¿Cómo sobrevivir localmente a un intento de ciberrobo?

Aunque aún es incipiente, los requerimientos de ciberseguridad comienzan a preocupar a los directivos debido a sus implicancias para los negocios.

Un ataque cibernético, puede hacer quebrar a una compañía. Como en la actualidad gran parte de los negocios se basan en el almacenamiento de datos sensibles de clientes y operaciones de las empresas, así como de transacciones financieras, entre otros movimientos, el hackeo –acceso a una cuenta privada para insertar un código malicioso en un sitio web– empieza a preocupar a las compañías uruguayas. La preocupación es, sin embargo,incipiente.

Según datos proporcionados a El Observador por el Centro de Respuesta a Incidentes de Seguridad Informática (CERT) –área de seguridad en este campo de la Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento (Agesic)–, en 2016 se produjeron 769 ciberataques en Uruguay – 33% más que el año anterior–. De estos, 15 casos fueron categorizados como de alta severidad y seis de muy alta severidad. Estos son solo los casos denunciados, lo que significa que pueden haber ocurrido varios más. Sin embargo, Uruguay ha avanzado en los últimos 10 años en materia de ciberseguridad y es el país de la región mejor evaluado, según el último reporte de la Organización Estados Americanos (OEA).

Impactos considerables

Un ataque informático en una compañía puede tener consecuencias en varios aspectos de su negocio. Primero, en su propia operativa, con consecuencias económicas del robo de información. Además de esto, la reputación de la compañía y la imagen que los clientes tienen de ella puede verse afectada.
La efectividad en la seguridad informática conlleva un cambio de cultura organizacional. Todas las áreas deben comprometerse con acciones concretas, y la capacitación de los profesionales es clave.

Fuente:http://www.elobservador.com.uy/como-sobrevivir-localmente-un-intento-ciberrobo-n1022976