Nº 77 junio 2022

SECURITY FORUM 2022

Los días 1 y 2 se celebró en el Centro de Convenciones Internacional de Barcelona, el Security Forum 2022.

AES contó en esta ocasión como en las ediciones anteriores, con un stand, y además este año contribuyó en el Congreso. L**a digitalización de la seguridad** fue uno de los pilares sobre los que se apoyó el contenido del día 2 de junio en el congreso. La jornada comenzó con una mesa redonda en un formato «Diálogo con…» organizado por AES, que contó con las intervenciones de Andrés Martínez, Director de Seguridad de Banco Sabadell, y Julio López Moreno, CISO de CIB (Corporate and Investment Banking) del BBVA, que contestaron a las cuestiones planteadas por los moderadores Julio Pérez, Área de Seguridad Electrónica; Manuel Rodríguez, Área de Ciberseguridad; e Íñigo Ugalde, Área de Seguridad Física, de AES.

Los invitados hablaron de la importancia de la resiliencia de toda la cadena de suministros, de la certificación de las soluciones ofrecidas desde las compañías de seguridad y de cómo hay retos, como el teletrabajo, que se deben mejorar todavía más para garantizar la mayor seguridad de las empresas. También pusieron en la importancia del dato para tomar mejores decisiones empresariales y en la importancia de atraer talento digital, especialmente en el área de la ciberseguridad.

En este interesante diálogo, se abordaron los temas que están afectando a la digitalización de la seguridad privada, la pandemia, la guerra de Ucrania o el oursourcing bancario. Todos elementos que han resultado catalizadores en el cambio.

Además, se trataron asuntos tan importantes como la figura del Director de Seguridad como persona que aglutina la seguridad global, los problemas en la cadena de suministro, la gestión de los proveedores.

La etapa que vivimos en la actualidad ha puesto de relevancia la importancia de la resiliencia y de tener buenos planes de contingencia.

Consejos para nuestras empresas: la certificación como elemento fundamental para la calidad de productos y servicios, la transparencia, la monitorización de la seguridad o los planes de continuidad de los partner.

Otro de los temas que se abordó fue la Directiva NIS. Su fin fundamental, asegurar y dar coherencia a la seguridad en las redes. Ha puesto de manifiesto la importancia de la colaboración público-privada.

Se habló también sobre el libro blanco del CISO, y la forma en la que acompañará a todas las organizaciones.

El teletrabajo es un reto que ha venido para quedarse y que aumenta la posibilidad de los ciberataques. Para que funcione hay que trabajar en las siguientes áreas:

- Seguridad en la nube porque ahí se almacenan todos los activos.
- Contratación de talento.
- Concienciación de los empleados y clientes.
- Gestión de la cadena de suministro.

La geopolítica es otro de los factores que afectan a la digitalización de nuestra industria. El concepto de guerra híbrida, con actores muy bien financiados, cuando los atacados tienen límites económicos para poder defenderse. Los ataques, además, son destructivos, por lo que son más rápidos.

Sobre la legislación de seguridad privada, los entrevistados se mostraron conformes en que se necesitaba una nueva ley que aborde temas que la de 2014 no aborda.

Siendo cierto que la regulación condiciona a la transformación digital, también lo es que supone que todos los actores jueguen con las mismas reglas. Sin embargo, hay también mucho espacio de mejora, ya que falta armonización entre los reguladores y los gobiernos, falta agilidad. Falta regulación a las entidades que venden servicios bancarios y no son bancos, por ejemplo.

Como conclusiones, para frenar los ciberataques es importante:

- Tener una norma de ciberseguridad.
- Plan de contingencia.
- Probar todos los procedimientos anualmente y comprobar que funcionan correctamente.
- Ciberejercicios: testear a la alta dirección.
- Zero trust: modelo a aplicar.

Recomendaciones para adaptar la industria de la seguridad privada a la digitalización:

- Planes de contingencia
- Data driving, analítica de datos en la cadena de suministros. Supone un valor añadido.
- Ser preventivo, buena cooperación, información en inteligencia artificial.

Al final, como siempre decimos en AES, la seguridad no es un gasto, sino una inversión, y siempre resulta más barato invertir en seguridad que solucionar los problemas cuando ya se han producido.

Fotos cedidas por Ediciones Peldaño