Ciudad de México a 29 Abril de 2016

Lecciones del #INEleaks:
¿si su empresa hubiera sido responsable de una fuga de datos?

Autor: Mtro. Rodrigo Orenday Serratos

Desde la semana pasada los medios no paran con notas sobre el hallazgo en los servicios de nube de Amazon de una copia de la Lista Nominal del Padrón Electoral sin salvaguardas de seguridad técnica: los datos de las credenciales para votar de todos los ciudadanos mexicanos registrados libremente accesibles para todo aquél que diese con ellos.

Con el transcurso de los días se fue dando a conocer que el origen de ese repositorio de información no había sido un ataque cibernético contra el Instituto Nacional Electoral, sino que la base de datos provenía de una de las copias que la autoridad electoral está obligada por ley a entregar a los partidos políticos. Más tarde trascendió que esa copia fue una de las entregadas en febrero del 2015 al partido político Movimiento Ciudadano. Éste salió rápidamente a medios para afirmar que había almacenado esa copia en la nube para prescindir de la que habían recibido en medios magnéticos, y que su almacenamiento en Amazon habría sido atacado por *hackers*, dejando expuesta esa información.

Mientras las autoridades electorales y penales investigan e imputan responsabilidades viene al caso preguntarse qué contingencias podría enfrentar su empresa ante una situación como ésta, y qué lecciones pueden aprenderse de ella.

1. Movimiento Ciudadano alega haber consultado a Indatcom, S.A. de C.V., sobre la mejor manera de administrar la base de datos recibida del INE; sin embargo esa empresa es una consultora de comunicación digital, no de seguridad informática, y la contratación de un servicio de cloud por sí solo no dota de seguridad a la información almacenada ahí, ya que cada cliente debe configurarlo de acuerdo a sus requerimientos.

Además de abogados especializados en protección de datos personales y cumplimiento normativo contamos con el respaldo técnico de la consultoría de seguridad informática Alferza, lo cual nos permite asesorarle puntualmente sobre la mejor manera de dar cumplimiento a sus obligaciones en materia de protección de datos y seguridad de los mismos más allá de las formalidades jurídicas que la materia exige.

2. El hallazgo de la base de datos habría ocurrido entre el 10 y el 16 de abril; sin embargo el INE la dio a conocer hasta el 22 de ese mes y después de que la prensa especializada en seguridad informática diera cuenta de ella. En el caso del sector privado la Ley de Protección de Datos Personales y su Reglamento imponen la obligación de dar a conocer la vulneración de la seguridad de datos personales a las personas afectadas una vez confirmado el evento y tomadas las medidas de remediación correspondientes,

informándoles de lo sucedido, las acciones tomadas al respecto y recomendaciones para su seguridad.

Naturalmente toda manifestación de una vulneración podría motivar el escrutinio de la autoridad de protección de datos personales, e incluso ser indicativo de deficiencias en la implementación del sistema de gestión de datos personales de la responsable vulnerada, por lo que es preciso considerar si su empresa en efecto ha dado cumplimiento cabal a sus obligaciones en la materia, pues de haberlo hecho podría quedar libre de responsabilidad por el evento si acreditase la conformidad de dicho sistema con el marco normativo aplicable.

¿Recuerda el caso de la venta de datos personales de clientes estadounidenses de AT&T por personal de Teleperformance, su call center en Monterrey? De acuerdo con comentarios de funcionarios del INAI hechos en foros sobre protección de datos, la verificación de esa autoridad concluyó que todas sus medidas de seguridad estaban debidamente implementadas y que el ataque fue resultado del dolo de su personal, no imputable al call center. Ese nivel de cumplimiento es el que se requiere para sortear exitosamente una verificación como esa.

3. Una vez atendido el evento será preciso revisar las medidas de seguridad física, administrativa y técnica que la normatividad de protección de datos personales requiere implementar. Ello puede requerir la revisión y modificación de resguardos físicos y digitales, limitación de privilegios de acceso a y uso de la información así como seguimiento de tal uso, restricción de la información personal que se almacene y utilice, modificación de la sintaxis de contraseñas o incluso realizar inversiones en la adquisición de *software* y equipos de monitoreo y seguimiento de accesos y tráfico en su red, entre otras.

4. ¿Qué contingencia podría enfrentar su empresa ante un evento como éste? Las multas que el Instituto Nacional para la Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) puede imponer son determinadas en función de la gravedad de la infracción, la reincidencia del infractor, la naturales de los datos vulnerados y la capacidad económica del responsable. Su cuantía va oscila entre 100 y 160,000 días de salario mínimo tratándose de infracciones “no-graves” y entre 200 y 320,000 en el caso de las “graves”, pudiéndose incluso duplicar cuando involucren datos personales “sensibles”.

Infracciones como la violación de la confidencialidad de los datos personales, la comunicación de los mismos a terceros incumpliendo la normatividad y la vulneración de la seguridad de una base de datos **imputable a la empresa** son sancionadas como graves.

Es importante enfatizar que la Ley de Protección de Datos no exige una seguridad absolutamente hermética y a prueba de balas; lo que si exige es que hayan sido implementadas cuando menos las medidas de seguridad indispensables y suficientes conforme a la naturaleza de los datos personales que su empresa maneje y los riesgos a los que estos podrían estar expuestos. Empresas como Teleperformance en el caso de AT&T han sorteado exitosamente la verificación del INAI tras el reporte de una

vulneración contando con las medidas de seguridad adecuadas no obstante que estas fueron vulneradas por el dolo de algunos empleados desleales.

Existen diversas metodologías para la medición del riesgo al que los datos personales que su empresa maneje podrían estar expuestos, y estándares para determinar el nivel de riesgo que podría asumir e implementar las medidas de seguridad más acordes con sus necesidades para minimizar tal riesgo. Nos complacerá poder brindarle la guía que requiera con relación a ello.