Portafolio

PORTAFOLIO - AGOSTO 17 DE 2017 - 09:09 P.M.
http://m.portafolio.co/negocios/empresas/la-ciberseguridad-es-responsabilidad-de-todos-508818

Ciberseguridad, responsabilidad de todos

El principal reto al que se enfrentan las compañías es llevar a cabo una transformación digital exitosa sin comprometer la seguridad.

Gianluca D'Antonio, Director del Máster en Ciberseguridad del IE Business School y presidente de ISMS Forum.

Cada vez más, las compañías le apuestan a pasar de la tradicional operación 'análoga' para entrar en el vertiginoso universo digital. Es un cambio radical que les permite moverse de una forma más eficiente y, sobre todo, rápida.

Pero, si bien son muchas las ventajas, también muchos los riesgos, y el ciberataque es uno de ellos. Sin embargo, hasta el momento, ese es un problema del que aún no se toma la suficiente conciencia. Gianluca D'Antonio, director académico del Máster en Ciberseguridad del IE Business School y presidente de ISMS Forum (Asociación Española para el Fomento de la Seguridad de la Información), quien participó en el foro 'Seguridad digital, confianza y corresponsabilidad', celebrado recientemente en Bogotá, hizo referencia a cómo el sector privado debe enfrentar ataques de seguridad digital y generar confianza entre los usuarios. El experto habló con Portafolio sobre este tema.

¿Cuáles son los mayores riesgos que enfrentan hoy las empresas?

Desde una perspectiva de riesgos tecnológicos, las empresas no han incluido, en su reingeniería de procesos de negocio, la ciberseguridad como un elemento básico para tener en cuenta. Según un reciente estudio, 'The hiscox cyber readiness report 2017', que ha analizado más de 3.000 empresas distribuidas en tres países, Estados Unidos, Reino Unido y Alemania, en términos de estrategia, recursos, tecnologías y procesos para hacer frente al cibercrimen, el 53 por ciento de las organizaciones evaluadas no estaba preparado para gestionar un ataque.

La transformación digital se basa en el uso masivo de las nuevas tecnologías. Estas son enablers, es decir, representan unos 'factores de facilitación', mientras que la ciberseguridad, por su naturaleza, introduce limitaciones a las capacidades de las tecnologías. Se trata, entonces, de buscar el equilibrio entre desarrollo tecnológico y gestión de los riesgos relacionados con este. Este es el reto principal al que se enfrentan las empresas: llevar a cabo una transformación digital exitosa, sin comprometer la seguridad de los procesos del negocio. Y esto solo es posible si las compañías y los profesionales que las componen asumen la ciberseguridad como responsabilidad de todos.

Los recientes ataques cibernéticos en el mundo encienden las alarmas. ¿Cómo enfrentar este lado oscuro de la tecnología?

Estamos asistiendo a un preocupante aumento de ciberataques a escala mundial. Y es precisamente su escala global la que nos tiene que hacer reflexionar sobre las posibles soluciones. La ciberseguridad es una necesidad para la sociedad en general: Estados, empresas y ciudadanos deben trabajar juntos para asegurar que la sociedad de la información y la economía digital puedan desarrollarse y prosperar sin amenazas. Para que esto sea posible, la ciberseguridad debe ser considerada 'un bien público'. La comunidad internacional, a través de sus organismos como la ONU, debe desarrollar un marco regulatorio global que discipline el uso de las redes y garantice el respecto de los derechos de los ciudadanos. En un mundo hiperconectado como el actual, las regulaciones de carácter nacional no son suficientes: el cibercrimen no tiene fronteras y puede llevar a cabo sus operaciones delictivas desde cualquier latitud, eludiendo de así las medidas de protección de los países.

¿Cómo se propagan virus informáticos como 'Wannacry o 'ransomware'?

Wannacry ha sido un ransomware insólito, ya que, a diferencia de los ransomware hasta hoy conocidos, tenía capacidades de propagación parecidas a las de un virus. En el caso de Wannacry, el ransomware disponía de un módulo de hunting capaz de buscar otras máquinas conectadas a la red e infectarlas. Los ransomware que habíamos conocido hasta la aparición de Wannacry no disponían de esta capacidad de infección, solo eran capaces de cifrar la información del ordenador destino de la víctima.

¿Se puede detener o eliminar esta epidemia? ¿Cuáles son sus recomendaciones?

Cada virus informático y cada ciberataque tienen características diferentes. El último al que hemos asistido recientemente, denominado Petya 2, por las similitudes con otro malware aparecido el año pasado, supone un nuevo reto para los expertos en ciberseguridad porque implementa nuevas técnicas de propagación. Ante este escenario de amenazas cambiantes, la única recomendación sensata es estar preparados, y esto significa gestionar la ciberseguridad como un proceso de mejora continua y no como un producto finito. Las empresas deben adquirir competencias en materia de ciberseguridad, y esto solo es posible a través

de una definición clara de roles y responsabilidades en este ámbito. En los próximos tres años necesitaremos de más de dos millones de profesionales expertos en ciberseguridad.

¿Qué factores deben tener en cuenta las empresas para implementar nuevas estrategias de seguridad?

Deben considerar la ciberseguridad una inversión en vez de un gasto. Algunos estudios (como el de Gemalto) aseguran que el 65 por ciento de los clientes de una empresa cambiarían de compañía si sus datos fueran sustraídos como consecuencia de un ciberataque. Consecuentemente, invertir en ciberseguridad puede suponer una ventaja competitiva sobre la competencia y un valor diferencial hacia los clientes y el mercado.

¿Confiar o no confiar en la nube?

¡Esto depende de la nube! La nube es un concepto genérico detrás del cual existen tantos modelos de negocio como tantas son las arquitecturas de sistemas que lo soportan. Mi recomendación es que cada organización lleve a cabo un atento análisis de riesgos antes de emprender el camino hacia la nube.

La seguridad de los sistemas de información es una responsabilidad compartida. ¿Qué están haciendo los gobiernos en esta materia?

Algunos gobiernos ya han implementado una Estrategia Nacional de Ciberseguridad, como es el caso de Estados Unidos, Reino Unido o de España, para citar solo algunos países. Este es el primer paso para desarrollar, de manera orgánica, las diferentes capacidades que un Estado necesita para hacer frente a este nuevo desafío. En la estrategia se definen los objetivos de un Estado y los recursos que va a emplear para su consecución.

Como lo señalé anteriormente, la ciberseguridad es un proceso de mejora continua, y para ello los países deben asumir el liderazgo de este nuevo escenario y promover las acciones oportunas para asegurar un ciberespacio libre de amenazas y confiable.

Rosa María Cárdenas