ENCUENTRO EXPANSIÓN-ECOFIN

La prevención de ciberriesgos, una asignatura pendiente para las pymes

SEGURIDAD/ Las grandes corporaciones tienen clara su estrategia frente a los riesgos cibernéticos, pero muchas pequeñas compañías aún no están preparadas frente a la amenaza de los 'hackers'.

EN LA DIANA

Más de la mitad de las pymes españolas sufrió algún **ciberataque** en 2018, según Incibe. Cada incidente cuesta una **media de 74.000 euros**.

Jesús de las Casas. Madrid

La amenaza de los riesgos cibernéticos es una realidad para las empresas españolas. A diario, los *hackers* firman ataques que, en el peor de los casos, llevan negocios enteros a la quiebra. Mientras que las grandes compañías invierten cada vez más en su protección, las pequeñas empresas no terminan de asumir lo que está en juego. Así, muchas organizaciones desconocen cuáles son las amenazas concretas que afrontan y cómo trabajar en su prevención.

"Hay desconocimiento en la sociedad sobre cómo enfrentarse a estos riesgos: las empresas son conscientes de que existen pero no saben cómo prevenirlos", comentó Rafael Sierra, director de *SegurosNews.com*. Trabajar en esa prevención es una necesidad imperante para las pymes y los autónomos, como se destacó durante el encuentro *¿Qué ofrece el seguro a las empresas para protegerse contra los ciberriesgos?*, organizado por EXPANSIÓN con el patrocinio de Foro Ecofin.

JL Pindado

De izq. a dcha., Rafael Sierra, director de SegurosNews.com; Karen Velandia, especialista en productos ciber de Chubb; Higinio Iglesias, consejero delegado de E2K; Carmen Segovia, directora de ciberriesgos de Aon España; Salvador Molina, presidente de Foro Ecofin; y Alan Abreu, responsable de riesgos cibernéticos de Hiscox.

Seguros

Por parte de las empresas, "la concienciación está creciendo pero todavía no se está pensando en el seguro o en la transferencia de riesgo, sino en medidas de seguridad perimetral", afirmó Karen Velandia, especialista en productos ciber de Chubb. Algunos sectores –como el financiero, hostelero o *retail*– tienen más exposición y son más sensibles a estos ataques, dado que presencian cada día casos reales de empresas que sufren incidentes.

Más allá de las grandes firmas, los expertos coincidieron en que muchas pymes han tomado conciencia en los últimos meses. No obstante, aún queda mucho camino por recorrer: "Las probabilidades de sufrir un ciberataque hoy son mucho mayores que un robo o un incendio, y eso es algo que las empresas deben tener en cuenta", remarcó Alan Abreu, responsable de riesgos cibernéticos de Hiscox.

En la misma línea, "antes la seguridad de una empresa se tenía que romper de forma física, pero ahora desde un ordenador puedes saltarte las barreras de seguridad y hacer mucho más daño", explicó Higinio Iglesias, CEO de E2K. En pymes y micropymes, reconoció Iglesias, "la penetración de este seguro es casi nula ahora mismo". A los riesgos directos, "se suma la responsabilidad ante entidades que regulan los derechos de los ciudadanos en cuanto a la privacidad de sus datos".

Para explicar el aumento de la concienciación, Carmen Segovia, directora de ciberriesgos de Aon España, subrayó tres factores principales: "Recientemente se han producido ciberataques mediáticos, la regulación y las sanciones son cada vez más severas y las grandes compañías comienzan a auditar a todos sus proveedores".

Puesto que esta exigencia afecta de forma directa aquellos que trabajan con grandes corporaciones, "muchas pymes comienzan a adquirir una póliza de ciberriesgos por una obligación contractual con su cliente".

ALAN ABREU
Responsable de riesgos cibernéticos de Hiscox

"Las empresas deben tener en cuenta que hoy es más probable sufrir un ciberataque que un robo o un incendio"

CARMEN SEGOVIA
Directora de ciberriesgos de Aon España

"La concienciación ha subido por los incidentes mediáticos, las sanciones y las grandes empresas que auditan a proveedores"

KAREN VELANDIA
Especialista en productos ciber de Chubb

"Las compañías son más conscientes, pero aún no piensan en el seguro, sino en medidas de seguridad perimetral"

SALVADOR MOLINA
Presidente de Foro Ecofin

"La llegada del 5G podría disparar la piratería online y el negocio de las compañías aseguradoras de ciberriesgos"

HIGINIO IGLESIAS
Consejero delegado de E2K

"La debilidad puede estar en cualquier lado: atacar a un proveedor pyme puede hacer daño a una gran compañía"

RAFAEL SIERRA
Director de SegurosNews.com

"Las empresas son conscientes de que los ciberriesgos existen pero desconocen cómo prevenirlos"

Ante la necesidad de adaptarse a lo que necesitan las empresas, las propias pólizas han evolucionado. Así, Segovia precisó que "se han ido añadiendo nuevas garantías, como los cupones de descuento para las pymes o la pérdida de beneficios". Estos nuevos productos facilitan que las empresas actualicen su visión sobre estas pólizas y las perciban como una herramienta que facilita la gestión del riesgo.

Otra alternativa es que los seguros de riesgos cibernéticos evolucionen hacia la paquetización con pólizas casi a la carta, como el multirriesgo empresarial. "Dependerá del segmento de mercado al que te dirijas pero, en los segmentos pequeños, seguramente se acabarán haciendo coberturas paquetizadas", consideró Higinio Iglesias.

Riesgos

Aunque el abanico de posibles vulnerabilidades es amplio, las compañías deben vigilar con especial atención algunos aspectos específicos. "Por suerte, en España no hemos tenido eventos de gran impacto en el último año pero sí se producen incidentes con mucha frecuencia", comentó Karen Velandia. En concreto, llamó la atención sobre las infecciones de *malware* provocadas por una protección insuficiente, errores humanos de empleados y ataques de *phishing*.

Por otra parte, "la gran epidemia hoy es la extorsión cibernética en todas sus versiones", matizó Alan Abreu. Además, añadió que existe preocupación por la posibilidad de que se repita un nuevo *Wannacry*, el mayor ataque de *ransomware* de la historia que tumbó más de 200.000 equipos en 150 países. Desde Hiscox, señalan que algunas versiones antiguas de Windows cuentan con una vulnerabilidad en términos de seguridad que podría poner en riesgo a las empresas que los utilicen, por lo que recomiendan su actualización.

"La debilidad puede estar en cualquier lado: basta con atacar a un proveedor del segmento pyme para hacer daño a una gran empresa", agregó Higinio Iglesias. Junto con la ciberextorsión, Carmen Segovia avisó de que el fraude por ingeniería social es el principal recurso utilizado por los *hackers* para acceder a una empresa.

En conclusión, "la ciberseguridad no puede ser sólo una cuestión de indemnizaciones para el sector de los seguros, sino un reto de prevención, con un asesoramiento previo a las coberturas que analice y cierre vectores de riesgo en las empresas clientes", recalcó Salvador Molina, presidente de Foro Ecofin.

La tecnología es un ingrediente explosivo para este cóctel de riesgos. "La llegada del 5G va a impulsar que millones de dispositivos lancen a la red millones de datos gracias al Internet de las Cosas, pero a la vez representan nuevas ventanas abiertas al mundo pirata de los *hackers*", comentó Molina. Esta coyuntura podría "disparar la era de la piratería online y el negocio de las compañías aseguradoras de ciberriesgos".