Ransomware e Ingeniería social, ¿cómo protegerse después del ciberataque que sorprendió al mundo?

Por ***Diego Taich***, director de Tecnología IT de PwC Argentina.

El creciente ataque que "secuestra" los propios datos de una empresa a cambio de un rescate.

Los ataques del virus W*annaCry* pusieron en jaque a grandes organizaciones de todo el mundo, afectando más de 200.000 computadoras en 150 países. Fue el primer gran golpe de una nueva modalidad de ciberataques: el *ransomware* –del inglés *ransom*, rescate, y *ware*, por software–, que vulnera a las compañías, dado que los datos de la víctima son encriptados y se le solicita un rescate económico, pagado con una criptomoneda, para permitir el acceso. En ese sentido tenemos también que mencionar la gran cantidad de ataques de este tipo durante 2017 (NotPetya, Locky y CrySis, entre otros).

Algunos analistas estimaron que durante el tercer trimestre de 2017, las empresas –en el nivel global– fueron atacadas cada 40 segundos por un *ransomware*, y lamentablemente, se espera que esta tendencia crezca en los próximos años. Asimismo, hay una progresiva cantidad de ataques sobre los sistemas de control en infraestructuras críticas, usados principalmente en las industrias de servicios públicos (agua, gas, combustible, electricidad, etc.). Trabajar en la ciberseguridad en este ámbito sin duda requiere de conocimiento experto y de la aplicación de medidas específicas de protección.

Una investigación realizada por PwC demostró que la mayoría de los incidentes de *ransomware* provocaron horas de inactividad e incluso algunas redes tuvieron que ser desconectadas hasta 10 días. Además, los atacantes conservan la información robada en su poder y pueden venderla o publicarla aún después de que la compañía pague el rescate.

A estos flagelos se han sumado recientemente las vulnerabilidades *Meltdown* y *Spectre* que se han detectado en los chips que equipan millones de computadores y smartphones, y que permitirían acceder a información sensible en forma no autorizada; si bien no hay señales de que hayan sido explotadas aún.

El impacto de *WannaCry* –uno de los *ransomware* más dañinos que se hayan registrado– disparó la alarma entre las organizaciones: ¿cuán vulnerables son los sistemas de seguridad en las compañías?, ¿qué medidas deberían tomarse para estar preparadas?

La protección efectiva contra los ciberataques no tiene tanto que ver con factores tecnológicos puntuales, sino con una administración de riesgo proactiva. Para ello, deberíamos considerar cinco factores clave:

1. **Mantenimiento digital sólido.** El episodio *WannaCry* destaca la importancia de una gestión de Tecnología de la Información en alerta, lo que esencialmente implica mantenerse actualizado con los últimos avances tecnológicos, pero también implementar prácticas rigurosas, como realizar copias de seguridad de los datos de la empresa, controlarlas regularmente y guardarlas en sistemas diferentes.

2. **La habilidad de detectar un comportamiento intruso.** El error humano sigue siendo la manera más frecuente de obtener acceso a información confidencial. Cualquier integrante de una empresa está expuesto a mostrar la información a una amenaza cibernética sin saberlo, a través de un correo electrónico fraudulento u otras técnicas de ingeniería social, y les otorgan acceso a los *hackers*. Las organizaciones que cuentan con prácticas de administración de riesgo efectivas, rara vez divulgan información sensible a personas ajenas, protegiendo particularmente cuentas administrativas y otra información privilegiada. La colaboración entre profesionales de la seguridad de diversas organizaciones es una de las mejores defensas contra la actividad de delito informático.

3. **Diseño cuidadoso de la infraestructura de la Tecnología de la Información.** Cada compañía posee activos de información que son especialmente valiosos: propiedad intelectual, datos confidenciales de clientes o información financiera, entre otros. Estos activos deben recibir una protección especial, por lo que es necesario que se diseñen sistemas acordes. ¿Qué vendedores, proveedores y socios tienen acceso a esta información, y qué se está haciendo para protegerla?

Es importante reconsiderar los controles de seguridad y autenticación, introduciendo datos biométricos, símbolos o la combinación de ambos.

4. **Planificación y ensayos anticipados.** De la misma forma que la organización desarrolla sus planes de emergencia (por ejemplo, en caso de incendios), se debería adoptar una estrategia similar para estar preparados al momento de los ciberataques. El plan debería especificar no solo cómo responder ante un hecho, sino también la cadena de mando de información para notificar a los clientes en caso de robo de la información que los afecte. Para estar preparado ante ataques, se debe establecer una matriz de decisión y determinar al momento del incidente quién recuperará la información de la copia de seguridad, o quién se comunicará con los secuestradores de la información. Pensar de antemano estas cuestiones ayudará a la organización a estar mejor preparada ante una crisis.

5. **Adopción temprana de tecnología en la nube**. Los sistemas basados en la nube se actualizan automáticamente, acumulan datos sobre ataques en tiempo real e incorporan restricciones integradas que separan las capas de software y bloquean el que resulte afectado. Esto constituye una ventaja respecto de los sistemas que dependen de las computadoras más vulnerables, en las instalaciones.

El *ransomware* representa una grave amenaza. Las acciones detalladas no serán efectivas si no se las integra a la cultura organizacional, para llevarlas adelante con plena conciencia en todos los niveles de decisión. Cuando estas acciones se hayan convertido en parte del ADN de la compañía, la destreza para el manejo de los riegos cibernéticos se transformará en un activo estratégico.