¿Cómo se ve afectada una pyme por un ciberataque?

Las pequeñas y medianas empresas son una parte importante de la infraestructura económica y cibernética de los países. Sin embargo, para algunas, la seguridad de su información, sistemas y redes, no es su principal prioridad. Generalmente, no cuentan con los recursos para invertir en seguridad de la información de la misma forma en que las empresas más grandes pueden hacerlo, lo que las hace más vulnerables a los ciberdelincuentes.

En este sentido, las pymes se pueden ver afectadas por un evento cibernético de varias formas:

- Perder dinero.
- Servir de acceso a objetivos más destacados por medio de su rol o sus productos y servicios en una cadena de suministro.
- Perder información crítica para administrar su negocio.
  Sufrir daños reputacionales que afecten la confianza de sus clientes.
- Perder ingresos como consecuencia de la interrupción de su actividad.
- Recibir sanciones de entes de control y vigilancia como consecuencia del mal uso de la información.
- Ser demandadas o recibir reclamaciones por parte de personas afectadas debido al mal uso de la información.

Pymes: en la mira de los ciberdelincuentes

El acelerado desarrollo de las tecnologías de la información y la comunicación que se ha dado en las últimas décadas, ha multiplicado las alternativas de interacción y conexión entre las personas y su entorno, masificando el uso de dispositivos que permiten enviar y recibir información de manera inmediata y en tiempo real.

Las empresas no son ajenas a esta realidad: hoy los negocios se realizan en el ecosistema digital y global. A través del ciberespacio viajan datos fundamentales para la operación de las compañías y en los servidores, los data centers y en la nube se almacena información confidencial. Esto incentiva la competitividad entre las empresas.

Un ejemplo de un ecosistema digital es internet. Esta tecnología se ha convertido en una herramienta imprescindible para las empresas del mundo en cualquier campo de acción. Se ha transformado en un espacio muy útil para ampliar los mercados, estar en comunicación permanente con las personas, almacenar información y recolectar los datos personales de clientes actuales y potenciales.

Sin embargo, la actividad en la red conlleva riesgos, como el cibernético, que aumenta en la medida en que se descubren novedosas formas de vulnerar la información.

¿Qué es el riesgo **cibernético?**

El riesgo cibernético se refiere a cualquier riesgo que proviene del uso de información electrónica y su transmisión, incluye el daño físico que puede ser causado, el fraude cometido por el robo de información, cualquier responsabilidad proveniente del almacenamiento, disponibilidad, integridad y confidencialidad de datos, la cual normalmente se encuentra relacionado con individuos, compañías o el mismo gobierno

Las causas de este riesgo van desde los ataques cibernéticos, los virus informáticos y los correos malintencionados, hasta los errores humanos, los empleados que buscan recibir beneficios de manera fraudulenta, el uso inadecuado de información por parte de los proveedores, entre otros.

Los riesgos cibernéticos no solo se suscriben a amenazas tecnológicas o a objetivos de los ciberdelincuentes. Su materialización no siempre pretende generar este tipo de impactos u obtener beneficios económicos o financieros. Algunos ataques son motivados, por ejemplo, por un acto de venganza, por despedir a un empleado, la emoción de causar daños o el reto personal e intelectual de un ataque exitoso.