La seguridad de los datos personales: directrices de ENISA sobre soluciones criptográficas

ENISA presenta hoy dos informes. El informe *"Algorithms, key size and parameters"* (*Algoritmos, tamaño clave y parámetros*) de 2014 es un documento de referencia que ofrece un conjunto de directrices a los responsables de las tomas de decisiones, especialmente a los especialistas que diseñan e implementan soluciones criptográficas de protección de datos personales dentro de organizaciones comerciales o servicios gubernamentales para ciudadanos. *"Study on cryptographic protocols"* (*Estudio sobre protocolos criptográficos*) proporciona una perspectiva sobre implementación, con directrices relativas a los protocolos necesarios para la protección de las comunicaciones comerciales en línea que contienen datos personales.

"Algoritmos, tamaño clave y parámetros"

Este informe ofrece un conjunto de propuestas presentadas en un formato que facilita su aplicación. Se centra en los servicios comerciales en línea que recogen, almacenan y procesan datos personales de ciudadanos de la UE. El informe proporciona una versión actualizada del informe sobre directrices criptográficas del año 2013 (*2013 cryptographic guidelines report*), en el que se tratan las medidas de seguridad necesarias para la protección de datos personales en los sistemas en línea. En comparación con la edición del año 2013, el informe es ahora más extenso e incluye una sección sobre canales secundarios de hardware o software, generación de números aleatorios y gestión de ciclo de vida. También se ha ampliado la parte dedicada a los protocolos, que ahora constituye un estudio completo sobre protocolos criptográficos.

El informe aborda dos aspectos relativos a los mecanismos criptográficos:

- ¿Es posible plantearse hoy el uso de un esquema o una primitiva concretos si estos ya han sido implementados?
- ¿Sería adecuado implementar un esquema o una primitiva en nuevos o futuros sistemas?

Se analizan tanto las cuestiones sobre la retención de datos a largo plazo como otros problemas generales relacionados con la implementación de primitivas y esquemas criptográficos. Todos los mecanismos abordados en el informe están en cierta medida normalizados y, o bien se han implementado, o bien esta previsto implementarlos en sistemas reales.

"Estudio sobre protocolos criptográficos"

El segundo informe se centra en el estado actual de los protocolos criptográficos y fomenta la realización de futuros estudios. El informe ofrece un resumen general de los protocolos empleados en áreas de aplicación relativamente restringidas, como las comunicaciones inalámbricas, las comunicaciones móviles o las operaciones bancarias (Bluetooth, WPA/WEP, UMTS/LTE, ZigBee, EMV) y los entornos específicos, especialmente la computación en nube.

El énfasis principal del informe recae sobre las directrices para los investigadores y organizaciones del sector, a saber:

- Los protocolos criptográficos y de seguridad deben ser diseñados por expertos en protocolos criptográficos, y no por expertos en redes y protocolos, como ha venido sucediendo hasta ahora. Asimismo, los investigadores necesitan simplificar el análisis y permitir que las herramientas automatizadas ofrezcan unas garantías informáticas sólidas.
- Debe prestarse más atención a la verificación automatizada, de modo que la implementación de un protocolo pueda satisfacer ciertos objetivos de seguridad. Al mismo tiempo, deberá determinarse cómo pueden garantizar las herramientas automatizadas la correcta implementación de un diseño de protocolo.
- Cambios pequeños e insignificantes en los protocolos pueden causar la invalidación de las pruebas de garantía.
- Los futuros protocolos deberán diseñarse basándose en principios de ingeniería sólidos y bien establecidos, análisis sencillos de seguridad formal, y el desarrollo de pruebas formales de seguridad, diseñadas en el criptoanálisis de sus primitivas constitutivas.
- Los futuros protocolos no deberían ser más complejos de lo necesario.
- Es necesario continuar trabajando en la verificación de API para protocolos de aplicación.

Udo Helmbrecht comentó lo siguiente acerca de los informes: *"Ponen de manifiesto la necesidad de contar con proyectos de certificación en todas las fases del ciclo de vida tecnológico. La "seguridad por diseño o por defecto" integrada en los procesos y en los productos es un principio básico que genera confianza. Normalizar el proceso es uno de los aspectos fundamentales de la garantía de la correcta aplicación de la reforma de la protección de datos al servicio de los ciudadanos de la UE y su mercado interior. La directrices de ENISA tienen por finalidad proporcionar el marco correcto para la seguridad de los sistemas en línea".*

El Reglamento 611/2013 de la CE menciona a ENISA como órgano consultivo a la hora de establecer una lista de medidas de protección criptográficas apropiadas para la protección de datos personales. Las directrices criptográficas de ENISA deberían servir como documento de referencia. En este sentido, las directrices facilitadas son más bien conservadoras de acuerdo con los estudios más avanzados, y tratan la cuestión de la construcción de nuevos sistemas comerciales dotados de un ciclo de vida más largo.

Para acceder a los informes completos: *"Algorithms, key size and parameters"* y *"Study on cryptographic protocols"*

Para entrevistas y más información al respecto: press[at]enisa.europa.eu