La fuga de información: tendencia de cibercrimen.

Nicaragua, septiembre 2017

NEWS

Preparado por:
Edwin Vargas, Ingeniero de Sistemas, Auditor TI.

El robo o la apropiación de datos de una empresa por parte de terceros siempre ha sido un problema en los negocios. Siempre han cohabitado actores internos y/o externos en estos hechos. Sin embargo, los datos de las organizaciones

Según ESET, en 2017 el 10% de las empresas en Latinoamérica han sufrido algún tipo de fuga de información y aunque la proporción no es tan grande, cada vez son más recurrentes este tipo de hechos en la región.

Igualmente se señala que, dentro del grupo de empresas, solamente el 30% de estas cuentan con un Plan de continuidad de Negocios o un Plan de respuestas a incidentes, por lo que la proporción de empresas comprometidas con fuga de información puede verse en aumento, incluso este mismo año.

Esta pérdida de datos puede comprometer a las organizaciones de maneras muy diversas: desde lo financiero hasta su imagen ante el mercado, haciéndose menos atractiva para sus clientes.

Generalmente, cuando las organizaciones son atacadas, las fuentes son externas, internas o mixtas.

Estos incidentes suelen incluso realizarse no de una forma masiva, sino periódica y sucesiva, que es realizada de manera sigilosa, por distintos medios: desde CD´s hasta microSD donde unos pocos megas de información pueden ser sustraídos.

Y la tendencia de fuga de información, también crece de manera exponencial con el tiempo que transcurre la dependencia de medios digitales para almacenar información.

ESET presentó en 2015 un estudio donde se analizan los registros de empresas a nivel global, que han presentado problemas con fuga de información en algún momento y a diversas escalas y se pudo apreciar que más del 70% de los casos habían ocurrido entre 2001 y 2014 (el estudio revisó datos de 2004 a 2014).

Esto sin lugar a dudas nos muestra cómo este incidente viene teniendo una tendencia creciente en lo que refiere a pérdidas de información para las empresas, y debería servir de alerta para considerar con una mayor importancia los controles enfocados en mitigar este tipo de riesgos.

De hecho, un dato curioso es que la cantidad de registros filtrados en los últimos dos años es casi igual al 90% de la cantidad de habitantes de Latinoamérica, lo cual sería como si en el último par de años se hubiera visto filtrada información sensible de 9 de cada 10 habitantes de la región.
Vale la pena anotar que en la lista de empresas afectadas por estas brechas de seguridad encontramos a Gmail, eBay, Adobe, Sony, Target y AOL entre otras grandes empresas que llegan a manejar grandes volúmenes de información sensible. Como ya lo hemos mencionado, la información publicada es solo un porcentaje de lo que realmente ocurre y por lo general está asociado con empresas de gran renombre.

Esto no quiere decir que aquellas empresas más pequeñas no sean vulnerables a este tipo de incidentes. De hecho, en lugar de pensar que por ser una pequeña empresa no va a ser atacada, la forma de pensar debería ser que, si pudieron afectar a una empresa grande con grandes controles de seguridad, la empresa más pequeña puede ser más vulnerable.

Industrias más afectadas e incidentes más comunes.

Una de las preguntas más comunes para los analistas de seguridad es cuál es el perfil de empresas que más buscan afectar los atacantes y de la información recolectada resulta que el 70% se encuentra en una de las siguientes categorías:

- Empresas web.
- Financieras.
- Empresas de salud.
- Gobiernos.
- Compañías de retail.

El restante 30% se reparte en empresas de transporte, energía, académicas y telecomunicaciones, entre algunas otras.

¿Cuáles son los incidentes más comunes que afectan a las empresas?

Resulta que cerca de la mitad de los incidentes están relacionados con ataques externos y una cuarta parte tiene que ver con equipos o dispositivos perdidos o robados con información sensible. El restante 25% se reparte entre información publicada accidentalmente, casos de fraude interno y niveles pobres de seguridad.

Si bien en la mitad de los casos, cuando se habla de ataques externos las causas pueden ser muy diversas, se pone en evidencia que amenazas como códigos maliciosos, vulnerabilidades, APTs entre otras son las mayores causantes de las fugas de información. En estos casos hay una variedad de controles que deberían implementarse de acuerdo a cada tipo de empresa, pero en el caso del 25% de los incidentes de fuga de información que se presentaron por pérdida o robo de dispositivos se hubiera podido prevenir con un control sencillo como el cifrado de información.

Recomendaciones.

Algunas recomendaciones importantes a seguir en este aspecto son:

- Buscar asesoría en infraestructura de sistemas y en ciberseguridad, además de realizar una auditoría de sistemas, en caso de no haber realizado ninguna de estas acciones.
- Realizar inspecciones periódicas y sistemáticas de los puntos de control más importantes.
- Invertir en capacitación del personal sobre el tema de ciberseguridad y cibercrimen.
- Valorar utilizar servicios de encriptación de datos y gestión digital de alta seguridad.
- Actualización constante de software y hardware de seguridad.