ISMS Forum reúne un año más a los expertos del sector de la Seguridad de la Información para analizar en qué punto se encuentran las compañías en este fuego cruzado contra los ciberataques.

http://www.computing.es/seguridad/noticias/1097720002501/organizaciones-cierran-filas-contra-ciberamenazas.1.html

ISMS Forum ha celebrado su XIX Jornada Internacional de Seguridad en el Teatro Fernando de Rojas del Círculo de Bellas Artes de Madrid, donde se han congregado expertos, profesionales, instituciones y empresas del sector. El evento giró en torno a la Ciberseguridad y la protección de datos en un mundo hiperconectado, y distintos ponentes de compañías internacionales compartieron su experiencia y puntos de vista acerca de los riesgos y amenazas que presentan la automatización y la digitalización de procesos.

Enrique Sánchez de León, director general de APD, dio la bienvenida al acto destacando la importancia del diseño de un nuevo marco normativo europeo de protección de datos que, *"a pesar de que muchas compañías recelen de su aplicación, es un inversión que tendrá, indudablemente, un impacto positivo en el negocio"*. Gianluca D'Antonio, director de sistemas de información en FCC Group y miembro fundador de ISMS Forum, secundó la idea de Sánchez de León apuntando a la necesidad de compartir información para la generación de inteligencia en seguridad ya que, en éste ámbito, *"tanto el sector público como el privado debe colaborar en pos de la creación de un marco de protección que nos beneficie a todos"*.

El capital humano de las empresas juega un papel fundamental

Analizar el tipo de riesgo al que se expone tu empresa es indispensable para crear herramientas para enfrentarse a él. Por este motivo, Andy Purdy, Chief Security Officer de Huawei Rechnologies USA, ha incidido en *"conocer al detalle las debilidades de cada uno de los elementos que conforman nuestra empresa (producto, calidad, cantidad, proveedores…), antes de adoptar cualquier medida"*, de esta manera garantizamos que la tecnología adquirida nos protege realmente de las amenazas reales y *"no son inversiones en vano"*.
Para el análisis antes citado, se necesita la colaboración de todos los clientes internos de la compañía, ya que, como reivindicaron muchos de los ponentes, *"*la responsabilidad en ciberseguridad no recae únicamente en el CISO *de la empresa, sino en todos los empleados de*

la misma”. El capital humano de la compañía juega en este entorno un papel fundamental, por lo que hay que concienciar a los trabajadores *“no hablándoles tanto en términos tecnológicos, sino en términos de los beneficios para el negocio que pueden suponer aplicar los códigos de buenas prácticas”. "La confianza del cliente es la única que nos prmite crecer"*

“Hasta ahora la Seguridad era considerada un área casi independiente de la empresa, actualmente estamos empezando a ser conscientes de que debe ser una unidad integrada en el negocio”, afirmó Tim Grieveson, Chief Cyber Security Strategist en EMEA de HPE.
Con el desarrollo del cloud, Internet de las Cosas, el Big Data corporativo y demás procesos sistematizados, los usuarios han empezado a percibir Internet como un entorno inseguro, *“algo que las empresas no nos podemos permitir”,* sentenció Adenike Cosgrove, de Cybersecurity Stratregy en EMEA de Proofpoint.

De esta manera, normativas como ISO y GDPR, o la creación de un registro de proveedores de tecnología certificados, como se plantea en EEUU; resultan fundamentales para acercar la empresa al cliente mediante los múltiples canales existentes y que éste no tema por la fuga de sus datos. Los profesionales presentes coincidían en que, al fin y al cabo, *“la confianza del cliente en la compañía es la única que nos permite evolucionar, crecer y mantenernos en el mercado”.*