DESCUBRA CÓMO ELABORAR UN PLAN DE CIBERSEGURIDAD

20 de octubre de 2017

Para evitar ataques informáticos, las pymes deben implantar protocolos de prevención adaptados, que los conozcan todo el equipo y mantener los sistemas electrónicos actualizados.

Por quinto año consecutivo, octubre vuelve a ser el periodo escogido por la Comisión Europea para celebrar el mes europeo de la ciberseguridad. Con esta iniciativa, el organismo comunitario quiere alertar a los diferentes sectores de la sociedad sobre el desafío que suponen los ataques informáticos.

Un riesgo al que se enfrentan día tras día las empresas españolas, como pudieron comprobar el pasado mayo los responsables de Telefónica. Junto a otras grandes compañías, el gigante de las telecomunicaciones tuvo que interrumpir su actividad cuando un virus encriptó sus archivos de información y emitió un mensaje exigiendo el pago de un rescate. De este modo, este suceso puso en el foco un problema que afecta tanto a multinacionales como a pymes. Así, aunque un pequeño negocio no disponga de un departamento específico para hacer frente a los piratas informáticos, sí puede seguir una serie de recomendaciones para disminuir sus opciones de ser atacado:

Método de acción. El método de actuación favorito de los hackers es mandar un correo electrónico infectado. Normalmente, el virus se presenta bajo la apariencia de un email inofensivo que en el asunto hace referencia a una factura impagada o a una reunión con un cliente. Las prisas llevan a los trabajadores de la pyme a hacer clic rápidamente y entonces se desencadena el ataque. "En algunos casos los virus son tan potentes, o la empresa tiene tantas brechas, que llegan a colarse en los sistemas de seguridad de la nube, con lo que cifran la información del negocio que está almacenada online", señala Noemí Brito, directora de derecho digital de Legislel. Estos ciberdelincuentes, que actúan a través de programas autónomos que investigan direcciones de IP susceptibles de ser atacadas, se preocupan de no defraudar a sus víctimas. Así, exigirán un rescate para recuperar la información que puede alcanzar los 20.000 euros.

Detectar el riesgo. El trabajador es el que abre el correo infectado, por lo que es indispensable que la plantilla reciba formación para que sepan reconocerlos y evitarlos. Así los emails que aparezcan con un remitente extraño, escritos con faltas de ortografía o que lleguen sin firma deben despertar las alertas del equipo. En este sentido, la clave está en incorporar cláusulas de confidencialidad en los contratos de todo aquel que tenga acceso a material sensible en la empresa. Con esto, se consigue que el empleado reflexione antes de actuar.

Medidas técnicas. Además de los empleados, los dispositivos donde se almacena la información deben estar preparados para dar una respuesta eficaz frente a la actuación de los hackers. En este sentido, es importante que el software, las aplicaciones y antivirus estén actualizados, puesto que sus últimas versiones incorporan las herramientas más novedosas para luchar contra los nuevos métodos empleados por los piratas informáticos. Además es fundamental disponer de copias de seguridad protegidas con contraseñas, que se cambien cada seis meses, y guardadas en diferentes soportes. Por otro lado, depositar la información en discos duros que no estén conectados a la red de la empresa es fundamental, ya que los pueden llegar hasta los datos que se almacenan en la nube.

Uso de los dispositivos móviles

Móviles, tabletas y ordenadores portátiles tienen que contar con medidas adicionales de seguridad ya que hoy son una herramienta más de trabajo. No sólo basta con poner una contraseña fuerte, de más de cuatro dígitos, por si se olvidan en el taxi, sino también instalar barreras anti-piratas. Precisamente, si esto ocurre, es necesario tener apuntado el número de identificación IMEI, que permite a la operadora y a los cuerpos de seguridad su localización y bloqueo inmediato. En ocasiones, pequeños trucos, como desactivar las notificaciones cuando la pantalla está bloqueada o las sincronizaciones automáticas con otros servidores externos, pueden ser muy efectivos. Además, los dispositivos móviles que se utilicen para trabajar deberían tener instalado el menor número de aplicaciones posible.

Fuente: www.expansión.com