Los riesgos de la firma electrónica

En este post voy a hablar acerca de los riesgos que tiene el uso de la firma electrónica. En el mundo en el que vivimos como ya sabemos toda tecnología puede ser “hackeada” y debido a ello se presentan una serie de riesgos.

La firma electrónica avanzada es confiable y segura debido a que como ya sabemos hace uso de un cifrado asimétrico. Por tanto, esta firma que es considerada al mismo nivel que la firma manuscrita es segura, entonces os podéis preguntar ¿de dónde vienen los riesgos?. Estos riesgos provienen como siempre del eslabón más débil que como ya podéis intuir es el usuario final que hace uso de la misma. Para realizar la firma electrónica avanzada se debe hacer uso de dos claves la pública y la privada. La clave pública es la que puede ser mostrada y accedida por un tercero y la privada será la que en ningún caso podrá ser conocida o accedida por otra persona, ya que esta clave lleva integrada nuestra identidad y nuestra firma. Por tanto, aquí podemos encontrar el mayor riesgo, que es la forma en la que se guarda esta clave privada en nuestros sistemas o si la misma es compartida o esta visible para otras personas.

El tener al descubierto la clave privada es un riesgo muy grave, ya que la custodia exclusiva de la misma es la garantía de no repudio de nuestras futuras firmas electrónicas, por lo que cualquier persona que disponga de la misma podrá realizar firmas fraudulentas con el mismo valor legal que si firmara a mano alzada. Por ello, es un riesgo muy grave ya que el conocimiento de una tercera persona de la clave puede traer consigo la suplantación de identidad, se podrá hacer pasar por nosotros y firmar en cualquier sitio.

Lo que ocurre muchas veces entre las empresas y los usuarios es que presuponen que únicamente ya el uso de una firma electrónica avanzada es una garantía de seguridad, pero esto es un error muy grave si no se tienen en cuenta dos reglas que son claves en este tema.

La primera de las reglas es tener la certeza de que nuestros certificados han sido generados por un prestador de servicios de certificación confiable y que para la creación de los mismos han hecho uso de un hardware criptográfico, el cual debería estar reconocido internacionalmente y aprobado por un laboratorio especializado en el tema. Esto es importante porque como hemos dicho antes la fuerza de estos certificados o su clave en cuanto a la seguridad reside en sus claves, clave privada, por tanto, la forma en la que ha sido generada la misma también es importante para mantener la seguridad de las mismas.

La segunda de las reglas es como ya he introducido antes la forma en que se custodian las claves de los certificados de los que hacemos uso. Una de las formas en las que los usuarios guardan estás claves es haciendo uso de una Smart Card que es seguro, ¿Pero ¿qué ocurre? para las empresas hacer uso de este tipo de tarjetas puede hacer que se ralentice el proceso, y por tanto lo que hacen muchas es guardarla directamente en el ordenador para acceder directamente a ella, en cualquier carpeta, vamos como si nosotros dejáramos en nuestro ordenador en un documento de texto accesibles todas nuestras contraseñas

de nuestras cuentas. Si a esto le añadimos la ausencia de control y gestión de los usuarios que tienen acceso a las claves dentro de la empresa, estamos corriendo el riesgo de la suplantación de identidad y de no saber al final quien es la persona que firma realmente.

Parece que las empresas no son conscientes del riesgo que corren dejando accesibles de esta forma sus claves, ya que es como si compramos una puerta blindada pero luego dejamos puesta la llave dentro de la cerradura. En este caso por mucha seguridad que nos de esta puerta si dejamos la llave accesible estamos dando acceso a la misma, pues lo mismo ocurre con la firma electrónica es un sistema fiable y seguro, pero en caso de dejar la clave a la vista o disponible para otros estamos dando la llave a terceros para que accedan como quieran.

Un ejemplo de este tipo de fraude que se ha presentado, de suplantación de identidad podemos encontrarlo en una noticia de este año [4] en la que se presenta el caso de que el banco BBVA ha estado usando durante dos años la firma de un empleado jubilado para firmar certificaciones de deuda del banco sin su permiso. El banco achaca el caso a que ha sido un error, pero aunque esto sea cierto es un ejemplo claro de una suplantación de identidad que se da por una mala gestión de las claves de firma de la compañía, ya que se estaba firmando como una persona que no estaba en la empresa, con los consecuentes consecuencias que podría haber traído el firmar esos

documentos con la identidad del mismo.

¿Cómo solucionar el problema de la gestión de claves en una compañía? Se debe tener una clara política de control y protección de claves, e implementar un sistema centralizado y seguro para la gestión de las mismas. Ese sistema debería tener el hardware criptográfico necesario para almacenar y gestionar las claves y permitir el acceso únicamente a los usuarios autorizados, y que nos permita saber quién firmo que y cuando.

A continuación, para terminar voy a presentar algunos consejos para poder tratar de evitar este tipo de fraudes. En caso de que se contrate un servicio de factura electrónica por internet, es interesante contratar el servicio que ofrece la firma electrónica en el que el cliente entra en la aplicación y usa el certificado que está instalado de forma segura en su propio ordenador y así de esta forma no se tiene que entregar acceso a la firma a la empresa que nos da ese servicio. En caso de haber entregado la firma ya, al dejar de trabajar con un proveedor se debe revocar ese certificado y generar uno nuevo que queda vigente desde el mismo momento en el que se genera, ya que así les obliga la ley a los prestadores de servicios de certificación. En el caso de que sea inevitable el uso de la firma por terceros, lo recomendable es que ese tercero compre su certificado propio y se le da la autorización para que con ese certificado realice los trámites correspondientes, y así de esta forma nunca conocerá ni hará uso de nuestras claves.

Referencias:

[1] “Los riesgos de no utilizar la firma electrónica avanzada”, Signaturit, consultado el 17 de noviembre de 2016,

https://blog.signaturit.com/es/los-riesgos-de-no-utilizar-la-firma-electronica-avanzada

[2] “Certificado digital peligros y riesgos para las empresas

y autónomos”, Blog sobre la relación de las Administraciones Públicas con las empresas, asesores y despachos de abogados, consultado el 17 de noviembre de 2016,

http://blog.notificaciones060.com/certificadodigital-notificaciones060.html

[3]”Cómo utilizar los certificados minimizando los riesgos de fraude”, Red seguridad, consultado el 17 de noviembre de 2016,

http://www.redseguridad.com/opinion/articulos/como-utilizar-los-certificados minimizando-los-riesgos-de-fraude

[4]”Un exempleado reclama 140 millones al BBVA por usar su firma sin permiso”, El País, consultado el 17 de noviembre de 2016,

http://economia.elpais.com/economia/2016/05/24/actualidad/1464104022_490054.html

[5] “Consejos para evitar fraudes con la firma electrónica”, Enternet, consultado el 17 de noviembre de 2016,

https://www.enternet.cl/consejos-para-evitar-fraudes-con-la-firma-digital/