3M | The experts in screen privacy.

Preparación en el RGPD
Preguntas y respuestas

Enza Iannopollo, Forrester Research

Enza es analista en el equipo de Seguridad y Riesgo y Profesional Certificada en Privacidad de la Información - Europa (CIPP/E). En Forrester, se encarga de la protección de datos, la privacidad, la analítica de datos y el Internet de las cosas, con un enfoque en el impacto de las normativas y las tecnologías que los sustentan.

El RGPD es uno de los cambios más importantes en reglamentos sobre políticas de privacidad en los últimos 20 años. Establece cómo las organizaciones deben tratar los datos personales de sus clientes, empleados y socios empresariales de manera continua. Recientemente, 3M se reunió con Enza Iannopollo de Forrester Research para analizar las medidas de seguridad, las políticas y los programas sobre cumplimiento de la privacidad que muchas organizaciones están implementando para cumplir con normativas como el RGPD. Enza nos ofreció información esclarecedora sobre la preparación del lugar de trabajo e hizo hincapié en la necesidad de contar con mecanismos de seguridad física para protegernos contra amenazas a la privacidad de los datos.

¿Qué está en juego?

Las organizaciones pueden recibir sanciones de hasta un 4 % del volumen de negocios anual global o

20 M € FINE

Esto fue los que nos dijo:

P. ¿Están los empleados preparados para cumplir el RGPD?

R. Nuestras cifras muestran que solo una de cada tres empresas en todo el mundo está preparada para cumplir el Reglamento General de Protección de Datos (RGPD). Puesto que el RGPD entrará en vigor el 25 de mayo de 2018, está claro que muchas organizaciones necesitan actuar con rapidez para ultimar sus preparativos.

En particular, estamos viendo que algunas firmas tienen problemas a la hora de cumplir el requisito de implementar y documentar formación en privacidad y programas de sensibilización para los empleados. Los reguladores de la UE han indicado que dichos programas son esenciales para el cumplimiento del RGPD. En cambio, hemos observado que las organizaciones que cumplen este requisito han mejorado su cultura de privacidad corporativa y establecido mejores prácticas que, a veces, superan los requisitos normativos.

P. ¿Las empresas de algunas regiones están más preparadas que otras?

R. Un 34 % de empresas estadounidenses afirma estar preparado frente a un 26 % de empresas europeas.[1] Las empresas que no cumplan el RGPD, tanto de manera consciente como si no, están cargando sobre sus espaldas un gran riesgo comercial. Aquellas empresas que consideran que están preparadas pero no lo están, están tomando un riesgo todavía mayor.

Es interesante observar que existen más empresas en EE. UU. que se consideran preparadas en comparación con Europa. Esto tiene que ver con el efecto extraterritorial del RGPD. La normativa se aplica a todas las empresas, independientemente de su ubicación, que tratan o mantienen datos personales de residentes de la Unión Europea. Esto quiere decir que no solo se les exigirá a las empresas europeas que cumplan estas severas normas de privacidad, sino también a muchas empresas con sede en EE. UU.

Sospechamos que una lectura superficial de las normas combinada con expectativas erróneas e injustificadas de una débil ejecución del RGPD podrían estar poniendo en entredicho la percepción de las empresas sobre su preparación.

P. ¿Qué mecanismos de seguridad física y de la privacidad exige el RGPD?

R. El RGPD es una normativa basada en principios. Esto significa que los reguladores no proporcionan a las organizaciones una serie de acciones definitivas a seguir. En cambio, las organizaciones deberían pensar en los requisitos del RGPD como una especie de «estado deseado» para sus prácticas de tratamiento de los datos. Además, quiere decir que las organizaciones deben identificar y evaluar riesgos específicos que necesitan mitigar para cumplir los requisitos del RGPD.

A la hora de identificar riesgos, las empresas deben tener en cuenta aquellos que presenta el tratamiento de los datos, en particular, como consecuencia de la pérdida accidental o ilícita de datos personales transmitidos, almacenados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. No importa si una divulgación no autorizada de los datos tiene lugar debido a un ciberataque sofisticado por parte de un pirata informático al sitio web de una empresa o a que un extraño haga una foto de datos altamente confidenciales mostrados en la pantalla del portátil de un empleado. Ambos constituyen riesgos igualmente graves y necesitan estrategias de mitigación apropiadas.

P. ¿Constituye un riesgo el pirateo visual?

R. Totalmente. Solo hay que recordar esto: para muchas organizaciones, las llaves del reino son un nombre de usuario y una contraseña. Basta con que una persona no autorizada le eche un vistazo rápido a una pantalla desprotegida para conseguir dichas claves y obtener acceso. El riesgo aumenta con la creciente complejidad de la ingeniería social.

Hace un año, un periodista fue pirateado mientras trabajaba en un avión.[2] El pirata en cuestión pudo describir detalles sobre el artículo que el periodista estaba escribiendo, correos electrónicos personales que había enviado y próximas reuniones de trabajo, información que dijo haber captado al piratear la wifi del avión. O, quizás, el pirata simplemente lo averiguó mirando la pantalla del portátil del periodista. El periodista estaba indignado, pero captó el mensaje: mientras estaba trabajando en un artículo confidencial, en este caso, analizando minuciosamente las profundas y amplias repercusiones para la privacidad a las que se enfrentaba Apple con su negativa a la petición del FBI de descifrar el teléfono de un terrorista, olvidó proteger la privacidad y la propiedad intelectual en su propio dispositivo. Al igual que ese periodista, muchas organizaciones cometen el mismo error de subestimar los riesgos de la piratería cibernética y visual.

P. ¿Cuáles son los beneficios de implementar mecanismos de seguridad física de baja tecnología?

R. Debido a la proliferación constante de noticias sobre violaciones de datos a gran escala, es fácil olvidar que los negocios digitales de hoy en día aún tienen que hacer frente a retos de seguridad física. Los beneficios de implementar mecanismos de seguridad física, como videocámaras de vigilancia, cierres en maletines para portátiles y filtros de privacidad para monitores, portátiles, tabletas y smartphones, son abundantes. Los filtros de privacidad, por ejemplo, proporcionan una sólida estrategia de mitigación frente a violaciones de privacidad y de datos. Basta con que los datos confidenciales de un cliente o un empleado se expongan a la persona equivocada para que se produzca una violación de datos potencialmente muy perjudicial (y de gran difusión).

Esta tecnología también puede servir de apoyo para el cumplimiento de otras normativas distintas al RGPD. Por ejemplo, hace unos años se despidió a una auxiliar médica de un hospital de la Universidad de Iowa por infringir las normas de privacidad de los datos de pacientes. La acusaron de pirateo visual a un compañero cuando este estaba examinando el historial médico de un paciente, algo que constituye una violación de la Norma de Seguridad de la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA).[3]

Los mecanismos de seguridad física, como los filtros de seguridad, pueden funcionar como recordatorio visual para los empleados de que las mejores prácticas de seguridad y privacidad son prioridades para la organización. Y, como siempre ocurre con la privacidad visual, no se trata solo de observar los requisitos de cumplimiento, sino de proteger los activos más valiosos que tiene una empresa.

P. ¿Cómo pueden las empresas aprovechar la privacidad para lograr una experiencia superior para los clientes?

R. Las empresas que están ejecutando sólidos programas en torno al RGPD y la privacidad están experimentando una serie de beneficios empresariales que van más allá del cumplimiento. Uno de ellos es ofrecer una experiencia superior para los clientes. La manera en la que una organización protege los datos de sus clientes puede tener repercusiones directas a la hora de generar —o destruir— el sentimiento subyacente de confianza que sus clientes han puesto en ella.

Por ejemplo, sabemos que los clientes se pasan a la competencia como resultado de una violación de la privacidad.[4] Aún más, nuestra investigación sobre las actitudes de los consumidores respecto a la privacidad resalta que un 30 % de individuos se rehúsa a completar una transacción online si lee algo que no le gusta en el aviso sobre privacidad de la empresa.[5]

Si está comprometido a proteger los datos de sus clientes y sus empleados reconocen y reflejan este compromiso en sus interacciones con los clientes, esto puede diferenciarle de la competencia.

P. ¿Hay alguna empresa que destaque por su compromiso con la privacidad y la seguridad?

R. La privacidad ha pasado de ser un tema especializado para departamentos jurídicos a convertirse en un valor esencial para muchas organizaciones. Hoy en día, responsables de seguridad de información y directores de marketing se encuentran entre los ejecutivos que, entre sus máximas prioridades, sitúan proteger los activos de datos contra ataques y el uso indebido. De nuestra investigación se desprendió que un 23 % de las empresas del Fortune 100 ha adoptado la privacidad como parte de sus esfuerzos de responsabilidad social corporativa (RSC).[6] Alrededor de un 70 % incluyó la seguridad en sus informes sobre RSC.

Un 23 % de las empresas del Fortune 100 ha adoptado la privacidad como parte de sus esfuerzos de responsabilidad social empresarial (RSE).

Asimismo, observamos que las empresas comprometidas con la privacidad y la seguridad se benefician del hecho de ser abiertas y transparentes en cuanto al modo en el que tratan los datos personales. Esto puede ser un método muy valioso para brindar seguridad a los clientes, empleados y socios empresariales por igual. No obstante, operar de conformidad con este compromiso no es tarea fácil. A menudo, las organizaciones deben cambiar la manera en la que trabajan para lograr que estos compromisos cobren vida y establecer una cultura corporativa que reconozca la privacidad y la seguridad como valores esenciales.

P. ¿Se están elaborando más normativas como el RGPD?

R. Sin duda: el RGPD indica una tendencia. Hace poco concluimos un nuevo estudio que analiza las normativas y prácticas sobre privacidad de 54 países.[7] Está claro que regiones como Asia-Pacífico consideran al RGPD como la posible evolución de las normas locales sobre privacidad. En Latinoamérica y Rusia, también se están incorporando elementos del RGPD, como la ubicación de los datos, a las normas sobre privacidad de los datos. Por último, el Parlamento Europeo está trabajando en la actualización de los requisitos de la Directiva sobre la Privacidad Electrónica actual. Aún es necesario concretar los detalles, pero la idea es equiparar los requisitos de la privacidad electrónica al RGPD.

3M es una marca registrada de 3M Company. ©3M 2017. Reservados todos los derechos.

[1]Forrester Business Technographics Security Survey, 2017
[2]Digital Trends, Apple vs FBI shown in different light as journalist hacked mid-flight, 25 de enero de 2016
[3]Veriphyr, Medical Assistant Fired for “Shoulder Surfing” and Breaching Patient Data Privacy, 2011
[4]Ponemon Institute, The Impact of Data Breaches on Reputation and Share Value, mayo de 2017
[5]Encuesta online europea de referencia de Consumer Technographics de Forrester Research (parte 2), 2016
[6]Informe de Forrester, The Future of Data Security and Privacy: Growth And Competitive Differentiation, 2017
[7]Forrester, Interactive Data Privacy Heat Map, 2017

FORRESTER®