Día de la seguridad informática, ¿cómo proteges la información de tu empresa?

La conectividad es uno de los términos más utilizados y que ha surgido en la era digital, ha cambiado la forma en la que interactuamos y nos comunicamos no sólo entre usuarios sino también a nivel empresarial. Este hecho, viene acompañado de riesgos en la seguridad de la información ya que los criminales han encontrado nuevas formas de atacar a través de la red.

La vulnerabilidad ante este tipo de situaciones es alta, y ya lo vivimos en los últimos meses con ciberataques simultáneos como WannaCry, donde cientos de empresas de 150 países fueron víctimas de este ataque masivo que “secuestró” más de 200 mil computadoras.

La pregunta es: ¿estamos preparados para enfrentar nuevos ataques como fue WannaCry?

Las cifras dicen que no. El cibercrimen ha crecido a grandes escalas y es uno de los delitos más rentables para quienes están detrás. En México, de acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) en 2016 aumentaron 123% las quejas por fraude cibernético, lo que implicó un millón 700 mil reclamos.

El costo promedio para resarcir las pérdidas es de alrededor de 1.9 millones de dólares; sin embargo, esta cifra se cree que es mucho mayor porque no todas las víctimas hacen una denuncia, ya sean usuarios, pequeñas o grandes empresas.

Los ataques se presentan en mayor medida en dispositivos móviles, debido a la masificación de la tecnología y la facilidad de acceso a internet. Aunque cabe señalar que cualquier dispositivo que pueda conectarse a la red, es susceptible de ser intervenido.

¿Qué se puede hacer al respecto?

Reconocimiento: Primero que nada, se debe asumir que cualquier persona o empresa es vulnerable a un ataque. En la mayoría de las ocasiones el cibercriminal está dentro del sistema espiando los movimientos antes de cometer el delito, que además puede afectar a los clientes de la víctima.

Tomar medidas: La actualización de los sistemas es una medida preventiva básicas que deberían llevar a cabo todas las empresas; así como hacer pruebas de penetración, uso de contraseñas seguras y segmentación en el acceso a la información de la red, por mencionar algunas.

Acciones: La protección de la seguridad de la información es posible, siempre y cuando se creen hábitos y se cuente con un plan de acción para el resguardo y protocolos a seguir ante una amenaza latente de un ciberataque.

Para llevar a cabo estas acciones, KIO Networks cuenta con Cyber Shield, el producto más completo en la industria de seguros informáticos, ofrece cobertura en caso de robo o pérdida de información, con un respaldo por pérdidas financieras y afectaciones en hardware; además de especialistas en informática, apoyo legal y de relaciones públicas.

El panorama es desafiante, ya que, a diferencia de hace algunos años, los ataques no se limitan a sitios de gobierno, empresas o instituciones financieras: también las universidades, centros de investigación o todos aquellos organismos cuyos datos puedan ser de interés para terceras partes, por ser confidenciales, información fiscal o propiedad intelectual.