

Lastpass: Los riesgos de los servicios en la nube

by javier - Miércoles, junio 17, 2015

<http://memoriasdeunsysadmin.tk/2015/06/17/lastpass-los-riesgos-de-los-servicios-en-la-nube/>

La noticia del día fue, sin duda, la intrusión que sufrió LastPass. Sin duda un golpe a la confianza de los usuarios normales en la nube. Para los que estamos más o menos en el tema, la inseguridad en la nube es un tema de todos los días. Después de todo, hay que tener en cuenta que, si es muy difícil mantener un servidor propio, seguro contra las innumerables amenazas desde internet, cuánto más difícil puede serlo un servicio popular en la nube, mucho más conocido que un servidor doméstico en nuestras casas y más aún, blanco de todas las miradas que buscan hacerse con cuentas ajenas. Y olvidamos un pequeño detalle... LastPass además, almacena millones de contraseñas de tantos otros distintos servicios y sitios en internet. Creo que poca gente había pensado detenidamente en esto, verdad?

Desgracia con suerte?

De acuerdo al [post original de LastPass](#), las contraseñas maestras NO fueron comprometidas, lo cual es una excelente noticia. Si no mienten acerca del proceso de encriptación y autenticación que utilizan, podemos tener una cierta tranquilidad. Mienten? Imposible saberlo. Después de todo, lastpass es propietario, tanto su código como sus servidores son cerrados. Esto implica que si bien se puede tener una idea de lo que hacen y cómo lo hacen, es prácticamente imposible confirmarlo

Debiera preocuparme por esto? Probablemente no. No más que lo que debieras preocuparte por usar tecnologías y servicios de Microsoft o Google.

Qué datos se vieron comprometidos?

De nuevo deberemos confiar(o no) en el reporte de LastPass: Según el blog oficial, los atacantes no se hicieron con ninguna contraseña maestra, pero sí con otros datos importantes, como los emails asociados a cada cuenta, los recordatorios de contraseñas, etc. Si bien insisten en que la encriptación es lo suficientemente fuerte como para que averiguar una contraseña en sus servidores por fuerza bruta(o diccionario) sea algo prácticamente imposible, es importante destacar que si, tu contraseña es muy débil o tu recordatorio de contraseña es demasiado claro, tu cuenta SI puede estar expuesta en este momento.

Debo tomar alguna medida?

Lo mismo que recomienda LastPass, te lo aconsejo yo también: Cambiar ahora mismo tus contraseñas maestras, siempre usando contraseñas fuertes. Cambiar además recordatorios de contraseñas y además, NUNCA usar la misma contraseña maestra como contraseña en otros servicios, ya que si estos son menos seguros que LastPass, solo estás poniéndoselo fácil a cualquiera que intente robarte cuentas. LastPass por su parte, indica que está tomando medidas extra(además de corregir los huecos de seguridad que encontraron).

Dejar LastPass?

Sinceramente, eso está en cada uno. El servicio de LastPass es bastante bueno y útil. Aún cuando acaba de ser hackeado, eso no es lo que debiera preocuparte, sino más bien que es un servicio privado y no podés saber con total seguridad QUÉ hacen con tus datos. Personalmente, no confiaría mis contraseñas en una solución online, pero la decisión es de cada uno.

En mi sección de [Soluciones Libres](#) vas a encontrar un par de alternativas a lastpass, aunque seguramente hayan otras.

Como siempre, te invito a que nos des tu opinión y nos acerques además cualquier inquietud o duda.

Saludos!

memoriasdeunsysadmin.tk