



PROBLEMAS DE IDENTIDAD

En mi negocio es importante identificar correctamente a los usuarios, tanto en el momento de su registro como en el acceso a los servicios ofertados. Necesitamos conocer exactamente su edad y su procedencia para poder determinar el rango de servicios al que pueden acceder.

Durante el registro de nuestros usuarios y, a falta de una solución *online* de validación de la identidad, tradicionalmente este proceso se ha llevado a cabo utilizando una mezcla de verificación documental (en función de la procedencia del usuario) y validación fuera de línea (ya sea mediante teléfono o correo ordina-

tor de autenticación, certificados, DNI electrónico, etc.

Dos de estas soluciones (quizás aquellas en que hemos depositado más nuestra confianza, por su relativo bajo coste de implantación y, sobre el papel, la tan ansiada infalible seguridad) han sido objetivo de ataques devastadores en el último año, devolviéndonos a la realidad de que la solución para identificar a nuestros usuarios no consiste en pedir a terceros que sean los que custodien las contraseñas, ya sea el secreto compartido utilizado para fabricar las soluciones de dos factores, como la clave privada de la autoridad de certificación.

autenticación en un entorno social donde los usuarios comparten información que en otro momento habiéramos considerado suficiente para evitar que nuestros adversarios suplantarán la identidad de nuestros clientes.

Dejando a un lado la obsolescencia de las preguntas "secretas" (que, por otro lado, probablemente nunca han sido tan seguras como desearíamos como mecanismo de autenticación), desde mi punto de vista el entorno social ofrece muchas posibilidades a nuestros esfuerzos de identificación: desde poder conocer mejor al cliente, ver desde dónde o cómo se conecta, hasta crear desafíos/respuesta sobre la marcha basándonos en la información que ha compartido con sus amigos ("¿dónde cenaste ayer?", "¿quién aparece en la foto que has tomado esta mañana?"). O mandarnos un "tweet" desde la cuenta asociada a su perfil social, o simplemente dejar que sean los amigos quienes den fe de la identidad de nuestro usuario.

Quizás nuestro problema es enfocar la identificación del usuario en mantener un secreto, identificarlo por lo que sabe más que por lo que es. Quizás deberíamos empezar a pensar que cada vez son más los datos accesibles *online* acerca de nuestros usuarios, que permiten crear un mejor perfil acerca de quiénes son nuestros clientes.

rio), con un coste considerable en tiempo y esfuerzo invertido por usuario.

Resulta complicado solucionar de forma sencilla este problema: no es suficiente asumir que el cliente ha proporcionado sus datos correctamente y, por otro lado, que los datos necesarios para validar la identidad del usuario durante su registro no están disponibles públicamente (quizás ahí es donde reside su valor), por lo que es probable que el proceso de validación de identidad durante el registro siga basándose en verificaciones fuera de línea a corto y medio plazo.

Más difícil resulta validar la identidad del usuario en el acceso repetido a los servicios, un problema extensible a cualquier otro sector de negocios en línea. La necesidad de mantener al usuario identificado sin permitir a terceros suplantar su identidad nos ha llevado a investigar mecanismos de autenticación "fuerte", alternativos a la contraseña que pudieran ofrecer una mejor protección frente a las amenazas actuales. Estoy seguro de que todos hemos investigado soluciones alternativas con mayor o menor éxito: tarjetas de coordenadas, segundo fac-

tor de autenticación, certificados, DNI electrónico, etc. Probablemente, deberíamos ver que el principal interesado en proteger su identidad es el cliente y que podemos utilizar esto mucho más a nuestro favor en lugar de intentar, con poco éxito, transferir el riesgo a los fabricantes de soluciones de autenticación.

Quizás nuestro problema es enfocar la identificación del usuario en mantener un secreto, identificarlo por lo que sabe más que por lo que es. Sin empezar a pensar en soluciones biométricas que, fuera del entorno empresarial, son difíciles de introducir y más difíciles aun de justificar, quizás deberíamos empezar a pensar que cada vez son más los datos accesibles *online* acerca de nuestros usuarios que permiten crear un mejor perfil acerca de quiénes son nuestros clientes.

En principio esto es una mala noticia para nuestros esfuerzos de autenticación. ¿Cuándo ha sido la última vez que hemos revisado nuestro mecanismo de recuperación de contraseñas para evaluar el nivel de protección de las preguntas "secretas" de nuestros usuarios? Quizá información como "el amigo de la infancia" o "el nombre de mi mascota" han perdido su valor como mecanismo de

Tampoco se trata de asustar al cliente ni de abusar de su confianza, sino más bien de establecer un punto intermedio donde ambas partes se encuentren cómodas compartiendo y validando información. Como muestra un botón: hace unos años nos hubiera costado compartir nuestro número de teléfono durante el proceso de registro en un nuevo servicio, hoy en día el teléfono móvil es un mecanismo utilizado rutinariamente como segundo factor de autenticación y como mecanismo seguro de recuperación de contraseñas perdidas.

Identificar inequívocamente a los usuarios, protegiéndolos de suplantación de identidad y a un coste asumible en tiempo y esfuerzo: este es el problema de identidad que me preocupa y para el que, de momento, no tengo una solución satisfactoria. ■



Lluís Mora
Responsable de Seguridad
de la Información
lluismh@gmail.com

**BWIN PARTY DIGITAL
ENTERTAINMENT**