La aplicación de la firma electrónica y sus usos fraudulentos

La firma electrónica es utilizada internacionalmente y tal es la seguridad que nos da si se usa de la forma correcta que como podemos encontrar en la prensa puede ser utilizada para dirigir un país. Esto ocurrió en el año 2011 cuando el presidente Hugo Chávez enfermó, y para poder seguir gobernando y tomando decisiones desde otro país, en este caso desde Cuba, implantó un sistema de firma electrónica que le permitía promulgar decretos desde la distancia [1].

Pero como ya introducimos en post anteriores el problema viene cuando no se tienen en cuenta los riesgos y no se toman las medidas necesarias para proteger las claves. Como en todo siempre pensamos a mí no me puede pasar, esas cosas pensamos que solo pasan a la empresa vecina y cuando pasan nos echamos las manos a la cabeza. Uno de los ejemplos es el caso que ha ocurrido en México en el que una serie de personas a través de un mensaje que circulaba en Facebook invitaban a la gente a acudir a recoger su firma electrónica, llamada e-firma en México, y entregarla con su contraseña correspondiente a cambio de dinero. De lo que se aprovechaban es de que alguna gente desconocía los riesgos que tiene ese hecho, y de que con ese certificado pueden hacerse pasar por ellos para cualquier trámite fiscal [2].

Otro de los casos que podemos encontrar en la prensa, es un caso de suplantación de identidad que ocurrió en Estados Unidos. En este caso, tres médicos del Hospital Magee-Womens de Pittsburgh denunciaron al centro médico en el que trabajaban, por incorporar sus firmas sin avisarles y sin su permiso en los resultados de diversas pruebas que se habían realizado en el centro [3].

Otra noticia que nos presenta los riesgos que ya se describieron anteriormente, es una noticia de un periódico español en el que se advierte de los riesgos de guardar los certificados electrónicos directamente en nuestro ordenador. En la noticia se advierte del riesgo real ya que se presenta el programa mediante el cual un consultor de seguridad afirma que puede sustraer todos los certificados almacenados en un ordenador con sistema operativo Windows, y utilizar los mismos para realizar el “mal” [4].

Un dato curioso que podemos encontrar en la prensa, es el resultado de una investigación que se ha realizado de la firma electrónica. Los resultados de la misma muestran que las personas que firmaban con la firma manuscrita, es decir con papel y boli, no engañaban ni trataban de obtener más beneficios, mientras que en el caso de los que firmaron con firma electrónica se veía, como los mismos habían obtenido más boletos que los que les correspondían. Por tanto, la conclusión a la que llegaba el estudio es que las personas no se identifican con su firma electrónica, y que solo ven que la misma tiene valor cuando la realizan de forma manuscrita [5].

Y algunos ahora os preguntareis, todo esto de la firma electrónica está muy bien, pero, ¿Puede ayudar la misma a el comercio electrónico internacional? Según un informe realizado en la Universidad de Londres [6], la misma facilita mucho la

relación para crear empresas en el extranjero y poder firmar documentos a distancia más rápidamente, pero dictamina que el problema que se encuentra la misma es el hecho de que en cada país se aplica una legislación, y que para la misma pueda ser utilizada con más seguridad debería impulsarse un consenso entre los diferentes países. Podemos decir que esto es lo que ha ocurrido en Europa mediante la publicación del Reglamento (UE) 910/2014, por lo que Europa podríamos decir que ha cumplido, y por tanto ahora los tramites a realizar dentro de Europa contarán con esa garantía que se pedía. Además, se aceptarán también certificados que no provengan de Europa siempre que cumplan con las exigencias descritas en dicho reglamento.

En cuanto al uso que se hace la misma en la industria, está claro que uso está en auge, como ejemplo podemos utilizar el caso de la empresa estadounidense Docusign [7] que está trabajando en hacer digital la documentación de empresas, particular y gobiernos y que ya opera en 43 países a nivel mundial. Es interesante ver como en la industria relacionada con la firma electrónica están trabajando y trayendo nuevas novedades que permitan hacerla más segura de lo que ya es, además de las soluciones biométricas que ya existían ahora se están introduciendo nuevas formas de firmar. Una de estas nuevas formas es la de realizar la firma mediante el uso de la voz, este sistema llamado FirVox [8] ha sido lanzado por una empresa española y el mismo convierte la voz en una firma electrónica avanzada, y cumple con lo establecido en el Reglamento (UE) 910/2014.

Por último y no menos importante, en el post anterior, hablamos de los prestadores de servicios de certificación y de

cómo ahora los mismos debían de ser auditados, pero nos dejamos algunas cosas en el tintero, por ello ahora voy a introducir cuales son los controles a realizar:

- Verificar que la infraestructura TI que soporta el proceso de firma electrónica está correctamente configurado, para garantizar que la información crítica está correctamente protegida contra modificaciones y accesos no autorizados.
- Verificar que los datos críticos de la firma electrónica están respaldados y almacenados de forma segura.
- Verificar que los dispositivos de creación de firma utilizados son auténticos.
- Verificar que para cada una de las firmas que se realizan con cada uno de los certificados, se guarda el registro de quien, en qué fecha y donde ha realizado dicha firma.
- Verificar que la firma permite comprobar los datos principales de los firmantes a partir del certificado, sin necesidad de usar herramientas especiales.
- Verificar que los documentos son verificables en cualquier momento por un tercero a partir de la información de representación visible del documento.
- Se debe revisar toda la documentación relacionada con la política de seguridad, la gestión de riesgos, la continuidad del negocio, gestión de incidentes, términos y condiciones, contratos firmados con terceros, seguros, planes de auditoria internos, listas de control de accesos y evidencias para contrastar las operaciones seguras, es decir protocolos y logs.
- Verificar que se cumplen los requisitos de las normas establecidas, que se utilizan las medidas criptográficas necesarias y otras medidas de seguridad.
- En caso de que sea necesario realizar pruebas para garantizar la conformidad de los prestadores de servicios de certificación, se podrán reutilizar las pruebas realizadas por el prestador y en caso de que

estas se vean que no son como deberían o no contemplen todos los casos necesarios se podrán realizar pruebas adicionales.

Referencias

[1] “Chávez gobernará desde La Habana con una firma digital”, El País, consultado el 27 de noviembre,

http://elpais.com/diario/2011/07/18/internacional/1310940008_850215.html

[2] “Alertan por fraude en emisión de firma electrónica por redes sociales”, Noticias 360º, consultado el 27 de noviembre,

http://noticias360.com.mx/index.php/2016/10/31/alertan-por-fraude-en-emision-de-firma-electronica-por-redes-sociales-matamoros/

[3] “Second lawsuit charges medical report falsification”, Post-Gazzete, consultado el 27 de noviembre,

http://old.post-gazette.com/localnews/20031219lawsuitr2.asp

[4] “La seguridad de los certificados para hacer la declaración en internet, ¿en riesgo?”, 20 minutos, consultado el 27 de noviembre,

http://www.20minutos.es/noticia/378330/0/vulnerabilidad/certificados/digitales/

[5] “La firma electrónica nos tienta a actuar de manera deshonesta”, Investigación y Ciencia, consultado el 28 de noviembre,

http://www.investigacionyciencia.es/noticias/la-firma-electrnica-nos-tienta-a-actuar-de-manera-deshonesta-13786

[6] “A review of electronic signatures regulations: do they facilitate or impede international electronic commerce?”, ACM Digital Library, consultado el 27 de Noviembre,

http://dl.acm.org/citation.cfm?id=1151458

[7] “Docusign busca desterrar el papel”, El País, consultado el 26 de Noviembre,

http://economia.elpais.com/economia/2014/08/01/actualidad/1406915943_812439.html

[8] “FirVox convierte la voz en una firma electrónica avanzada imposible de falsificar”, Europapress Portaltic, consultado el 27 de Noviembre,

http://www.europapress.es/portaltic/software/noticia-firvox-convierte-voz-firma-electronica-avanzada-imposible-falsificar-20161011144048.html

[9] “Electronic Signature (E-Sign) Audit Work Program”, Knowledge Leader, consultado el 27 de Noviembre,

https://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/WPElectronicSignature!OpenDocument

[10] “Auditing Framework for TSPs”, European Union Agency for Network and Information Security, consultado el 27 de noviembre,

https://www.enisa.europa.eu/publications/tsp-auditing-framework

[11] “Auditoria”, Firma electrónica de confianza, consultado el 27 de noviembre,

http://firmacertificada.es/auditoria/