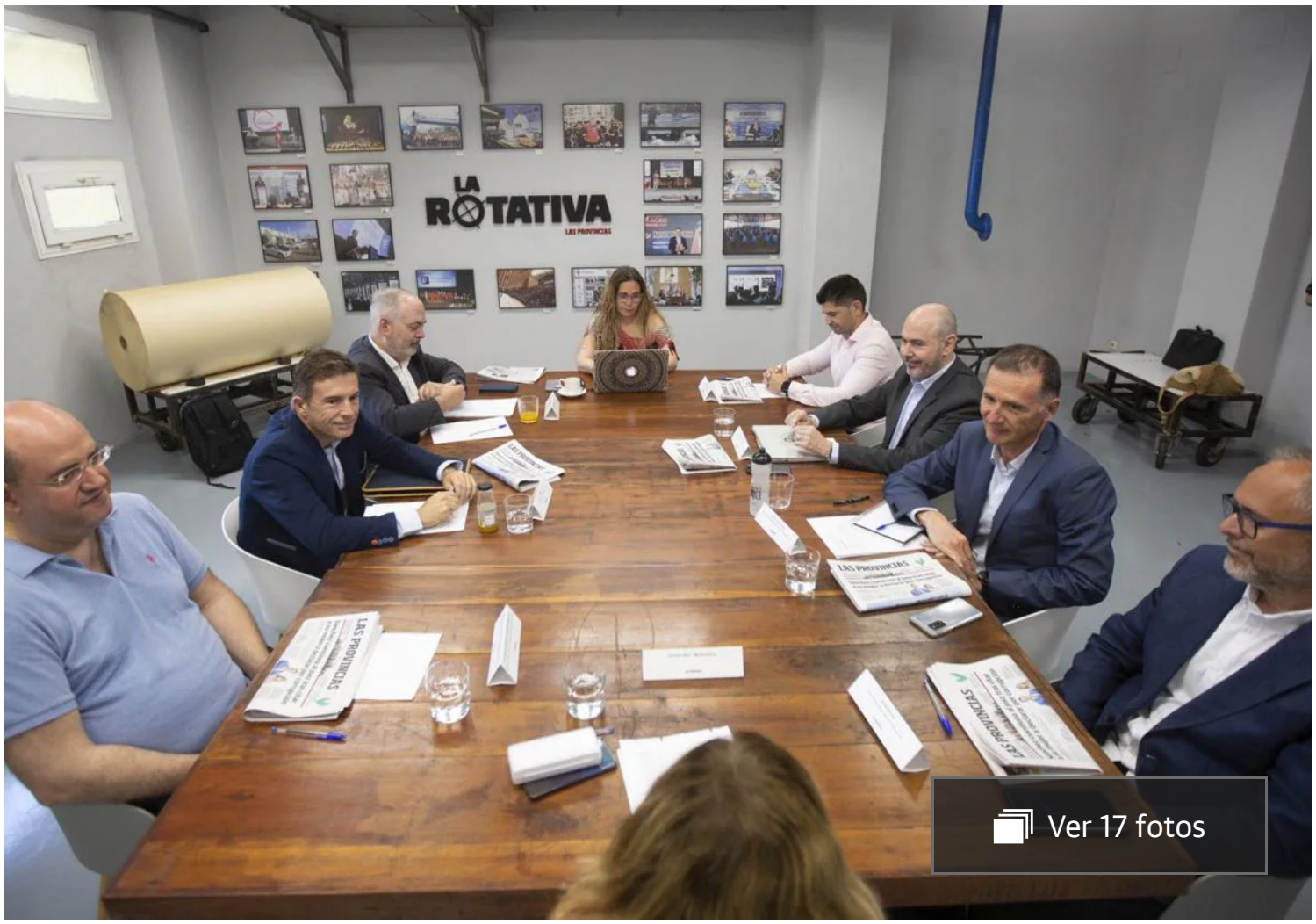
LAS PROVINCIAS

MESA DE EXPERTOS

«La identidad es el activo más importante a proteger por parte de empresas y particulares»

LAS PROVINCIAS organiza un encuentro con expertos en ciberseguridad para hablar de la situación actual en España y la Comunitat, así como de los retos de futuro que la IA y la tecnología pone sobre la mesa



Desayuno sobre Ciberseguridad

Sandra Paniagua

+ Seguir

Sábado, 8 de junio 2024, 00:48 | Actualizado 11:04h.

«Las cifras que mueve el cibercrimen son preocupantes. Debemos de tener en cuenta que, si hablamos en términos de PIB, el cibercrimen asciende al 1,5% del PIB mundial, es decir, sería la tercera potencia más importante del mundo. Actualmente, los ciberdelincuentes ya no son jóvenes que intentar acceder a archivos de organizaciones o burlar la seguridad de empresas o Estados, esta delincuencia digital es una industria bien organizada y, además, utiliza la última tecnología para ser más eficiente», señaló Manel García, responsable Comercial de la Zona Noreste en SIA, an Indra Company, al inicio de la mesa de expertos sobre ciberseguridad que organizó LAS PROVINCIAS. En el debate también estuvieron presentes: Germán Sánchez, consultor de ciberseguridad en Inforges; Daniel Rodríguez, director de Operaciones en Edgewatch; Santiago Escobar, director de la Cátedra de Ciberseguridad INCIBE-UPV; Carlos Estrela, director de Leader Redes y Comunicaciones; Marcelino García, consultor comercial en ciberseguridad de Sothis by Nunsys Group; y Benito Hernándiz, director general de Neotic.

Durante el encuentro, los ponentes hablaron sobre la situación actual de la ciberseguridad en España y en la Comunitat Valenciana, el uso de la Inteligencia Artificial tanto en los ataques que sufren las compañías y particulares como para la defensa de las mismas, así como la ciberseguridad de la IoT en la industria, la Directiva NIS2, la concienciación y la formación en este aspecto, la

falta de profesionales en el sector o la importancia de asegurar la cade... de suministro.

Desayuno sobre Ciberseguridad

La tecnología ha facilitado la vida tanto laboral como personal, pero también ha traído consigo una serie de riesgos que la sociedad todavía no tiene interiorizados. Estamos hablando del secuestro de datos, del robo de identidad, de la sustracción de documentos, de claves o contraseñas, incluso de estafas económicas... En definitiva, de diferentes tipologías de crímenes. Y es que los ciberataques se han convertido en uno de los mayores problemas de esta era tecnológica. De hecho, según datos de las Fuerzas y Cuerpos de Seguridad del Estado, si comparamos enero y febrero del 2024 con los dos primeros meses del año anterior, el cibercrimen ha aumentado en un 13,5%.

No obstante, del mismo modo que no se dejan las llaves de la casa puestas o la puerta abierta, las empresas y la sociedad en general puede y debe tomar precauciones para evitar estos delitos. Los ponentes señalaron que se ha avanzado mucho a lo largo de estos años en ciberseguridad, que cada vez se está más concienciado, aunque todavía queda mucho camino por recorrer y añadieron que los criminales van siempre por delante y, por ello, hay que invertir más en este sentido.

De hecho, según el reporte de Hiscox, se estima que, a lo largo del año pasado, la mitad de las empresas españolas sufrió algún tipo de ciberataque. Este mismo informe destacó el exponencial crecimiento de los ciberataques a pymes. Lo que convierte a este dato en preocupante, puesto que en España el tejido industrial está compuesto en un 98% por pymes, lo que hace que se encuentre en

el punto de mira de los ciberdelincuentes. Además, debido a su tamaño y facturación, las pymes son las que menor cantidad de su presupuesto dedican a estos menesteres.

No obstante, «la ciberseguridad debe entenderse como una inversión y no como un gasto por parte de los empresarios», estuvieron todos los ponentes de acuerdo en señalar, a la vez que Santiago Escobar explicaba que «actualmente, se están implantando una serie de normas que las empresas van a tener que cumplir, por lo que ya no es solo una cuestión de concienciación, ya que si no se cumple y la entidad sufre un ataque van a tener que asumir su responsabilidad».

A lo dicho, Carlos Estrela apuntó que «en muchas ocasiones las compañías no se dan cuenta de que han sido vulneradas, han sufrido un ataque o de que les han robado información. Solo cuando repercute en la fabricación, los balances no cuadran, o se hace público el espionaje industrial es cuando los ataques se hacen evidentes» y añadió que a todo esto se suma que «muchas veces las empresas no cuentan que han sufrido ataques por lo que, esa falta de información, también hace vulnerables a otras empresas del mismo sector, incluso de otros».

Los ponentes señalaron que compartir la información es fundamental para poder protegerse, ya que si se sabe qué método se está usando o las vías a través de las que están atacando, se puede tomar medidas para frenar nuevos ataques.

Al hilo de esto, Santiago Escobar explicó que «es cierto que puedes no enterarte nunca de que has sufrido un ataque, puesto que los ciberdelincuentes pueden tener como objetivo atacarte para llegar a otras empresas o bien por espionaje industrial. De hecho,