

La mala gestión de los datos por parte de las empresas y sus consecuencias

El caso reciente de la masiva exposición de datos privados en Ecuador es una buena oportunidad para que las empresas evalúen qué acciones están llevando adelante para proteger sus activos

La noticia sobre la exposición de datos privados de **más de 20 millones de personas en Ecuador** a raíz de una base de datos mal configurada generó revuelo en ese país, pero debería servir a muchas empresas y organizaciones para reflexionar acerca de qué posibilidades existen de que algo semejante pueda ocurrirles y qué aspectos de seguridad deberían mejorar para evitar un escenario similar.

En el caso de Novaestrat –empresa propietaria del servidor que expuso la información–, tengamos presente que el incidente de seguridad que afectó aparentemente a casi la totalidad de la población de Ecuador, se produjo como consecuencia de la mala configuración de una base de datos. **Es decir, un error humano.** Es importante que las empresa y organización no solo dediquen tiempo y recursos a los aspectos tecnológicos de la seguridad, como pueden ser las soluciones de cifrado o las soluciones de prevención de fugas de información, sino también a la elaboración de procesos y políticas de seguridad que incluyan los debidos controles y contribuyan a que la gestión de la seguridad sea la adecuada.

Si bien cifras del ESET Security Report 2019 comprueban que el **61% de las empresas en América Latina** manifestó que sus tres principales preocupaciones de seguridad son: el acceso indebido, el robo de información y la privacidad de la información; en países como Ecuador y Perú, menos de la mitad de las empresas cuenta con una política de seguridad.

En la edición 2017 de este mismo informe, **1 de cada 10 empresas de Latinoamérica** afirmó haber sufrido una brecha o fuga de información, y en ese entonces apenas el **30% de las organizaciones** dijo contar con un plan de continuidad del negocio o de respuesta a incidente, algo que permitía ver que era muy factible que este tipo de incidentes siguiera ocurriendo, predijo hace dos años el jefe del laboratorio de ESET Latinoamérica, Camilo Gutiérrez cuando explicó las consecuencias de una fuga de datos.

Si bien para analizar por qué siguen surgiendo nuevos casos de exposición y/o brecha de datos es necesario considerar múltiples factores, sin dudas que el responsable de un alto porcentaje de las brechas que se dan anualmente es el error humano. En este sentido, la exposición de datos como consecuencia de la mala configuración de una base de datos no es una novedad. En 2018 solamente, se observaron al menos tres casos de exposición de datos privados que involucraron a millones de individuos en distintas partes del mundo como consecuencia de bases de datos mal configuradas, uno de ellos en Brasil y otro en México.

Es importante recordar que una brecha de información puede provocar graves consecuencias para la compañía que sufre el incidente, además de las que afectan a los usuarios. Una de estas consecuencias es de índole económica, ya que muchas empresas están obligadas a resarcir económicamente a los usuarios cuya información se filtró o deberán pagar multas según la legislación local. Asimismo, puede suceder que la información que se filtra afecte a la competitividad de la empresa o que interrumpa el negocio alterando la dinámica productiva, lo cual también generaría consecuencias económicas.

Según datos de la edición 2019 del reporte global “El costo de las brechas de datos” que realiza IBM junto al Instituto Ponemon, el costo promedio de una brecha de datos en países como Brasil es de \$1.35 millones de dólares, siendo el país con el costo promedio más bajo en el estudio, mientras que en Estados Unidos esta cifra asciende a \$8.19 millones. Además, el costo promedio por cada registro a nivel global es de \$150 dólares y el tiempo promedio estimado para identificar y contener una brecha de datos es de 279 días.

El daño a la imagen y a la confianza que se tienen de la marca puede tener consecuencias importantes. Facebook, por ejemplo, tras el caso de Cambridge Analytica en 2018 perdió en proporciones enormes la confianza que tenían los usuarios en la red social y le significó un daño importante a la imagen que se tenía de la compañía.

Está claro que el incidente que acaba de ocurrir esta semana en Ecuador pone en evidencia la necesidad de seguir trabajando en concientización y educación, tanto con las empresas como con los usuarios.