Ciberseguridad ¿Estamos preparados?

Por Enrique Larrieu-Let
elarrieulet@gmail.com

No es novedad que casi todos los días aparecen en el mundo noticias sobre ciberataques, es más, hasta hay series de televisión que tratan estos temas. La ficción también toma en serio al cibercrimen, además, existen pruebas de que la ficción no está tan lejos de la realidad. Los ciberataques aparecen en las noticias casi todos los días a nivel mundial, y la ciberseguridad ha cobrado mayor importancia en los planes de líderes globales, tanto en el sector empresarial como de gobierno. Ellos están pidiendo colaboración y soluciones ya.

La ciberseguridad y la ciberdefensa no deben ser una preocupación, deben ser una ocupación.

De acuerdo con una encuesta reciente de El Estado de la Cíber-seguridad: Implicaciones para el 2016, formulada por ISACA y *RSA Conference*, ha habido un incremento continuo de ataques en los últimos dos años, dichos ataques han generado una demanda a nivel global de personal capacitado, una demanda que hoy día supera a la oferta. Los resultados de la encuesta de ciberseguridad muestran que un diez por ciento (10%) de los encuestados consideró que solo la mitad de los aspirantes al puesto se encuentran calificados para los roles en ciberseguridad. Más de la mitad afirman que toma entre tres y seis meses encontrar buenos candidatos, y el treinta y cinco por ciento (35%) se ve incapaz de cubrir los puestos vacantes.

La pregunta es: ¿quién cuida de la compañía mientras estos puestos continúan desatendidos? Existe también una falta de habilidades: más del setenta por ciento (70%) afirma que sus candidatos no comprenden el negocio, lo cual es un grave problema. La tecnología debe estar al servicio del negocio, y por lo tanto la gestión de TI debe estar alineada con la gestión del negocio y sus necesidades para poder agregarle valor.

Existe un lado positivo, no obstante: la certificación de conocimientos, habilidades y experiencia se considera extremadamente valiosa, y casi un setenta por ciento (70%) de los encuestados dice que contar con una certificación es indispensable para asumir roles en ciberseguridad eficientemente.

Sobre el autor
Ing. Enrique Larrieu-Let, CISM,
Profesional en Seguridad y Tecnologías de Sistemas de Información
Asociación de Auditoría y Control de Sistemas de Información - ADACSI, IAIA, Universidad del Salvador

Si bien la mayoría de los directivos se siente seguras de que sus respectivos equipos de seguridad están capacitados para la detección y respuesta ante incidentes, no obstante, de ese mismo grupo de directivos, casi la mitad se siente seguro solamente si el problema es sencillo de resolver y, conforme la complejidad de las amenazas de seguridad crecen, esto se vuelve más crucial.

La ciberseguridad está ganando el respeto del sector de liderazgo, esto se evidencia en la encuesta porque los presupuestos para seguridad han aumentado, y casi el noventa por ciento (90%) de los líderes ejecutivos están apoyando los emprendimientos en ciberseguridad.

La encuesta también revela que el lugar que tiene la seguridad de la información dentro de las organizaciones está cambiando. Hoy, todavía en la mayoría de las compañías, la seguridad de la información es considerada al nivel de TI como temas solamente técnicos y reportan su gestión a áreas de tecnología. Afortunadamente la cultura organizacional está madurando y comienza a divisarse como cada vez más organizaciones ubican a los CISO (*Chief Information Security Officer*) y a los CIO (*Chief Information Officer*) reportando directamente al CEO de la empresa facilitando la alineación de la gestión de TI con el gobierno de TI y éste a su vez alineado con el gobierno corporativo.

Nos encontramos en un momento crítico. Aquellos que hemos adquirido un poco de conciencia sobre la gravedad de la situación debemos desarrollar juntos una fuerza de trabajo con la intención de prevenir, detectar y responder a los sofisticados ataques de hoy en día. Es vital concientizar, entrenar y formar técnicos y profesionales capaces de realizar una gestión de TI y un gobierno de TI eficaz y eficiente.

Creo que estamos a tiempo, el momento indicado para formarse y entrenarse es ahora.

ISACA, consciente de ésta necesidad, ha creado *Cibersecurity Nexus* (CSX). A través de *CSX*, ISACA se compromete concienzudamente a solucionar la falta de habilidades en ciberseguridad. Ahora los profesionales pueden tener acceso a un valioso número de guías, herramientas, *networking* y entrenamiento, todo en el mismo lugar. La ciberseguridad es un problema dinámico para distintas organizaciones alrededor del mundo; la misma tecnología que nos brinda beneficios tan valiosos puede ser también utilizada para infligir graves daños.

Desde la Comisión Directiva de AADECA se está promoviendo el desarrollo de cursos sobre ciberseguridad orientados específicamente al sector industrial para facilitar el acceso a nuestros miembros al conocimiento en este campo en explosiva expansión.

La ciberseguridad y la ciberdefensa son actividades dinámicas y continuas por lo tanto requieren de capacitaciones también dinámicas y continuas.

La ciberseguridad y la ciberdefensa la debemos ejercer todos y desde todos los ámbitos. El simple acto de un joven de bajar una inocente aplicación en el dispositivo móvil de su padre, que trabaja en una compañía generadora de energía, podría terminar en infectar infraestructura crítica y dejar sin suministro eléctrico a toda una región o nación. La seguridad tradicional trata al incidente de infectar un dispositivo móvil como un hecho técnico y aislado, cuando desde el punto de vista de la ciberseguridad se podría tratar de un vector de ataque que forma parte de lo que se conoce como una amenaza avanzada persistente (APT por sus siglas en inglés).

Debemos trabajar juntos para crear un mundo digital más seguro. Después de todo, la ciberseguridad debe ser un "negocio" de todos. ❖