Trabajos realizados para el despliegue de DNSSEC en «.Py»

Tareas de documentaciones y definición de políticas.

- NIC-PY DNSSEC Practice Statement «DPS[1]»

Se ha trabajado arduamente en definir un modelo de DPS que establezca las políticas de las extensiones de dominios de seguridad y las prácticas actuales en las operaciones del Registro de NIC-PY. En este documento, se especifican las prácticas y especificaciones que el NIC-PY empleará en la prestación de servicios de gestión y firma de la zona.

- NIC Paraguay DNSSEC Key Ceremony Scripts «KCS»

Al igual que con el DPS, se ha trabajado en la definición de un «KCS» que defina los pasos y procedimientos técnicos y logísticos para la Ceremonia de la firma.

Cabe mencionar que tanto para el «DPS», como para el «KCS», se han tomado como modelos, las plantillas establecidas y utilizadas por el Nic.cr, a quienes agradecemos mucho la colaboración prestada.

Tareas técnicas.

El plan inicial que se ha definido fue utilizar smartcards (tarjetas chip como HSM). Luego de dos (2) días sin lograr hacerlos funcionar, con la confianza necesaria, se han analizado opciones y se ha decidido utilizar llaves en software protegido, con políticas de seguridad (escrito en el DNSSEC Practice Statement).

El mecanismo define que en ningún momento nadie tiene acceso a una llave sin estar acompañado de los responsables de Seguridad y otras personas responsables de la Institución. Para el KSK se ha decidido implementar «m-of-n»[2], basados en discos flash USB sellados en bolsas de evidencia.

El objetivo inicial propuesto fue lograr hacer una ceremonia de llaves, pero con la demora y la necesidad de cambiar la solución técnica, esto no fue posible en los días de trabajo. Una ventaja de no usar los smartcards es que se puede ahora trabajar con llaves más grandes que 2048 bits.

[1] Based on .SE DPS 22 April 2010 Licensed under a Creative Commons License

[2] (http://point-at-infinity.org/ssss/)

Se tiene previsto que la firma de la zona sea realizada en el primer trimestre del 2016, mediante una ceremonia.

Preparación de Infraestructura

- Instalación y configuración de SO, para el equipo que estará en producción, «signer».

- Creación de Scripts para la ceremonia de firma.

  - Generación de las KSK.
  - Creación de los scripts de generación de las partes de las KSK. (PY-cryptokey).

Tareas Logísticas y organizativas previas

- Análisis de los dispositivos y componentes a ser utilizados.
- Compra de todos los componentes «RNG, Bolsas de Seguridad, Smartcards, smartcards-readers, pendrives 3.0, cajas de seguridad, racks de seguridad, conectores y adaptadores, etc.).
- Preparación de las oficinas de trabajo.

Equipo Humano

El Centro Nacional de Computación ha contribuido con la participación de ocho (8) técnicos de primer nivel para acompañar y trabajar directamente en las tareas relativas al despliegue del DNSSEC, conjuntamente con el experto Robert Martin-Legène. Las tareas fueron desde el día jueves 10/12 al martes 15/12, en horarios bastante extendidos, que iban desde las 08:00 hasta aproximadamente las 23:00. También se ha puesto a disposición un equipo de dos (2) colaboradores, para los días mencionados, que estaban a cargo de la logística en general.

Impactos en la prensa local.

Los trabajos realizados durante la estadía de Robert Martin-Legène en Paraguay, ha tenido un amplio destaque en medios de prensa local, tanto escritos, como radiales, se adjunta los enlaces de referencia a los mismos.

http://www.hoy.com.py/nacionales/centro-implementara-sistema-para-evitar-hackeos-a-dominios-paraguayos

http://m.ultimahora.com/cnc-pretende-dar-mayor-seguridad-sitios-py-n954201.html

http://www.ip.gov.py/ip/?p=72980

http://nanduti.com.py/2015/12/24/una-desarrolla-tecnologia-proteccion-sitios-web/

Entrevista radial ñanduti 1020 AM sábado 26/12/15. Programa Mandi'oCast.