WannaCry: un vistazo de cómo ha evolucionado el cibercrimen

La seguridad dentro de las empresas es fundamental. Lo podemos ver en grandes corporativos al entrar, en los que solicitan en la puerta identificación, nombre, firma y un recorrido por detectores de metal, revisión de bolsos y registro de computadoras. Estos protocolos preventivos deberían seguirse en todos los aspectos de seguridad de una empresa, ya que muchas veces, lo más importante que tienen no está en sus escritorios, sino en sus computadoras.

Un ejemplo es el que vivimos hoy, con el virus WannaCry: actúa de manera remota y hasta el momento, ha trascendido que afectó a 74 países. Una de las empresas afectadas es la española Telefónica.

WannaCry bloquea el acceso al administrador y los usuarios reales, pidiendo una recompensa a cambio. Normalmente ésta se exige en Bitcoins, una criptomoneda (medio digital de intercambio) prácticamente imposible de rastrear.

Para Gustavo Chapela, director general de Sm4rt, unidad de negocio de Seguridad de la Información de KIO Networks, es una muestra que todas las empresas, sin importar tamaño, son susceptibles a un ciberataque: en el caso de las pequeñas, porque no suelen estar atentos a sus vulnerabilidades; y en el caso de las grandes, por la ganancia que pueden representar.

Ante este escenario, es fundamental actualizar constantemente los sistemas y la seguridad de los mismos, realizar una evaluación de los riesgos cibernéticos para determinar qué medidas son necesarias implantar, desde adquisición de nueva tecnología, capacitación de los colaboradores hasta la adquisición de un seguro.

En el caso de México, se calcula que sólo 1 de cada 4 empresas cumpliría con prácticas internacionales para resguardar sus datos. Aunque, enfrentan el riesgo de una intrusión, cuyo costo promedio para resarcir las pérdidas puede sumar alrededor de 1.9 millones de dólares

Hoy vemos un ejemplo claro de la importancia que pueden tener estas medidas preventivas. En el caso de un seguro, lo deseable es que resguarde más allá de lo financiero, pues como vimos hoy, el impacto también va sobre la reputación e imagen; además de repercutir en servicios a terceros.

###

Acerca de KIO Networks

KIO Networks, inicia operaciones en el 2002 con capital 100% mexicano, es un proveedor de servicios de Tecnologías de Información de misión crítica y de servicios de Outsourcing que opera los Centros de Datos de última generación y más alta seguridad, disponibilidad y densidad en Latinoamérica. KIO Networks ofrece servicios y soluciones integradas de TIC, tanto para el sector público como para el sector privado, soportadas en sus 32 Centros de Datos dentro de un ambiente seguro, escalable y profesional. La compañía combina de manera óptima infraestructura, metodología, procesos, herramientas y personal certificado, proporcionando los niveles de servicio más rigurosos en cumplimiento con los estándares mundiales conocidos como TIER IV, ICREA, ITIL, SSAE16, ISO20000, ISO27001 y SAP. KIO Networks tiene presencia en México, Panamá, Guatemala, República Dominicana, Estados Unidos y España.

KIO se origina de la lengua swahili que significa espejo y simboliza los elementos esenciales de dualidad y redundancia, componentes medulares de los servicios de la compañía.

Contacto de prensa

Viridiana Romero
KIO Networks | Meraki
viridiana@merakimexico.com
Móvil.55 2909 5149