Urge poner en marcha y/o madurar programas de ciberseguridad maduros

Paula Álvarez, socia de Riesgo Cibernético de Deloitte, alerta sobre el incremento acelerado del cibercrimen

En México, uno de los casos de cibercrimen más sonado, conocido por todos y que cambió los paradigmas de la visión que tenían las organizaciones con respecto a la manera de protegerse, es el ataque al SPEI (Sistema de Pagos Electrónico Interbancario) sucedido hace tres años, un robo sofisticado realizado por ciberdelincuentes. Y aunque desde entonces se comenzaron a reforzar -en distintas industrias- las medidas de ciberseguridad, expertas como Paula Álvarez, socia de Riesgo Cibernético de Deloitte, aseguran que aún hay un largo camino por recorrer para hacer frente a este problema que enfrentan los negocios.

En entrevista, la Socia de Deloitte sostuvo que lo relevante del citado caso radica en que se atacó al sector más maduro en términos de ciberseguridad. "Fue a la industria financiera, los bancos y no sólo a uno, sino a algunos", enfatizó.

De acuerdo con Álvarez, este ataque fue planeado con tiempo, no sucedió de la noche a la mañana e incluyó al crimen organizado. "Hay que puntualizar que tiene un componente de crimen organizado local, pero también un componente importante de actividad cibernética, porque todo se dio a través de los sistemas", anotó.

Tras reflexionar sobre el tiempo y el modo de operar de estas organizaciones, la experta en riesgos cibernéticos sostuvo que esto pudo evitarse a través de programas de ciberseguridad maduros. "Entendiendo a la ciberseguridad como todos los mecanismos que podemos poner alrededor de nuestros sistemas y espacio virtual para estar mejor protegidos", dijo.

Y es que aseguró, el cibercrimen viene incrementándose de manera acelerada y que si bien las organizaciones hacen inversiones en materia de ciberseguridad, no están a la altura del escenario de amenazas actual. "Hay muchas puertas que hacen que la superficie de exposición al riesgo, que antes era más reducida, como puede ser solamente una red interna y un centro de cómputo propio, ahora se expande mucho más, derivado de las tendencias tecnológicas que están apalancando de forma acelerada las transformaciones de las organizaciones en las diferentes industrias (no solo es una transformación digital)", indicó.

¿Qué es el cibercrimen?

- Son todas organizaciones criminales que se dedican a atacar, vulnerando sistemas y que operan en el ciberespacio principalmente
- Opera en todo el mundo
- Al ser global, su target abarca a las organizaciones de todos los continentes

LA NUEVA ERA DE PROFESIONALES

Ante lo ya comentado, la situación global, regional y local respecto a la disponibilidad de talento en este espacio de la ciberseguridad es muy reducida, por no decir sumamente escasa. Actualmente algunas entidades educativas vienen trabajando en los últimos 2-3 años en desarrollar carreras y posgrados para que una persona pueda también estudiar "ciberseguridad", dado que hoy principalmente la especialización se va logrando con la experiencia laboral, certificaciones, y cursos especializados que no forman parte de un plan de estudios integral.

Paula Álvarez, socia de Riesgo Cibernético de Deloitte

Al respecto, Álvarez indicó que los hackeos son cada vez más complejos y persistentes, por lo que los directivos de las organizaciones y empresas deben prestar atención en este tema y por ello se requieren más profesionales expertos que se encarguen de tomar liderazgos al respecto.

Por ello, Deloitte apuesta a la especialización y profesionalización de nuevo talento, recién egresados o por egresar, quienes deberán contar no sólo con el talento técnico sino también con la capacidad para traducir los conceptos técnicos en términos entendibles para el negocio.

CIBER-ACADEMIA DELOITTE

A fin de cerrar parte de esa brecha que hay en el mercado de la ciberseguridad, Deloitte contrató y capacitó de manera virtual durante 5 meses a 110 profesionales de más de 15 países de Latinoamérica y de más de 20 universidades distintas, estudiantes que cursan el último semestre de sus carreras, para incorporarlos a sus prácticas.

A decir de Paula Álvarez, recientemente tuvieron la graduación de la primera generación de estudiantes de esta ciber academia, quienes recibieron diversas capacitaciones en materia de ciberseguridad, incluyendo competencias denominadas como "soft skills", con la idea que puedan seguir especializándose en Deloitte, a la vez que desarrollan una carrera profesional.

"Es un esfuerzo muy grande y responde a que no hay las suficientes personas para atender lo que se debe atender", mencionó la experta, para quien iniciativas como está ayudarán desde la arista de la falta de talento y especialización.

Sin embargo, dijo, para poder ganarle a esta "ciber tormenta perfecta" que hoy experimentamos, se requiere que las organizaciones hagan una labor grande que es el cierre de la brecha que tienen en términos de cibserguridad, comenzando con una estrategia de ciberseguridad, que les permita madurar sus capacidades de ciberseguridad en los ámbitos de la tecnología, procesos y personas para poder convertirse en organizaciones más seguras, vigilantes y resilientes, estando a la altura de las circunstancias.