Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

UNA CONTRASEÑA PARA GOBERNARLOS A TODOS

Said Ramírez Hernández

numero-30

Hoy en día, la mayoría de las personas se encuentran registradas en al menos una red social o tiene acceso a una cuenta de correo electrónico. Por esta razón, la mayoría de las aplicaciones y plataformas han decidido integrar el concepto de *single sign on*, el cual es un método utilizado para

permitir a los usuarios acceder a múltiples recursos o instancias mediante una sola identificación, que por lo general es un usuario y una contraseña. Este tipo de mecanismos es de gran utilidad debido a que se simplifican los procesos de registro y de autenticación, pues únicamente se debe otorgar autorización a la aplicación y listo.

Sin embargo, ¿alguna vez te has detenido a pensar sobre qué pasaría si un atacante lograra apoderarse de tu usuario y contraseña de Facebook, de Google o cualquier otra de tus redes sociales? La respuesta más obvia sería que tendría la capacidad de vulnerar la privacidad de tus mensajes, notas personales, fotografías y todo tipo de información que tengas almacenada en esa red; incluso también podría dañar tu imagen y reputación. Si tienes cuentas vinculadas el impacto no se queda ahí.

Pensemos por un momento en una compañía de la cual han comprometido sus credenciales de LinkedIn con el objetivo de publicar contenido inapropiado o que va en contra de sus políticas. Si esta cuenta está configurada para publicar automáticamente en Facebook y Twitter, el contenido de dichas publicaciones tendrá una mayor audiencia, lo cual provocará que el nombre de esta compañía esté en boca de todos, inclusive podrían llegar a perder la confianza de sus clientes, lo que se traduciría en una pérdida económica para la organización.

El punto es que podemos concentrar una cantidad finita de aplicaciones vinculadas con una sola identificación, y eso no tiene nada malo, siempre y cuando se tomen las medidas apropiadas para protegerlas. Tomemos como ejemplo a Facebook; si un atacante se apoderara de tus credenciales, solamente tendría que ir a la sección de *Apps* dentro de la pestaña de configuración para obtener el listado de aplicaciones que has autorizado, y así poder autenticar en cada una de ellas y causar un daño mucho mayor. Interesante, ¿no? Como J. R. R. Tolkien escribió en sus obras para referirse al “anillo único” y haciendo una analogía con este tema, se podría decir:

“Una contraseña para gobernarlos a todos, una contraseña para encontrarlos, y causarles mucho daño”

Lo ideal sería contar con una contraseña para cada sitio web o aplicación que utilices en tu vida diaria, de esta forma, se minimizaría la superficie de ataque en caso de que la seguridad de tus credenciales se viera comprometida. Actualmente existen un sinfín de gestores de contraseñas, algunos son nativos del sistema operativo como el Keychain de macOS y otros son multiplataforma, como Buttercup, KeePass o 1password por mencionar algunos.

Pero al final estamos cayendo en la misma situación, depositamos todos nuestros accesos en un solo contenedor protegido por una contraseña maestra, una huella dactilar o cualquier otro tipo de elemento biométrico. Hay que recordar que, por definición un sistema no es 100% seguro y siempre existirá una vulnerabilidad asociada con este, imagina por un momento que olvidas la contraseña maestra de tu gestor de contraseña, toda aquella información que hayas almacenado se perderá. También existen las fallas de seguridad asociadas con el desarrollo de software, basta con recordar algunas aplicaciones como LastPass, Keeper Password Manager o Dashlane Password Manager, entre muchas otras, que han sido afectadas por vulnerabilidades que permiten comprometer la seguridad de la información almacenada y “protegida” por ellos.

Es importante mencionar que la mayoría de las plataformas, aplicaciones y servicios que utilizamos día a día, cuentan con un apartado dedicado a la seguridad dentro de sus opciones generales. En la mayoría de ellos se pueden habilitar acciones como el envío de alertas por correo o mensaje de texto ante eventos como inicios de sesión o nuevas autorizaciones o cambios de contraseña. Incluso puedes habilitar un segundo factor de autenticación (2FA) mediante la integración de un tercero como Google Authenticator, Microsoft Authenticathor o Authy por mencionar algunos. Con esta medida de seguridad, además de autenticarte con tu usuario y contraseña en la forma tradicional, tendrás que ingresar un código que se actualiza cada cierta cantidad de segundos (60 segundos es el valor más común).

Desafortunadamente, muchas de estas opciones de seguridad vienen deshabilitadas por defecto y requieren que el usuario le dedique unos minutos para su configuración. Además, atiende estas recomendaciones para mejorar tu seguridad.

- Revisa el apartado de seguridad de todas las aplicaciones y plataformas con las que trabajas en tu vida diaria.
- Recuerda que es importante cambiar tus contraseñas con frecuencia, no compartirlas con los demás, y si por alguna razón lo tienes que hacer, cámbiala inmediatamente después de que la hayan terminado de ocupar.
- No uses palabras que aparezcan en un diccionario o que sean fáciles de adivinar (tu nombre, fecha de nacimiento o aniversario, letras o números consecutivos), no las escribas en un papel y no las guardes en un archivo de texto plano sin protección en tu computadora, si lo llegas a hacer, recuerda que hay mecanismos para cifrar su contenido como PGP (*Pretty Good Privacy*).
- Revisa el historial de los dispositivos en los que has iniciado sesión, y si no reconoces alguno, siempre tendrás la opción de forzar el cierre de sesión.

Sin embargo, existe un problema común con el que te puedes enfrentar al momento de habilitar el 2FA

y que tiene que ver principalmente cuando se utiliza una aplicación desarrollada por un tercero para acceder a un determinado servicio como el correo electrónico o un dispositivo como una consola de videojuegos o un reproductor de contenidos digitales. Pero no te preocupes, porque siempre podrás generar una “contraseña específica por aplicación” y evitarte este problema, la cual mantiene un nivel alto de seguridad y sin la necesidad de memorizarla.

Recuerda que la seguridad la hacemos todos, no simplifiques el trabajo de los atacantes y protege tu información siempre.

REFERENCIAS

- Apple. (2017). Uso de contraseñas específicas de la aplicación. Recuperado el 15 de septiembre del 2017 de https://support.apple.com/es-mx/HT204397
- Facebook. (2017). Consejos de seguridad. Recuperado el 15 de septiembre del 2017 de https://es-la.facebook.com/help/379220725465972/
- Google. (2017a). Aumentar la seguridad de tu cuenta. Recuperado el 15 de septiembre del 2017 de https://support.google.com/accounts/answer/46526?hl=es
- Google. (2017b). Acceso mediante la contraseña de la aplicación. Recuperado el 15 de septiembre del 2017 de https://support.google.com/accounts/answer/185833?hl=es-419
- LinkedIn. (2017). Recomendaciones de seguridad y privacidad de una cuenta. Recuperado el 15 de septiembre del 2017 de https://www.linkedin.com/help/linkedin/answer/889?lang=es
- Microsoft. (2017). Contraseñas de aplicaciones y verificación en dos pasos. Recuperado el 15 de septiembre del 2017 de https://support.microsoft.com/es-mx/help/12409/microsoft-account-app-passwords-two-step-verification
- Pontiroli, S. (2013). PGP – Privacidad, seguridad y autenticación fiables para todos. Recuperado el 15 de septiembre del 2017 de https://www.kaspersky.es/blog/pgp-privacidad-seguridad-y-autenticacion-fiables-para-todos/1781/
- Twitter. (2017). Consejos de seguridad de la cuenta. Recuperado el 15 de septiembre del 2017 de https://support.twitter.com/articles/349068?lang=es
- Wei, W. (2017). 9 Popular Password Manager Apps Found Leaking Your Secrets. Recuperado el 15 de septiembre del 2017 de http://thehackernews.com/2017/02/password-manager-apps.html

SI QUIERES SABER MÁS, CONSULTA:

- 5 consejos prácticos para mejorar la seguridad en redes sociales
- Redes sociales, entre la ingeniería social y los riesgos a la privacidad

---