Después de un año con el Reglamento de protección de datos, ¿qué cambió?

La sanción más cuantiosa por la nueva normativa europea hasta la fecha ha sido la que impuso Francia a Google de 50 millones de euros por falta de consentimiento en sus anuncios

Giridhara Raam
Marketing Analyst en ManageEngine

Las empresas están formadas por diferentes departamentos y profesionales con múltiples intercambios de datos que fluyen a través de la organización. Cuando hay una fuga de datos los agentes de protección de datos (OPD), los CIO y CISO son los que se llevan la culpa generalmente. Sin embargo, desde la introducción del Reglamento de Protección de Datos (GDPR), la responsabilidad se ha repartido más equitativamente con todo el personal de la organización. El GDPR ha traído un planteamiento unificado sobre la gestión de la seguridad de los datos lo que ha aumentado la concienciación entre los interesados de todas las organizaciones.

El GDPR entró en vigor el 25 de mayo de 2018, introduciendo así más seguridad a los datos personales de los ciudadanos de la UE. Aunque esta legislación europea de protección de datos ha traído una mayor seguridad a los usuarios, también ha dejado a muchas empresas con dificultades para modificar sus procedimientos de manejo de datos personales. Las empresas de todo el mundo han redefinido sus estrategias de gestión para hacerse compatibles con el GDPR con el fin de evitar las enormes multas impuestas debido a negligencias en la protección.

Sin embargo, el número de ataques cibernéticos y las violaciones de datos no han disminuido a pesar de los procedimientos más estrictos sobre su manipulación. Ha pasado un año desde la entrada en vigor del GDPR pero todavía hay una gran cantidad de cosas que hay que mejorar en lo que respecta a la gestión de los datos personales.

El GDPR trajo grandes cambios en las organizaciones en cuanto a la recogida de datos, su almacenamiento, procesamiento y procedimientos de eliminación; he aquí los hechos más relevantes ocurridos tras su introducción

- Las autoridades de protección de datos de la UE han registrado un gran número de quejas desde el 25 de mayo de 2018. En el primer mes, había más de 10.000 quejas, y el número de quejas creció hasta 60.000 en los próximos seis meses, con el tiempo la cifra ascendió a 95,180 quejas en enero de 2019. Todas estas quejas fueron presentadas por las personas que sentían que no se habían respetado sus derechos bajo la GDPR.
- La mayor parte de las quejas relacionadas con el cumplimiento GDPR se han dirigido al *telemarketing*, *e-mails* promocionales, y la videovigilancia.

● Sobre la base de las normas de violación de datos, si las organizaciones experimentan una brecha de datos necesitan informar de ello a las autoridades de protección de datos dentro de un periodo 72 horas. Debido a esto, las autoridades de protección de datos de la UE recibieron 41,502 denuncias de violaciones de datos hasta enero de 2019, 5000 de las cuales en junio de 2018.

● Desde mayo de 2018 se han registrado 255 casos transfronterizos iniciados por las autoridades nacionales y las juntas europeas responsables de la protección de los datos de los ciudadanos.

● Hay varios casos activos contra las empresas que no cumplen los requisitos del GDPR que podrían recibir multas de hasta un 4 por ciento de la facturación anual de la empresa infractora de acuerdo con las estipulaciones GDPR. Cinco multas de gran repercusión han sido emitidas por el incumplimiento de la ley desde abril de 2019. La sanción más cuantiosa hasta la fecha ha sido la de Francia a Google de 50 millones de euros por falta de consentimiento en sus anuncios. También una empresa de taxis en Dinamarca recibió una multa de 1,2 millones de coronas danesas por no borrar la información de sus clientes.

● El GDPR es directamente aplicable a todos los países de la UE; en abril de 2019, 23 Estados miembros han adoptado GDPR- todos los países miembros de la UE, aparte de Bulgaria, Grecia, Eslovenia, Portugal y la República Checa.

● Con más de 300.000 menciones en los medios de comunicación en 2018, el GDPR ha recibido aún más cobertura que Mark Zuckerberg.

● En mayo de 2018, el GDPR estaba en la parte superior de Google Trends, mucho mayor que cualquier famoso de Hollywood.

Sobre la base de los informes de la Comisión Europea hasta diciembre de 2018 más del 50 por ciento de las organizaciones reguladas aún no se han adaptado al GDPR.

Las organizaciones necesitan adaptarse utilizando una vieja fórmula: redefinir su estrategia de seguridad, la identificación de su entrada de datos y puntos de salida, así como la determinación de la localización de su almacenamiento de datos y los procedimientos de gestión. Cómo es de esperar esto requiere una gran cantidad de tiempo, recursos y trabajo. Sin embargo, con las herramientas adecuadas de gestión de seguridad de datos, esta estrategia global se puede simplificar, proporcionando una mejor visibilidad y la seguridad de los datos personales de los usuarios.

¿Cómo deberían las empresas adaptarse al cumplimiento del GDPR antes de que sea demasiado tarde? Las empresas tienen que identificar las estrategias de seguridad de datos adecuadas para poner en marcha su cumplimiento con el GDPR. CIO y CISO deben identificar estas estrategias mediante el nombramiento de oficiales responsables de la protección de datos para cuidar de los datos de la organización y mejorar su seguridad frente a ataques cibernéticos. Las empresas que ya están en camino de cumplir con el GDPR tienen que comprobar si serán capaces de mantener su cumplimiento a largo plazo.

ISTOCK

Las empresas que aún no han puesto en marcha sus procedimientos de seguridad de datos tienen que seguir los siguientes pasos para no quedarse atrás: identificar cómo existe un dato dentro de la red en varios puntos diferentes como el punto de entrada, cual es la finalidad de la recogida de datos, el procesamiento de los datos, y la localización del almacenamiento y la duración en dicho lugar y los puntos de salida.

Las compañías serían capaces de adaptarse sin problemas mediante la utilización de *software,* soluciones de administración o gestión de datos adecuados, ya que estas herramientas pueden proporcionar una perspectiva crítica sobre los datos de la organización.