Procedimiento para la eliminación de fraudes de suplantación de personalidad

QUEDA CLARO QUE, SI SE PRETENDE ELIMINAR O REDUCIR EL IMPACTO DEL FRAUDE, DEBERÁ SER LA ENTIDAD FINANCIERA LA QUE APLIQUE PROCEDIMIENTOS QUE LO IMPIDAN

José Carrillo Verdún

PROFESOR

Facultad de Informática UPM

Recientemente he podido leer noticias como:

- Ciberespías y asociaciones criminales armadas con programas especiales que roban información digital a empresas generaron en 2008 pérdidas por un billón de dólares, según un estudio de McAfee.
- La confianza en Internet ha comenzado a perderse por efecto del fraude y el robo de identidad, advirtió esta semana en Cartagena de Indias el director de Privacidad del gigante informático Microsoft, Brendon Lynch. El problema viene de la identidad en la red, donde es "relativamente fácil suplantar un sitio web de renombre", ... y apuntó que "los consumidores están acostumbrados a compartir 'secretos' en línea y también están 'cansados de nombre de usuario y contraseña'".

Está claro que tenemos un problema importante (un billón de dólares) como consecuencia de un deficiente control de identidad en operaciones realizadas usando canales no presenciales (cajeros automáticos, TPV, fraudes a través de la red, ...).

> Es un hecho el que por mucha formación que se aporte a los clientes nunca se podrá predecir el comportamiento humano

¿Por qué no se toman medidas para solucionarlo?. ¿No compensa hacer un esfuerzo que evite esta enorme cifra de fraude que, a la larga, pagamos todos?. ¿Se puede justificar el fraude por razones de "comodidad" del Cliente?.

Todas estas interrogantes tienen su respuesta y las mías me llevan a una última pregunta, ¿Es que se sabe ya cómo podrían ser evitados?.

Indudablemente ya existen métodos conocidos que aplicados pueden reducir considerablemente o eliminar estos problemas.

Dadas las características de los fraudes de suplantación de personalidad los requisitos mínimos que deben cumplir los procedimientos a aplicar tendrán en cuenta que:

a) Debe seguirse un procedimiento de autenticación mutua obligando a que también se identifique la Entidad Financiera frente al Cliente.
b) Debe impedir que el Cliente conozca todas las claves a utilizar en la autenticación hasta que no se haya autenticado la Entidad Financiera frente al Cliente
c) Las claves que se utilicen en la autenticación mutua sean de un único uso (OTP) de forma que no puedan ser reutilizadas en posteriores operaciones

El problema de su aplicación reside en la mayor o menor complejidad en su implementación, el coste de la misma y de cómo la nueva operativa pueda afectar a la comodidad del usuario. Dentro de este apartado de

problemas que debe superar la solución no se puede olvidar el relativo a la forma de comportarse que tendrán sus usuarios. Es un hecho el que por mucha formación que se aporte a los usuarios nunca se podrá predecir el comportamiento humano.

Dentro de los métodos por mi conocidos, que cumplan estos requisitos, hay uno que por su sencillez y bajo coste de puesta en marcha así como su sencillez de uso y amplio abanico de aplicaciones (operaciones en Internet, cajeros automáticos, TPV…), creo que conviene darlo a conocer.

Es un procedimiento de autenticación, que se describe en una reciente Patente Europea de la empresa española Diversid Consultoría, que permite la identificación y autenticación en nuestras transacciones electrónicas de banca on-line.

Con la aplicación de dicho procedimiento es posible evitar los fraudes de suplantación de personalidad incluidos los más frecuentes de la banca on-line, como son el Phishing y Man In The Middle.

Los beneficios son claros:

- se reducen los costes directos del fraude así como los derivados de las pólizas de cobertura y la inversión en procesos de prevención del fraude
- al dejar de ser rentable su actividad, los delincuentes tendrán menor motivación para lanzar nuevo malware
- se aumenta la confianza de los Usuarios en el uso de las transacciones electrónicas lo que repercutirá en un incremento del volumen de operaciones que se realicen
- se prima la Seguridad y Calidad de los Sistemas de Autenticación frente a la mal entendida "comodidad" del Cliente. ¿Acaso, por razones de comodidad, usted dejaría de pedir el DNI cuando un cliente vaya a operar con su tarjeta?

Este procedimiento de autenticación se caracteriza por realizar una autenticación mutua de los intervinientes por medio del intercambio de tres claves OTP almacenadas simétricamente en el teléfono móvil (o dispositivo token) del Cliente y en el ordenador, por ejemplo, del Banco.

Esta autenticación mutua, tomando como ejemplo su aplicación a la banca on-line, se fundamenta en que:

- El Cliente envía al Banco una primera clave para identificarse.
- Sólo el Banco sabe cuál es la segunda clave con la que debe responder a la primera clave recibida del Cliente.

Dado que estos sistemas ya existen, y la patente mencionada es uno de ellos, basta con que las Entidades se decidan a utilizarlos

- Únicamente el Cliente, por medio de la aplicación instalada en su móvil, puede saber cuál es la tercera clave que responde a la recibida de su Banco.
- El Cliente no llega a conocer el valor de ésta tercera clave hasta que teclea en su móvil la clave recibida del Banco y la aplicación verifica que es la correcta. Esto hace que sea imposible que, por medio de engaños, se la hubiera proporcionado a una tercera persona que posteriormente la usara en su nombre (PHISHING).
- Las claves intercambiadas son de un único uso (OTP) con lo que si algún defraudador las hubiera copiado no le servirán de nada pues en el siguiente proceso de autenticación las claves a utilizar tienen que ser distintas.

Como se puede ver, ya el Cliente no puede limitarse a repetir siempre la misma clave y ello implica el asumir la incomodidad de tener que usar un nuevo dispositivo que se las proporcione.

La solución propuesta por Diversid Consultoría evita también éste problema ya que permite que el dispositivo a usar sea el teléfono móvil que ya habitualmente llevamos con nosotros.

Para terminar vuelvo a las preguntas que ya formulé anteriormente ¿Por qué no se toman medidas para solucionarlo?. ¿No compensa hacer un esfuerzo que evite esta enorme cifra de fraude (un billón de dólares) que, a la larga, pagamos todos?. ¿Se puede justificar el fraude por razones de "comodidad" del Cliente?.

En mi opinión, dado que estos sistemas ya existen, y la patente mencionada es uno de ellos, los responsables del desarrollo de los sistemas que las empresas emplean para la autenticación de sus clientes deben aplicar estos procedimientos potenciando la seguridad y confianza en los sistemas frente a la mal entendida "comodidad" del cliente.

Creo que ya es hora de que las empresas se pongan de acuerdo con el fin de soslayar el problema de competencia que existe entre ellas y que está impidiendo el uso de sistemas de autenticación que impliquen un mayor, pero necesario, esfuerzo del cliente. Si todas las empresas aplicaran procedimientos seguros ninguna de ellas se vería afectada por el hecho de que disminuir la comodidad del uso de su sistema pueda suponer una pérdida de clientes a favor de aquellas otras que mantienen los sistemas 'cómodos'.

En éste sentido, ¿Quién podría imponer una norma de éste tipo?