Publicado en Madrid el 05/01/2021

Crecen un 23% las brechas de seguridad por el auge del teletrabajo en 2020

El aumento de la transferencia de datos durante el Covid-19, detrás de uno de los ciberataques más frecuentes en el último año, capaz de ocasionar "la destrucción total o parcial" de información sensible para empresas y usuarios, según los analistas de LIFe

Los incidentes y brechas de seguridad se han disparado un 23% en el último año, como consecuencia de los efectos de la pandemia del Covid-19 en el teletrabajo y la movilidad de los datos, según el informe Estado actual de la seguridad de los datos móviles corporativos en España de Kingston. Se estima que casi 1 de cada 10 empresas (el 7%) ha recibido este ciberataque en cinco ocasiones o más.

Alrededor de 19 millones de españoles teletrabajaron en 2019, según Randstad, y esta modalidad de empleo ha incrementado su popularidad a raíz de la crisis sanitaria del coronavirus, cuyo impacto ha comprometido 3.300 millones de empleos en todo el mundo, de acuerdo a la Organización Internacional del Trabajo (OIT).

El repunte del teletrabajo ha provocado un aumento paralelo en las brechas de seguridad, definidas por el Laboratorio de Informática Forense europeo (LIFe) como "un incidente se seguridad que afecta a datos de carácter personal". Con independencia de su origen "accidental o intencionado", pueden ocasionar "la destrucción total o parcial, perdida, alteración, comunicación o acceso no autorizado a los datos antes mencionados".

Para este laboratorio fundado en 2010, especializado en la prestación de servicios de ciberseguridad y asesoramiento jurídico, la adecuada gestión de brechas de seguridad destaca por la inmediatez de su respuesta a la amenaza, obligada por el Reglamento (UE) 2016/679 de Protección de Datos. "El plazo para la notificación a la Autoridad de Control de Protección de Datos será de 72 horas desde que la organización tiene conocimiento de esta brecha de seguridad", señalan desde LIFe.

La gestión de este incidente debe contemplar, a su vez, el daño infligido a terceros, pues "dictamina dicho Reglamento que si la brecha de seguridad ha ocasionado daños graves tiene que comunicar la organización dicha brecha de seguridad a los interesados de dichos datos", explican los expertos de este laboratorio de informática forense con sede en Madrid.

Las brechas de seguridad, como cualquier otro delito, dejan un rastro, una huella visible. De su análisis e investigación dependen no sólo que no se vuelva a producir, sino que las autoridades competentes sean informadas del suceso en detalle y con arreglo a la legislación.

"Para ello se deberá recabar información", apuntan desde LIFe, y el punto de partido son los medios

que han posibilitado este incidente. "Los medios son variados y múltiples: robo/perdida de un dispositivo con información, se ha compartido conscientemente o por error datos de carácter personal, un virus ha cifrado toda nuestra información de los ordenadores y/o servidores, alguien de la organización ha caído en una trapa de suplantación de la identidad, etcétera".

Los expertos de LIFe también proceden, durante la investigación de la brecha informática, a identificar el origen de la misma, así como la intencionalidad. El estudio de las víctimas (clientes, empleados, alumnos, etc.) aportan una valiosa información, así como reconocer "si los datos afectados son básicos o son datos especialmente protegidos".

Estos datos se recaban con la doble finalidad de informar a la Agencia Española de Protección de Datos (AEPD) y de blindar la propia seguridad con miras al futuro. Desde el laboratorio de informática LIFe recomiendan, en este sentido, la adopción de "nuevas medidas técnicas y organizativas", a fin de que "no vuelva a ocurrir la brecha de seguridad".

Acerca de LIFe
LIFe es un laboratorio de informática y telecomunicaciones forense especializado en análisis forense, asesoramiento técnico y jurídico, recuperación de datos, brechas de seguridad y peritación de correo electrónico y otros servicios informáticos, mediante un riguroso proceso de identificación, testeo y prototipación de ideas susceptibles de proporcionar una ventaja diferencial.

Datos de contacto:
LIFe (Laboratorio de Seguridad Telemática S.L.)
Tfno: Website: https://www.laboratoriodeinformaticaforense.com Dirección: Calle Cruz Verde, 5. 36202 - Vigo
(+34) 910 600 599

Nota de prensa publicada en: Madrid

Categorías: Ciberseguridad