personal, como fotos, correos electrónicos…

En todos los foros se destaca la bonanza del internet de las cosas, los procesos disruptivos y de cómo la tecnología nos facilitará la vida pero, ¿estamos seguros de ello realmente? Si nos diesen a escoger entre un robo forzando la cerradura de casa o el robo de mis archivos profesionales ¿cuál de los dos causaría menos daño? De igual forma que fuimos mejorando los sistemas de protección físicos ahora también hay que protegerse de los delitos cibernéticos. Aquí desgranamos varias soluciones:

- La primera y más elemental es evitar este ataque , o por lo menos minimizar sus daños, por tanto no abrir ningún correo que no estemos seguros de que debamos recibir respuesta, no abrir links en correos electrónicos, no clicar en anuncios en páginas webs. Muchas veces estos anuncios nos llevan a páginas no deseadas y es mejor no arriesgarse.

-La segunda es hacer copias de seguridad continuas, aunque sea muy antiguo, es de lo más

efectivo. En archivo externo o en la nube, lo mejor en ambos lugares (recordamos que además de la puerta de entrada hay que reforzar las ventanas).

Estos consejos son relativamente sencillos de aplicar para un particular, pero en el caso de una empresa resulta más complejo, al entrar los empleados continuamente en nuevas páginas webs sin confirmar previamente su seguridad. Además, no siempre es fácil detectar que se trata de un correo no deseado. ¿Quién no oyó hablar o abrió el famoso email de Correos en el que informaban de un paquete que no había podido ser entregado? Pues bien, ese virus resultó tan rentable en España que los hackers lo lanzaron dos veces. Numerosas empresas se vieron afectadas cuantitativa y cualitativamente por este virus. Entonces, ¿cómo pueden hacer frente las empresas a este gran riesgo, tan difícil de controlar? Siendo estrictos con el cumplimiento normativo mejoramos la seguridad.

- La tercera, dedicar tiempo a la formación de los empleados ante los nuevos peligros, designar un coordinador que resuelva las dudas de los mismos de forma presencial o en línea, en caso de duda.

Ya se conocen numerosos casos de profesionales abogados y administradores de fincas, pequeñas y medianas empresas que se ven obligadas a cerrar al perder sus datos y no poder hacer frente al pago de un rescate. Para protegerse frente a los efectos de un ataque de este tipo, que incluso con las prevenciones adoptadas puede hacer daños, se hace imprescindible **la cuarta solución**, el seguro de ciberriesgo que garantiza las pérdidas o sanciones de la Agencia de Protección de datos por aplicación de la LOPD u otros organismos, que sufra la empresa como resultado de un ataque de malhechores cibernéticos, así como la responsabilidad civil (pérdida de información confidencial, datos de clientes, etc.) .

Fuentes: elaboración propia

Comentarios