FECE informa

Por **Marta Pérez Dorao**, directora general de **FECE**

Ciberseguridad: asignatura pendiente

A pesar de que en España entre el 65%-70% de los ciberataques van dirigidos contra pymes, casi ninguna se considera objetivo para un ciberataque.

La creencia general es que la mayoría de los casos se producen contra las redes públicas, la administración, y no es cierto. Según datos de la consultora Arrabe Integra, el 60% de las que sufren un ataque severo desaparecen en los 6 meses siguientes. Y también aumenta el coste medio de estos ataques: en 2021 se calculaba en 105.655€, frente a los 54.388€ en 2020.

Y un problema adicional es que las pymes tardan mucho en identificar un ataque, en promedio 212 días, y 75 días más en contenerlo.

La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales, empezando por detectar y parar ciberataques. Como ya indicamos en un artículo anterior, el factor humano es crucial. Muchos ataques se dirigen a los empleados, y así a través de ellos acceden a los sistemas de la empresa. Por eso es importante impartir sesiones periódicas de formación, pues la delincuencia informática es cada vez más sofisticada. Aunque los ataques sencillos siguen siendo efectivos: el 91% de los ciberataques comienzan por un email de phishing. Es importante que todos sean conscientes de que no se deben bajar archivos o pinchar en links desconocidos, antes de abrir un email mirar bien la dirección del remitente… parece un correo normal de tu propia empresa o de otra muy conocida, pero hay que fijarse en la dirección o extensión del servidor, que normalmente es extraña.

¿Qué persiguen los ciberdelincuentes? Dinero. Ya sea chantajeando a la empresa a la que ha bloqueado los sistemas, o bien accediendo a sus cuentas o a información valiosa. Pero el mayor perjuicio puede estar en el bloqueo de los sistemas que impida a la empresa su tráfico habitual.

Ataques más frecuentes

Por eso es conveniente familiarizar a los empleados con los términos y ataques más frecuentes:

- El phishing al que nos hemos referido antes es la suplantación de identidad a través de correo electrónico con el objetivo de obtener información sensible. Normalmente incluye una llamada a la acción a través de un enlace malicioso.
- Malware o cualquier tipo de software o programa malicioso. Debe advertirse a todos que no se instalen programas en los dispositivos sin el visto bueno de la empresa.
- Virus: es un malware que infecta o altera el funcionamiento de programas y dispositivos con fines dañinos o ilícitos.
- Spyware o troyano: son programas de apariencia normal o que se ocultan en otros para robar información.
- Ransomware: software que infecta los equipos y desde el que se coacciona a los usuarios para que faciliten información o entreguen dinero.

Es fundamental, si se sospecha que puede haber habido brecha de seguridad, avisar cuanto antes a la Agencia de Protección de Datos, en cumplimiento de LOPD. De no hacerlo hay riesgo de importantes sanciones. Y sobre todo, ponerse inmediatamente en manos de un experto.

Medidas que pueden tomar las empresas y los empleados

¿Qué se puede hacer para prevenir estas situaciones? Además de evitar entrar en sitios no seguros, no facilitar datos sensibles a terceros y no descargar archivos dudosos, conviene tomar ciertas medidas, tanto la empresa como los empleados:

1 - La empresa debe actualizar tanto el software como el hardware. Los equipos obsoletos son más vulnerables. Además, es muy importante instalar un buen antivirus y mantenerlo actualizado. Instalarlo igualmente en los teléfonos, en los cuales también conviene borrar cookies e historial periódicamente.

2 - Además debe formar y concienciar periódicamente a los empleados, con reglas claras, y que estos sepan que:

- No deben usar contraseñas débiles y cambiarlas con frecuencia. Y, por supuesto, no compartirlas.
- Solo el personal autorizado debe poder instalar programas o descargar archivos.
- Recordar que no abran archivos sospechosos. No compartir equipos de trabajo con nadie, con la familia, etc. No usar nunca redes públicas o abiertas. Cuando no se esté trabajando, bloquearlo o cerrar la sesión. No reutilizar memorias USB encontradas. Desactivar Bluetooth o WiFi del móvil si no se están usando.
- Usar redes seguras. El 'router' de la WiFi debe estar provisto de cortafuegos y actualizado. Es necesario usar una VPN en caso de estar teletrabajando.

La velocidad es clave: los empleados deben estar formados en reglas básicas de detección de amenazas y cómo actuar en caso de que se produzca un ataque o haya una sospecha. Y fundamental: tener un plan de prevención y acción en caso de crisis, que minimice los tiempos de reacción. Y por supuesto, disponer de 'backups' o copias de los datos para restablecer el sistema ■