Cómo combatir los ciberataques (antes de que sucedan)

La ciberseguridad comienza a ser un punto para tener en cuenta en las pymes que buscan anticiparse a una problemática cada vez más común. Por qué aumentó la preocupación, qué acciones hay que tomar y las recomendaciones para no caer.

La conciencia de la ciberseguridad ha llegado a las Pymes. El uso de la tecnología cada vez más desarrollada en sus procesos de trabajo, ha generado también una mayor preocupación por los denominados hackers. Si la información se pierde, la empresa se cae. Es por eso mismo que luego de un largo periodo de inestabilidad en la materia, las pequeñas y medianas empresas empiezan a tantear el terreno de a poco e insertarse en la temática.

Según el International Business Report de Grant Thornton, la gran mayoría de las empresas medianas argentinas (67%) cree que las compañías entienden la severidad del riesgo digital. Dentro de lo que es riesgo, un 39% está de acuerdo con que, debido a nuevas regulaciones, se les ha prestado más atención a los problemas de privacidad que a la ciberseguridad en los últimos años. Es decir, el porcentaje de esta compañía, ya tienen un proceso en marcha que revisa las ciberamenazas, la privacidad de la información y las alteraciones a las operaciones en conjunto.

En entrevista con *Multitaskers*, Jerónimo Basaldúa, organizador fundador de Ekoparty, la conferencia de seguridad informática más grande de América Latina, se refiere a este aumento de la preocupación y aclara las razones: “Dentro del mundo de la seguridad informática hay una frase popular que dice: ‘existen dos tipos de empresas: las que fueron víctimas de una ciberamenaza y las que fueron víctimas pero que aún no se dieron cuenta’, y es a partir de esa toma de conciencia que surgen interrogantes como: ¿cuándo pasará? ¿de qué modo se producirá el incidente? ¿cuánto tiempo necesitará el atacante encontrar información valiosa? Todos estos interrogantes son cada vez más fuertes hoy en día y es por esto que cada vez se le presta más atención”, comparte.

Los puntos débiles

En el mismo reporte, Grant Thornton se refirió a las debilidades de las empresas consultadas y ellas mismas definieron sus puntos débiles en materia de protección cibernética. La más común entre las que respondieron, elegida por el 48% de las empresas, es depender demasiado en que el software haga todo el trabajo. Le sigue el hecho de que los empleados no logran entender de qué riesgos son responsables, con un 31%. Por último, un 17% cree que su estructura

de administración del riesgo digital está desactualizada o que no es adecuada para lo que se quiere lograr. Un 23% de empresas no sabe cuáles son sus puntos débiles.

Con los puntos frágiles definido, la pregunta ahora es: ¿hay buenas propuestas por parte de las compañías de seguridad? ¿Es accesible la incorporación de un especialista en la temática? En el reporte, más de la mitad de los encuestados (57%) está de acuerdo con que las empresas de seguros deberían mejorar su oferta de protección contra el riesgo de privacidad de la información. En respuesta a esto, Basaldúa opina que existen "múltiples ofertas de empresas de seguridad para mitigar estas amenazas". Más allá de esto, aclara que las Pymes deberían primero, antes de contratar soluciones de forma reactiva, "realizar diagnósticos de seguridad, para entender el nivel de riesgo y exposición de cada negocio". Entre los ejemplos, remarca que los servicios de SOC "Security Operation Center", permiten a las empresas "identificar los peligros antes de que sucedan, monitoreando 24x7 las redes de sus clientes".

Otra de las grandes problemáticas que afrontan esta problemática es la falta perfiles especializados. La ausencia de profesionales en ciberseguridad es un conflicto mundial. Según informes de ISC2, faltan aproximadamente 3 millones de profesionales que cuenten con las habilidades suficientes para satisfacer la demanda en este campo. En América Latina solamente, se necesitan más de 130.000 profesionales en ciberseguridad para cubrir la demanda que existe.

Qué hacer y cómo reaccionar

Sobre las acciones a realizar una vez que la empresa recibe un ciberataque, el fundador de Ekoparty, explica que lo primero que hay que intentar es "contener la amenaza" y detalla: "Dependiendo del tipo de ciberataque esto puede tener mayor o menor complejidad, por lo que siempre es recomendable llamar inmediatamente a expertos en seguridad que puedan asesorar correctamente en este sentido". Bajo esta línea, explica que existen políticas de manejo de incidentes "con metodologías y protocolos a seguir" y advierte que muchas veces, ante la urgencia de controlar un ataque, "hay acciones que pueden provocar la pérdida de validez legal de información que podría permitir identificar a los atacantes".

Por otra parte, a la hora de hablar de las consecuencias, el especialista explica que el impacto entre las grandes empresas y las pymes es diferente. En el primero de los casos, por ejemplo, los ciberataques son alarmantes, pero no sorprendentes. Caso contrario puede ocurrir en las pequeñas y medianas compañías donde, por ejemplo, un ataque de Ransomware, (un software malicioso que al infectar el equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar los archivos) en el ERP, que no tenga protección ni procedimiento de backups, "puede causarle un perjuicio enorme incluso dejarla fuera del negocio de forma indefinida".

Como cierre, desde Grant Thornton, ofrecen tres pasos para la administración integrada del riesgo digital. A continuación, cada uno de ellos:

1. Decida quién es responsable de manejar el riesgo de ciberseguridad y privacidad de la información, trace sus actividades y flujos de trabajo diarios, y vea si hay alguna superposición. Elimine procesos duplicados.

2. Asegúrese de que los procesos de riesgo digital se estén administrando según el enfoque end-to-end. Por ejemplo, la evaluación de terceros debería tener en cuenta ciberseguridad y privacidad de la información. Ambos factores deberían ser evaluados cuando se clasifica la información.

3. Cree un equipo o función integrado de manejo del riesgo digital que tenga las habilidades para manejar las amenazas de ciberseguridad y privacidad de la información. Encabécela con un director ejecutivo de riesgo digital capaz de luchar por el riesgo y de asegurar de que la función esté integrada a las decisiones estratégicas y operacionales en toda la empresa. Asegúrese de que la Junta supervise el riesgo digital activamente.