El grupo de hackers La Nueve, vinculado al colectivo Anonymous, atacó el sitio web de la escuela de negocios IESE por medio de una vulnerabilidad, según explican los mismos hackers.

Los piratas informáticos compartieron un enlace descubierto que alberga cientos de documentos con nombres, apellidos, correos electrónicos, usuarios y contraseñas de clientes de IESE, tanto de empresas como particulares.

> *«Trabajar con servidores bajo Windows XP y ASPNET es una osadía, mucho más si se almacenan en ellos 41.728.180 correos, 301.148 datos personales..»,* escribió el grupo en Twitter.

El enlace compartido por los hackers brindaba acceso a cualquier persona al contenido del servidor de IESE Publishing, distribuidor de material docente del IESE. Al acceder, el sistema no pedía ningún tipo de credencial, por lo que estaba totalmente desprotegido.

Una hora después de la publicación, el enlace fue removido de la red abierta. El directorio al que se podía acceder estaba bajo el nombre *«var»*.

Según La9, esta vulnerabilidad en más grave de lo que se creía en un principio, ya que afirman que *«hay 28 bases de datos Oracle expuestas, 23 desde el servidor que acaban de tirar».*

Esto podría significar que técnicos del IESE tratan de encontrar la fuente del fallo, pero todavía no han sido capaces de resguardar todos sus servidores.

> *«De momento, a estas horas, los agujeros de seguridad no se han resuelto, todos siguen el camino que les hemos enseñado», dicen los hackers a El Confidencial. «Hemos dado un index abierto y un pantallazo de una web de compras y todos han seguido esa linde, desde los más expertos hasta los más incipientes»,* dijeron a las

> 11:10 am del lunes 17.

Mientras tanto, IESE publicó un comunicado sobre lo sucedido:

> *«Los servidores web del IESE Business School están siendo víctima desde ayer por la noche de continuados ataques informáticos. Se ha producido un acceso no autorizado a datos de clientes. La página web IESE Publishing se ha visto afectada. El ataque ha alcanzado también al portal de conocimiento IESE Insight. Ambas páginas están ahora offline. Lamentamos profundamente este hecho, y estamos poniendo todos los medios para resolver el incidente en la mayor brevedad posible. En IESE conscientes de la importancia de salvaguardar los datos de nuestros clientes, alumnos, trabajadores y colaboradores externos y sentimos lo ocurrido. Estamos trabajando con expertos en ciber seguridad y estamos informando a todos nuestros antiguos alumnos y a los clientes de IESE Publishing»*.

Este fallo podría causar una investigación y sanción por parte de la Agencia Española de Protección de Datos (AEPD) si el IESE no justifica por qué gestionaba parte de sus servidores web con información delicada mediante software desfasado.

Luego de la entrada del famoso Reglamento General de Protección de Datos (RGPD), lanzado el pasado mes de mayo, muchas compañías están obligadas a nombrar a un delegado de protección de datos (DPO) para el control de todo lo relativo al almacenamiento y gestión de información personal de sus clientes y usuarios.

Esto se explica en el artículo 37 de la nueva normativa. Todos los organismos públicos, empresas que gestionen datos a gran escala y aquellas que traten datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas, el tratamiento de datos genéticos y biométricos, datos relativos a la salud y datos relativos a la vida sexual o a la orientación sexual de una persona física, son quieren deben acatar este reglamento.

Por su parte, el abogado especializado en Internet y privacidad, Carlos Sánchez-Almeida, afirma que en este caso, la normativa vigente a aplicar es el Real Decreto-ley 12/2018 de seguridad de las redes y sistemas de información.

Según los artículos 36 y siguientes, el fallo cometido por el IESE puede suponer una falta grave o muy grave.

> *«De momento lo que tiene que hacer la AEPD es iniciar la investigación de oficio. Si el IESE ha notificado el incidente, no tiene por qué haber sanción. Lo que estpa claro es que la normativa estaba en vigor en el momento del hackeo»,* explica el abogado.