FACUA.org - España - 5 de diciembre de 2018

El secretario de Estado para el Avance Digital conocía el fallo de seguridad cuando dirigía Change

El secretario de Estado para el Avance Digital y exdirector de Change.org en España conocía desde al menos 2013 el fallo de seguridad que acaba de denunciar FACUA-Consumidores en Acción ante la Agencia Española de Protección de Datos (Aepd). La irregularidad permitía acceder a datos personales y suplantar la identidad de cualquier usuario de la plataforma con sólo introducir su dirección de correo electrónico.

El actual secretario de Estado para el Avance Digital del Ministerio de Economía fue director de Change España hasta el año pasado. **Polo**creó en 2010 la plataforma de recogida de firmas Actuable, que en 2011 fue absorbida por la multinacional estadounidense Change.org.

En febrero de 2013, el informático **Ricardo Galli** denunció públicamente que habían firmado en su nombre varias peticiones en Change, tras lo que otros usuarios advirtieron de que habían sufrido también suplantaciones. Preguntado por las irregularidades por el diario *La información*, **Polo** se limitó a restar importancia al asunto y no anunció ningún cambio para impedir que siguiesen produciéndose.

El problema de seguridad ha seguido existiendo hasta que el pasado 21 de noviembre FACUA se dirigió a la empresa para indicarle que estaba vulnerando el Reglamento general de protección de datos. La matriz de Change en EEUU ha corregido la irregularidad pero no ha eliminado el historial de firmas y comentarios realizados de forma no segura ni ha enviado una comunicación a sus usuarios para informarles de lo ocurrido.

> El secretario de Estado para el Avance Digital, @franciscopolo, debería explicar por qué no hizo nada para acabar con el agujero de seguridad en @change_es pese a que conocía su existencia cinco años antes de la denuncia de @facua. https://t.co/88ibrVqKyz
>
> — Rubén Sánchez (@RubenSanchezTW) 4 de diciembre de 2018

Un problema simple y fácil de resolver

El origen del problema de seguridad era tan simple como fácil de resolver. Change permitía que cualquier persona crease, firmase y comentase una petición sin comprobar si era realmente el titular de la cuenta de correo electrónico introducida para ello en la plataforma. Además, el introducir un mail que ya estuviese registrado en la web, la empresa revelaba el nombre, apellidos, localidad y profesión del usuario.

Tras la reclamación de FACUA, Change ha introducido medidas para que un usuario ya registrado no pueda firmar una petición sin una verificación. Asimismo, si se introduce la dirección de correo electrónico de un usuario ya registrado, la web ya no muestra sus datos personales, sino que insta a introducir su contraseña para poder firmar o crear una petición.

Asimismo, la empresa ha comunicado a la asociación que ha implementado modificaciones para que cualquier persona que se dé de alta en Change *"no pueda registrar su firma sin una verificación"*. Pero lo cierto es que esta irregularidad sigue produciéndose a día de hoy, algo de lo que FACUA ha advertido de nuevo a la compañía.

La denuncia en la AEPD

Change no ha aceptado, como le reclama FACUA, proceder al envío de una comunicación a todos sus usuarios para informarles del problema de seguridad que venía produciéndose en la plataforma, tal y como establece el artículo 34 del Reglamento general de protección de datos. La empresa tampoco ha accedido a eliminar todas las firmas y comentarios de peticiones que se hubiesen producido por parte de usuarios que no estuvieran correctamente logueados (con su correo y contraseña).

Ante esto, FACUA ha puesto los hechos en conocimiento de la AEPD. La asociación considera que Change.org ha vulnerado los artículos 6 y 32 del Reglamento general de protección de datos al haber facilitado la publicación de firmas y comentarios de usuarios sin recabar su consentimiento y no haber establecido los sistemas de protección necesarios para impedir que terceras personas pudieran suplantar sus identidades y tener acceso a sus datos. También entiende que ha incumplido el artículo 9 del Reglamento al haber tratado datos especialmente protegidos, relativos a opiniones y creencias políticas, sindicales, religiosas... sin las medidas de protección adecuadas