Asociación de Internautas

Los datos personales "bajo llave" frente a ciberataques empresariales

Los datos personales "bajo llave" frente a ciberataques empresariales

Cuando se cumplen treinta años del Día Mundial de la Ciberseguridad, esta jornada que se celebra hoy como cada 30 de noviembre coincide con el despegue de un nuevo marco legal en Europa para asegurar la privacidad de los datos personales en caso de brechas de seguridad y ciberataques contra empresas.

EFEfuturo | Amaya Quincoces Riesco .-

Para concienciar a las empresas y las personas de los riesgos de los ciberataques ya en los prolegómenos del surgimiento de internet en 1988, la Association for Computing Machinery (ACM) institucionalizó el Día Mundial de la Ciberseguridad o de la Protección Informática del que se conmemora hoy su trigésimo aniversario.

Desde esa fecha, la tendencia a lo digital ha sido imparable, con la popularización del correo electrónico tras la aparición de la red de redes o el actual “boom” del “internet de las cosas” y los avanzados desarrollos en inteligencia artificial y aprendizaje automático de máquinas conectadas a “la nube” tecnológica.

En paralelo, las ciberamenazas también han aumentado progresivamente, con cifras que de hecho, se disparan año tras año, con ataques cada vez más sofisticados y lucrativos contra todo tipo de organizaciones, coinciden los expertos consultados por Efefuturo.

Un nuevo marco legal sobre privacidad

El reglamento europeo sobre privacidad vigente desde el 25 de mayo ha dado un gran paso en su objetivo de proteger la intimidad del ciudadano al castigar con multas millonarias a las empresas que no custodien correctamente el uso de datos personales de sus usuarios.

No obstante, esa normativa contiene un inherente “efecto perverso” al favorecer indirectamente al cibercriminal, que ahora tendrá “una nueva fuente de ingresos” si chantajea a la víctima cuyos equipos infecta porque la podrá denunciar por brecha de seguridad, advierte el director general de Check Point Iberia, Mario García.

Según sus datos, el 87 por ciento de las empresas no están todavía protegidas frente a ciberamenazas avanzadas aunque cada vez adoptan más medidas para hacerlo, y más del 96 por ciento de las organizaciones carece de sistemas de seguridad frente a ataques a sus móviles, mientras que en el caso de los usuarios de a pie las cifras son mucho peores, advierte el responsable de Check Point.

Por su parte el ingeniero experto en ciberseguridad Deepak Daswani, autor del reciente libro “La amenaza hacker”, publicado por Deusto, del grupo Planeta, advierte de que cualquier vulnerabilidad puede ser aprovechada por un cibercriminal para acceder a los sistemas de una organización y sustraerle información confidencial o bloquearle los equipos, porque existen “muchísimos vectores de ataque”.

Daswani advierte de que, lamentablemente todavía existen empresas que no tratan correctamente la información personal que manejan incluso la de carácter más “sensible” e insta a que “se pongan las pilas” cuanto antes para garantizar la privacidad de los usuarios.

Desde la Asociación de Internautas, su presidente, Víctor Domingo, advierte de que la seguridad informática a nivel de usuario es “una de las asignaturas pendientes para el desarrollo de la Sociedad de la Información”, porque éste debe aprender también a protegerse y gestionar correctamente sus propias claves.

Más de 400 notificaciones de brechas de seguridad

Desde la entrada en vigor en mayo del nuevo reglamento europeo sobre privacidad, **un total de 418 notificaciones de brechas de seguridad de organizaciones** han llegado a manos de la Agencia Española de Protección de Datos (AEPD); de ellas, sólo 11 han pasado a la subdirección de Inspección, por requerir una investigación adicional, según los datos facilitados a Efe.

Previamente a esta normativa, la notificación de este tipo de incidentes -que causan destrucción, pérdida o variaciones de los datos personales- debe manifestarse a la autoridad competente que en el caso español es la AEPD y la obligación de comunicarlos hasta la entrada en vigor del reglamento se ceñía casi exclusivamente a los operadores de servicios de comunicaciones electrónicas.

De hecho, en el período del año pasado desde el 25 de mayo hasta el primero de diciembre, fueron solo cuatro las notificaciones por quiebras de seguridad, según la AEPD.

La nueva normativa europea exige a las empresas que gestionan información personal comunicar el suceso en un máximo de 72 horas desde que sea conocido salvo si fuera improbable que la brecha de seguridad supone riesgo para los derechos y libertades de las personas físicas.

Además el responsable del tratamiento de datos debe informar a los afectados con lenguaje claro y sencillo y de forma concisa y transparente en caso de que el incidente entrañe alto riesgo para los derechos y libertades de las personas, por ejemplo en caso de acceso ilícito a datos de usuarios y contraseñas de un servicio.EFEfuturo

---