Una Introducción a DNSSEC

Marzo 2012

Una Publicación de .CO Internet S.A.S. | Versión 1.0

Una Introducción a DNSSEC

Marzo 2012 | Versión 1.0

Reconocimientos

Deseamos agradecer al equipo de Neustar, Inc. (www.neustaregistry.biz), nuestro socio de servicios de soporte tecnológico de operaciones (back-end) en temas de TI y Seguridad DNS, por su permanente apoyo durante el proceso de firma de la zona y su implementación. Adicionalmente, muchos agradecimientos a Hugo Salgado (NIC-Chile) por sus valiosas contribuciones relacionadas con los contenidos de este documento.

Exención de Responsabilidad

Hemos tomado todas las medidas y precauciones necesarias para proporcionarle una información clara y detallada en esta Guía Informativa DNSSEC. Cabe aclarar que ni .CO Internet S.A.S., Arcelandia y/o Neustar, ni ninguno de sus directivos o agentes, se hará responsable por cualquier error, imprecisión u omisión en este documento. Esta guía es de carácter exclusivamente informativo y el uso y confianza en la información aquí proporcionada será de la entera responsabilidad del usuario.

Una Introducción a DNSSEC

Marzo 2012 | Versión 1.0

Visión General

Los usuarios de internet son bombardeados diariamente por una multitud de amenazas a su seguridad en línea. Desde sitios fraudulentos de productos hasta el hurto de identidad y mucho más, ha generado que los individuos se encuentren cada vez más preocupados por su seguridad en línea. Habida cuenta que los malhechores se valen de herramientas cada vez más complejas y sofisticadas para operar, resulta imperativo que nosotros fortalezcamos nuestro Sistema de Nombres de Dominio (DNS), así como nuestros sitios Web, a fin de proporcionarle una experiencia en línea segura durante cada paso de su experiencia en Internet.

Estamos orgullosos de haber implementado las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) en el espacio .CO, como parte del compromiso de .CO Internet por combatir proactivamente el uso abusivo de nombres de dominio, y de convertir el espacio de nombres de dominio .CO en una de las extensiones de dominio más confiable y segura en Internet.

Por favor utilice esta guía como una introducción y un recurso de información básica sobre DNSSEC.

¿Qué es DNSSEC?

Entre otras cosas, DNSSEC incorpora firmas digitales a la infraestructura del Sistema de Nombres de Dominio (DNS) para contribuir a combatir los ataques de suplantación de identidad, ataques contra la integridad de la información y el riesgo de que los usuarios sean redirigidos hacia cualquier sitio Web inseguro o no deseado. DNSSEC es un conjunto de especificaciones técnicas para salvaguardar ciertos tipos de información proporcionada por el DNS, que pretende proteger a los usuarios de la Internet contra cierto tipo de riesgos y ataques maliciosos mediante la firma digital de la información para que usted pueda tener certeza acerca de su validez.

Sin embargo, a fin de eliminar la vulnerabilidad de la Internet, debe realizarse en cada etapa de la búsqueda de directorio, desde la zona raíz hasta el nombre de dominio final (por ejemplo, www.ejemplo.co). Más importante aún, DNSSEC no cifra la información. Simplemente certifica la validez de la dirección del sitio visitado.

Con la implementación de la actualización técnica, DNSSEC señalará automáticamente que los usuarios han sido dirigidos a los sitios Web reales que pretendían visitar – mitigando el riesgo de que sean inconscientemente raptados o erróneamente dirigidos a sitios falsos que pudieran poner en riesgo su seguridad.

Con la firma de la zona raíz por parte del ICANN el 15 de julio de 2010, la Administración del registro .CO consideró igualmente importante proporcionar a los registrantes .CO y a los usuarios de Internet a través del mundo la seguridad de que los sitio web .CO que visiten se encuentran protegidos. La zona .CO fue firmada el 1 de marzo de 2011.

Una Introducción a DNSSEC

Marzo 2012 | Versión 1.0

Create Your Opportunity

¿Cómo funciona el DNSSEC?
Los servicios DNSSEC lo protegen contra la mayoría de las amenazas al Sistema de Nombres de Dominio (DNS). Es un conjunto de extensiones de seguridad técnicas del DNS, que le brindan:

a) Autenticación de origen de los datos DNS,
b) integridad de la información, y
c) negación de existencia autenticada.

DNSSEC no proporciona confidencialidad de la información ni protege contra ataques de denegación de servicio (DDoS).

¿Quién debe implementar DNSSEC?
Todos deberían hacerlo! Cualquier dueño o Registrante de un nombre de dominio .CO que realice transacciones de datos altamente sensibles en su sitio Web, pero más específicamente, las grandes compañías e instituciones tales como las empresas de telecomunicaciones, Proveedores de Servicios de Internet, bancos, cooperativas de crédito, asociaciones u otras organizaciones que realizan ventas y transacciones en línea a través de su sitio Web.

¿Cómo mejorará DNSSEC mi seguridad?
La plena implementación de DNSSEC asegurará que Usted, el usuario final, se está conectando al sitio Web real o a otro servicio correspondiente a un nombre de dominio en particular. Aunque ello no solucionará todos los problemas de seguridad que existen en Internet, protege una parte crítica -la búsqueda de directorio- complementando otras tecnologías como SSL y proporciona una plataforma válida para las mejoras de seguridad aún por desarrollarse.

¿Cómo implemento DNSSEC en mis nombre(s) de dominio .CO?
Si usted desea implementar DNSSEC en sus nombre(s) de dominio .CO, por favor contacte directamente a su Registrador. El Administrador del dominio .CO no puede implementar DNSSEC directamente en los dominios .CO registrados, pero lo ha puesto a disposición dentro del espacio de nombres para esta importante actualización de seguridad.

Clave de Firma & Administración DNSSEC
DNSSEC trabaja mediante la firma digital de registros para la búsqueda DNS empleando ciframiento público de claves. El registro de clave correcto es autenticado mediante una 'cadena de confianza', a partir de un conjunto de claves públicas verificadas. Cuando la cadena de confianza es autenticada a través de un proceso de búsqueda completo, la firma digital es verificada y un usuario puede confiar en la seguridad de la navegación hacia el sitio web deseado.

La Gestión de Llaves DNSSEC, incluido el proceso de Sustitución de Llaves (Key Rollover), se realiza usando software DNSSEC especializado: herramientas independientes o complementos (add-ons) a su software DNS. Los principales productos de software DNS deberían contar al menos con una funcionalidad parcial DNSSEC incorporada en los próximos años.

Más Información y Recursos DNSSEC

Existen muchos sitios informativos y de recursos para el uso de DNSSEC. Para mayor información, por favor visite algunos de nuestros recursos favoritos:

Internet Society: Programa Deploy360
(http://www.internetsociety.org/deploy360/dnssec/)
El Programa Deploy360 de la Sociedad Internet (ISOC, por sus siglas en inglés) proporciona información de interés global sobre asuntos tecnológicos, incluyendo DNSSEC y IPv6.

DNSSEC-Tools
(http://dnssec-tools.org)
DNSSEC-Tools mantiene herramientas de software, parches ("patches"), aplicaciones, envoltorios o adaptadores (wrappers), extensiones y plugins que contribuirán a facilitar el uso de tecnologías afines DNSSEC.

Infoblox
(http://www.infoblox.com)
Un pionero en el desarrollo de componentes o dispositivos para servicios básicos de red, que brinda una resolución de nombres de dominio (DNS) de calidad.

Práctice Safe DNS
(http://www.practicesafedns.org)
Sitio educativo de .ORG, el Registro de Interés Público (PIR, por sus siglas en inglés), administrador del dominio de nivel superior .ORG, que presenta métodos para promover e implementar las mejores prácticas contra los ataques cibernéticos al Sistema de Nombres de Dominio.

DNSSEC-Deployment
(http://dnssec-deployment.org)
El Grupo de Trabajo sobre Despliegue de DNSSEC es un grupo de expertos de la Industria que trabaja activamente en el desarrollo o implementación de DNSSEC.