RETOS Y TENDENCIAS DE LA SEGURIDAD INFORMÁTICA EN ASIA PACÍFICO

Este artículo pretende describir las tendencias y particularidades del Mercado de la Seguridad Informática en Asia Pacífico. El articulo presenta las opiniones personales de Alex Quintieri y Daniel Cabezas, y no representan de manera alguna, las opiniones corporativas de Ernst & Young o GE Capital.

La región de Asia Pacifico está considerada una de las de mayor crecimiento económico a nivel mundial, con una media de un 6% de crecimiento en 2012, según el FMI. Pero no solo la economía crece rápidamente en Asia Pacífico. La demanda de profesionales de la Seguridad Informática sigue en aumento, con una previsión del 11.9%[1] de crecimiento sostenido.

El panorama de la Seguridad Informática en la región presenta unos niveles de madurez muy heterogéneos. Este hecho viene derivado de una gran diversidad en el marco legislativo y aplicación del mismo, así como en los requerimientos corporativos respecto al Gobierno de las TI.

Por ejemplo, países con influencia anglosajona han desarrollado y aplicado rápidamente un marco legislativo en Privacidad de Datos. Este es el caso de Hong Kong, donde en 1997 se definió la Ordenanza de Datos Personales[2], o de Australia, publicando la Ley de Privacidad[3] en un temprano 1988. Japón creó a su vez la Autoridad Supervisora para la Protección de Datos Personales en 1998, y la ley de Protección de Datos Personales en 2003.

Otros países en la región no han sido tan ágiles desarrollando un marco de regulación para la Privacidad de Datos. Este es el caso de Filipinas[4], donde la Ley de Privacidad de Datos acaba de entrar en vigor el pasado agosto 2012. Lo mismo sucede con la reciente aprobación, en el parlamento, del Proyecto de Ley para la Protección de Datos Personales de Singapur, el cual se espera entre en vigor el próximo enero 2013.

Muchos otros países, en Asia Pacífico, están todavía trabajando para establecer un marco legislativo en materia de Privacidad de Datos. Esta diversidad de madurez en cumplimiento normativo, viene complicada por una carencia de tendencias a converger, o alinear, las leyes relacionadas con Privacidad de Datos y Seguridad en Asia Pacifico. Más aun, en algunos casos el desarrollo de marcos heterogéneos de cumplimiento regulatorio se ha visto menguado por intereses de la industria, o desalineación con la realidad de los mercados en Asia Pacífico. Este es el caso ocurrido en la implementación de los requerimientos derivados de Basilea III.

Al mismo tiempo que las empresas centran esfuerzos en alinearse con el cambiante entorno de cumplimiento normativo,las empresas en Asia Pacifico están centrando esfuerzos en otras áreas de mejora, en la Seguridad de la Información.

Primero de todo, las compañías están concentrando recursos en sus Planes de Continuidad, para así garantizar la operativa de negocio. En una región con grandes países, densa población, y grandes volúmenes de información, los retos para una robusta estrategia en la Continuidad de Negocio son también grandes.

Otro reto al que los Directores de Seguridad se encuentran inmersos, es la presión empresarial para alinearse con el acceso masivo a dispositivos electrónicos personales, y el uso de los mismos con fines Corporativo (BYOD[5]). Las empresas están estableciendo objetivos de migrar hacia un uso de Dispositivos Personales, para permitir el acceso remoto de empleados a los Sistemas Corporativos. Sin embargo, muchas compañías no están aún preparadas para adecuar el marco de Seguridad Corporativa, y ofrecer las garantías necesarias en las comunicaciones, y protección de datos, a través de dispositivos personales.

La Seguridad en Redes Sociales es también un factor en auge para muchas empresas en Asia Pacífico, en un intento de acercarse aún más a los clientes. La integración de plataformas transaccionales con Facebook o Weibo[6], entre otros, trae nuevos retos para garantizar que la autenticación y seguridad de los datos están bajo control.

Como no podría ser diferente, en una región donde la protección de la Propiedad Intelectual es un asunto sensible, y tiene a países punteros en subcontratación de T.I. (India, Indonesia o China, entre otros), la prevención de fuga de Información está en auge. Despliegues de soluciones técnicas DLP, iniciativas de Clasificación de la Información, o la creación de procesos para controlar las Transferencias de Datos, están creciendo en toda la región.

Finalmente, la Seguridad en *Cloud* sigue siendo un asunto de preocupación para los legisladores, y es un área de interés para las compañías en Asia Pacífico. A pesar de encontrarse una madurez de Servicios *Cloud* bien establecidos, como son herramientas de CRM, Recursos Humanos, o herramientas de comunicación, pocas compañías han tomado el paso de migrar su información crítica de negocio a entornos de *Cloud* Público. Hay muchas razones para no haber tomado ese paso, pero una de las grandes preocupaciones es la falta de control, y retos a nivel de auditoría, para garantizar la Seguridad de los Datos en plataformas de *Cloud* Público.

Adicionalmente, diferentes marcos legislativos relacionados con la conservación y clasificación de datos, incrementan la complejidad y los riesgos de responsabilidades asociadas a externalizar los servicios críticos de las T.I. Por ejemplo, en China, el gobierno tiene definida la Ley del Secreto de Estado, la cual prohíbe el almacenamiento de cualquier Secreto de Estado fuera del país. Dado que la definición del concepto de Secreto de Estado, en la Ley, es amplia y confusa, muchos Directores de T.I. se muestran reacios a almacenar una amplia variedad de datos corporativos fuera de China. Por otro lado, el Banco Central de Indonesia, requiere a cualquier entidad de Servicios Financieros con oficinas en el país, a almacenar los datos de sus clientes en repositorios locales. Este hecho incrementa los costes de mantenimiento y seguridad para operar en el país.

En conjunto, el mercado de la Seguridad Informática en la región de Asia Pacífico se halla inmerso en grandes retos. Una gran variedad de cambios en el marcolegislativova a incrementar la presión en las empresas, para garantizar un alineamiento adecuado del Gobierno de las T.I. con las nuevas regulaciones. Las multinacionales también están requiriendomayor madurez en el Gobierno I.T., homogeneizado los niveles en todos los países, y reduciendo las diferencias que previamente existían. Más aun, existen síntomas que muestran empresas demandando controles más estrictos en la Seguridad Informática, para aquellos países de rápido desarrollo económico, o donde la protección de la propiedad intelectual es motivo de preocupación. ■

Alex Quintieri
Deputy CISO Asia Pacific
GE CAPITAL

Daniel Cabezas
IT Security Manager
ERNST & YOUNG

[1] Previsión de la Demanda para Profesionales de la Seguridad de la Información en Asia Pacífico (2010 - 2015). *Frost& Sullivan 2011 (ISC)² Global InformationSecurity WorkforceStudy.*

[2] Ordenanza de Datos Personales, Hong Kong. http://www.pco.org.hk/english/ordinance/ordglance1.html#dataprotect

[3] Ley de Privacidad, Australia.http://www.privacy.gov.au/act/ipps/index.html

[4] Ley de la República 10173, Filipinas. http://www.gov.ph/2012/08/15/republic-act-no-10173/

[5] BYOD de las siglas en Inglés "BringYourOwnDevice" (trae tu propio dispositivo)

[6] Weibo esuna de las Redes Sociales más populares en China, similar aTwitter (http://weibo.com)