Privacidad desde una perspectiva internacional: Riesgos

En el post anterior hemos obtenido una visión global de la situación empresarial en el ámbito de la privacidad, tanto Europea como Estadounidense. A pesar de que todo parece estar bastante bien regulado, siempre existen riesgos en el tratamiento de datos personales. Por eso hoy hablaremos sobre estos riesgos.

La mayoría de empresas cuentan con el documento de privacidad, que como ya hemos comentado anteriormente, recoge las políticas de esta empresa en lo referente a tratamiento de datos personales. A pesar de que a través de este documento la empresa en cuestión nos prometa ciertas garantías pueden existir brechas de seguridad y otros diversos problemas, ya que los datos personales son un tipo de información muy valiosa y delicada, y por ello es necesario ser consciente de los riesgos que su manipulación implica. Muchos de estos riesgos suceden en entornos web en los que el usuario es preguntado por ciertos datos, por ejemplo la información de facturación y envío cuando realizamos una compra online. En la siguiente tabla [1] se recogen algunos de los más importantes que se dan en este tipo de entornos:

Título	Frecuencia	Impacto	Descripción
Vulnerabilidades de aplicación web	Alta	Muy alto	Las vulnerabilidades son un problema clave en cualquier sistema que resguarde y opere con datos sensibles para el usuario. Realizar un diseño e implementación inadecuados o detectar un problema y aplicar un parche de forma abrupta son situaciones propensas a tener brechas de seguridad.
Filtración de datos por parte del operador	Alta	Muy alto	Fallar en la prevención de la filtración de cualquier información que contenga o esté relacionado con datos de usuario, a cualquier entidad no autorizada resulta en una pérdida de datos confidenciales. Esto puede ser causado por una gestión de accesos inadecuada, almacenamiento inseguro, duplicación de datos o falta de conciencia.
Respuesta insuficiente ante una brecha de datos	Alta	Muy alto	Puede suceder cuando no se informa a los propietarios de los datos sobre la posible brecha o filtración, cuando no se consigue solucionar un problema relacionado con este tipo de datos o cuando no se limita la información filtrada.

Borrado insuficiente de datos personales	Muy alta	Alto	Esto ocurre cuando no se borran los datos correctamente, o en un cierto tiempo después de finalizar el propósito para el cual han sido recogidos o tras una petición.
Políticas, Términos y condiciones no transparentes	Muy alta	Alto	Esto sucede cuando no se provee suficiente información acerca de cómo se procesan y son tratados los datos, así como su recolección y almacenamiento. No hacer esta información accesible y entendible para personas sin conocimientos legislativos también es motivo de que esto suceda.
Recolección de datos innecesaria para el propósito primario.	Muy alta	Alto	Recolectar datos descriptivos, demográficos o cualquier otro tipo de datos innecesarios para los propósitos del sistema. Esto también se aplica a los datos recogidos sin consentimiento previo del propietario.
Compartición de datos con entidades de terceros	Alta	Alto	Proveer datos de usuarios a una entidad externa sin obtener el consentimiento del usuario. También puede deberse a una compartición de resultados por una transferencia o por un intercambio en forma de compensación monetaria o por uso inadecuado de recursos de entidades externas en sitio web.
Desactualización de datos personales	Alta	Muy alto	El uso de datos de usuario desactualizados, incorrectos o fraudulentos. También existe este riesgo cuando se falla al actualizar o corregir estos datos.
Expiración de sesiones insuficiente o inexistente	Media	Muy alto	Incumplimiento de la terminación de sesiones efectiva. Esto puede resultar en la recolección de datos de usuario adicionales sin su consentimiento o consciencia.
Transferencia de datos insegura	Media	Muy alta	Sucede cuando se realizan transferencia de datos a través de canales inseguros o sin ningún tipo de encriptación, excluyendo de esta forma la filtración de datos. Esto también incluye no promocionar los mecanismos que limitan la superficie de filtración.

Los riesgos citados están muy orientados a los entornos web, aunque también existen algunos riesgos algo más generales [2] que pueden darse en otro tipo de ámbitos.

- **Riesgo de incumplimiento:** descubrir un caso de incumplimiento a través de una auditoría, una investigación o una evaluación de riesgos necesita cambios en las prácticas de negocio.
- **Riesgo contractual:** el hecho de que una empresa no cumpla con sus obligaciones de privacidad especificadas supone una gran riesgo para cualquier entidad, y sobre todo para las personas encargadas del tratamiento de datos dentro de esa entidad.
- **Riesgo para el propietario de los datos:** el uso inadecuada de la información personal de una persona puede derivar en un gran daño en forma de pérdida de capital, otro tipo de pérdidas financieras, daño a su reputación, discriminación y otros muchos.
- **Riesgo ético:** en algunos casos las organizaciones tratan los datos de de forma correcta técnicamente, pero aun así puede considerarse un proceso no ético. En algunas jurisdicciones, la mayoría de leyes y regulaciones referentes a la privacidad y protección de los datos no han sido escritos contemplando las prácticas de negocio modernas y los avances tecnológicos, por lo que no tienen en cuenta los problemas de privacidad que han surgido a raíz de este desarrollo tecnológico. Por este motivo este riesgo se debe de tener en especial consideración en áreas como Big Data, Internet of Things y Cloud Computing.
- **Riesgo de demostración de responsabilidad:** se espera de las empresas el uso responsable de la información, pero además de serlo las empresas han de demostrar al resto del mundo que su gestión de la privacidad es efectiva. Si una empresa no es capaz de demostrar esto se encuentra en una situación delicada.
- **Riesgo de imagen y reputación:** una mala gestión de la privacidad puede derivar en daños irreparables para la imagen de una empresa, y si esto sucede, dicha empresa no podrá tener éxito, ya que no será deseado contratar sus servicios.

Tras analizar posibles riesgos que existen en este entorno, deducimos que es necesario una fuerte regulación para prevenir que estos riesgos se conviertan en realidad. Esto se realiza a través de la auditoría de privacidad, por lo que este será el siguiente tema a tratar.

Referencias:

[1] <<OWASP Top 10 Privacy Risks Project>>, Owasp, acceso el 28 de noviembre del 2017, https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project#tab=Top_10_Privacy_Risks_2

[2] <<Privacy Risk>> Nymity, acceso el 28 de noviembre del 2017, https://www.nymity.com/products/Privacy-risk.aspx