GIANLUCA D'ANTONIO, CISO DE FCC Y PRESIDENTE DE ISMS FORUM

"La seguridad condiciona la transformación digital pero no la paraliza"

María José Marzal

Las organizaciones se encuentran, en su gran mayoría, abordando procesos de transformación digital en los que una parte crítica es la seguridad. ¿Cómo se enfoca desde su organización este paso desde el punto de vista de la seguridad y de la figura del CISO?

Es cierto que toda la sociedad se encuentra inmersa en ese proceso del paso de una sociedad analógica a una digital y, en ese camino, creo que es absolutamente necesaria la existencia de una figura que englobe toda la seguridad. Una seguridad en mayúsculas que integre la seguridad física y la lógica y hacia ese objetivo tenemos que encaminarnos todas las organizaciones.

Invertir en seguridad es algo que supone un gran esfuerzo sobre todo en el convencimiento de su necesidad hacia la alta dirección. ¿Cree que las empresas españolas deberían invertir más en este capítulo?

Sí es cierto lo que comenta y, sí, es necesario incrementar la inversión en seguridad en torno a dos puntos porcentuales. En estos momentos, la inversión

en seguridad en España ronda entre un 3-4% del presupuesto global de tecnología y, desde mi punto de vista, debería incrementarse hasta al 6-7% que es lo que apunta Gartner Group.

Parece que otro de los grandes problemas en esta área de la seguridad en nuestro país es la escasez de profesionales. ¿Qué opina desde su óptica de presidente de ISMS Forum?

Es cierto, y es uno de los grandes problemas a resolver. Estamos hablando de que aproximadamente el 35% de los puestos de trabajo en seguridad informática no se pueden cubrir en España por falta de profesionales.

El pasado año se perdieron más de 14.000 millones de euros por ciberdelitos. ¿Por qué se sigue perdiendo tanto dinero cuando parece que la tecnología cada día es más sofisticada?

Cierto que se pierde mucho dinero pero comparándolo con qué. Desde el momento en que el mundo se mueve desde el entorno analógico al digital, el dinero también lo hace también ese nuevo entorno. Hoy tenemos menos atracos a oficinas bancarias y más atracos por transacciones vía web. Dentro de este proceso de transformación tecnológica que vive la sociedad hay que ser conscientes de que el dinero cada vez es más electrónico, y no hay que olvidar que la criminalidad se mueve hacia donde se mueve el dinero.

¿Damos por hecho que el entorno digital es inseguro?

Bueno, cada vez es más seguro. Se trata de hacer un recorrido hacia la madurez y, en estos momentos, existe una mayor sensibilidad hacia todo lo relacionado con la seguridad y todos los proveedores de tecnología son conscientes de que la seguridad debe estar presente en todas sus propuestas ya que se debe fortalecer el área de la gestión del riesgo tecnológico.

"La inversión en seguridad debería incrementarse dos puntos porcentuales"

Muchas veces nos acordamos de los riesgos cuando ya se ha finalizado el proyecto y esto es un problema. Es necesario tener en cuenta que la seguridad debe ir contemplada desde las primeras fases de análisis funcional de un proyecto, así como la obligatoriedad de realizar previamente un análisis de riesgos del proyecto. En resumen, creo que el reto está en que la seguridad vaya embebida, que sea algo así como una característica más de cualquier servicio.

¿La seguridad o la ciberseguridad podrían estar actuando como frenos hacia la transformación digital?

Sinceramente no creo que se así en ningún caso. La seguridad es un condicionante. No se puede entender que transformemos todo nuestro entorno y que a su vez no intentemos que sea más seguro.

Ciberterrorismo, Deep Web... ¿Es necesario este toque alarmista para que las empresas se conciencien?, ¿no puede llegar a ser paralizante?

Creo que esos mensajes alertan, no paralizan. Aun así, es cierto que en algunos casos deberíamos modular el mensaje. No hace falta asustar cuando el objetivo es concienciar, alertar y paralizar.

¿Es común entre la empresa española disponer de una política de seguridad global?

La seguridad tiene que ser parte de la agenda del board de una empresa, de la misma forma que lo están las TI, ya que estamos hablando de la gestión del riesgo del uso de la tecnología. Y sí, todas las empresas del IBEX35 y la mayoría de las grandes organizaciones españolas disponen

Perfil de "un docente por vocación"

Gianluca D'Antonio se define como "un experto en seguridad de la Información, apasionado por las nuevas tecnologías y analista de riesgos tecnológicos". Con 15 años de experiencia en la gestión de proyectos y equipos orientados al análisis y mitigación de riesgos de TI es "docente por vocación, analista por naturaleza" y un "impulsor convencido de equipos multidisciplinares".

Desde diciembre de 2005 D'Antonio es director de Seguridad de la Información en el Grupo FCC, empresa matriz de una de los principales grupos de servicios medioambientales europeos que opera en los sectores de Energía, Agua, Medioambiente, Infraestructura, Transporte y Cemento. Su misión, en estos años, ha consistido en crear la función desde cero, desarrollando la estrategia corporativa de gestión de riesgos de la información y tecnológicos.

Además, D'Antonio es miembro fundador y presidente de la Asociación Española para el Fomento de la Seguridad de la Información (www.ismsforum.es), organización sin ánimo de lucro, creada en enero de 2007 para fomentar la mejora de la seguridad de la información en España. ISMS Forum Spain, con casi 150 organizaciones y 850 profesionales asociados es hoy la asociación de referencia en España para la promoción de una cultura empresarial y ciudadana de Seguridad de la Información.

El experto forma parte también, desde 2010, del Comité de Expertos de la Agencia Europea para la Seguridad de las Redes y de la Información (ENISA). Y desde 2009 es miembro del Comité de Seguridad y Riesgos de Forrester Research. Por último, como miembro del Comité Internacional de Certificación del Cloud Security Alliance ha sido uno de los impulsores de la certificación CCSK para Cloud Computing.

"Es necesaria la existencia de una figura en la empresa que englobe la seguridad física y la lógica"

de una política de seguridad global. No disponer de ello supone asumir un alto riesgo y es absolutamente inconcebible.

Ahora mismo hay mucha oferta tecnológica en materia de seguridad. ¿Están cubiertos sus requerimientos como CISO de FCC?

Sí, en líneas generales. Depende mucho del ámbito al que nos estemos refiriendo. Aun así, es cierto que es necesario mejorar en gran medida la experiencia de usuario. Llevamos años queriendo abandonar las contraseñas y todavía no lo hemos logrado. Cierto es que hay muchos servicios basados en biometría que no se integran con todos los protocolos que rigen los sistemas legacy. Lo que yo demando como CISO de FCC es seguridad y robustez tecnológica.

Cierto, pero ¿esa tecnología sofisticada también es útil para los ciberdelincuentes?

Exacto y por eso no se puede bajar la guardia. No podemos mirar solo la eficiencia en costes. Las empresas demandan las soluciones smart y el cliente busca una experiencia de cliente cada vez mejor, y para ello debemos ser conscientes de que debemos elevar los niveles de seguridad en general y de los datos en particular.

Por último, ¿podría como presidente de ISMS Forum hacer una valoración de su aportación durante en el último año?

Por supuesto. Hemos llevado a cabo proyecto que son referenciales a nivel europeo. Muchas veces pienso que realmente no somos conscientes del esfuerzo que estamos haciendo en ISMS Forum y de los logros conseguidos. Por ejemplo, durante el pasado año hemos puesto en práctica los ciberejercicios en los participan más de 15 empresas del IBEX35 Mas de 15 empresas del IBEX35. CSO