¿Qué pasa si el virus es tan nuevo que no se encuentra en tu póliza?

Los gastos asociados a la recuperación de un ciberataque pueden borrar tu empresa de la faz de la tierra. Así trabajan las compañías de seguros para anticiparse al desastre y solucionarlo sin quebrar en el intento

Cualquier empresa del tamaño que sea y del sector que sea está expuesta a sufrir una incidencia.

En este bombo de adversidades en potencia cabe de todo: terremotos, incendios, picos de tensión y cada vez más ciberataques. No en vano, los hechos conocidos de infracciones penales relacionadas con la cibercriminalidad pasaron de constituir 42.182 en 2012 a alcanzar los 81.307 en 2017, de acuerdo con las estadísticas que recopila el Ministerio de Interior.

¿Cómo se defiende uno en un ecosistema cada vez más digital y en el que la cibercriminalidad se ha duplicado en seis años? Cuando un virus informático llama a tu puerta, es mejor que estés preparado. Pero si tu antivirus no es suficiente y el condenado consigue entrar, las consecuencias pueden ser letales, a menos que tengas una ciberseguro. Al final los vamos a necesitar sí o sí. Simplemente por el hecho de cubrir nuestra responsabilidad civil el caso de pérdida de información y demás, lo vamos a necesitar. Serán productos que se convertirán en algo convencional como complemento a otras medidas de ciberseguridad", razona Marco Lozano, coordinador de empresas y profesionales de Instituto Nacional de Ciberseguridad (INCIBE).

Las más beneficiadas de estos modelos de cobertura son en la actualidad "todas aquellas organizaciones o empresas que tengan que responder frente a una responsabilidad civil, ahora que se producen tantas fugas de información, pérdidas de datos o atentados contra la privacidad de las personas". La clave está en el dinero que están juego cuando se produce alguno de estos incidentes. "Son los que exigen desembolso económico mayor al que muchas empresas no pueden hacer frente de una manera convencional, sobre todo, pymes y microempresas".

Puesto que la idea es que sean las aseguradoras las que neutralicen estos

gastos, como siempre, de acuerdo con lo establecido en las pólizas, la estimación del riesgo es clave para que el negocio tenga sentido.

"Durante muchísimas décadas ha habido determinados tipos de seguros que han sido iguales a lo largo del tiempo. Al final tenemos muy claro por dónde nos vienen los problemas y cada cuánto más o menos vamos a tener un problema grande". Pero un *ramsonware* no es lo mismo que un terremoto. Al hacer frente uno de estos virus secuestradores de información, se complica la tarea de estimar la probabilidad del ataque, su impacto y las particularidades del *malware* en cuestión. El aumento de la cibercriminalidad también ha venido acompañado de un aumento en la variedad de las armas empleadas por los cibercriminales. Diariamente cargan contra las redes nuevas familias de virus pensadas para saltar las barreras que frenaron a sus predecesores. Este riesgo nos cambia totalmente la vida porque se mezclan muchas cosas y el mundo tecnológico va muy rápido.

¿Qué pasa si la cepa que nos ha atacado no está en la póliza? ¿Tiene sentido asegurarnos y pagar el coste que ello implica en un entorno tan cambiante? La respuesta es sí, si tu seguro es suficientemente adaptable. Las pólizas están escrita de manera lo suficientemente amplia como para que cubran esas variaciones de un día para otro. Además, acompañan sus coberturas con servicios de asesoramiento experto 24/7 y programas de formación para que la empresa cuente con una barrera adicional en el que suele ser su punto débil: los empleados. "Consideramos que aproximadamente el 85% de los incidentes que ocurren en las organizaciones están provocados por empleados, la mayoría, de manera no intencionada. Cubriendo esas necesidades de formación tendríamos bastante espectro cubierto y podríamos considerar que las empresas están más o menos protegidas", coinciden especialistas.

Las aseguradoras, de hecho, parten con ventaja en este terreno, puesto que, junto con el sector financiero, son el caramelito más apetecible para los cibercriminales. Según los datos que se manejan, este ámbito concentró un 19% de los ataques e incidentes registrados en 2018.

Desde el Instituto Nacional de Ciberseguridad han asistido al nacimiento de este mercado, inexistente hace tan solo unos años, en España. "Desde nuestro punto de vista, tenemos una oferta que es suficiente y que cubre, por lo menos, los aspectos más críticos, que podrían dejar a una empresa sin actividad o causarle un gran daño".

Fuente de información:

https://retina.elpais.com