DNSSEC

Protección para sus nombres de dominio

Cuando accede a un sitio web e introduce información personal, ¿hasta qué punto está seguro de que su información está protegida? Utilizar DNSSEC puede ayudarle a sentirse más seguro de ello.

DNSSEC actúa como una barrera hermética para los datos de los nombres de dominio, ayudándole a verificar que se está comunicando con el servicio o el sitio web correctos.

Con el tiempo, la validación de DNSSEC formará parte de los sistemas operativos y será un componente estándar de las infraestructuras de redes.

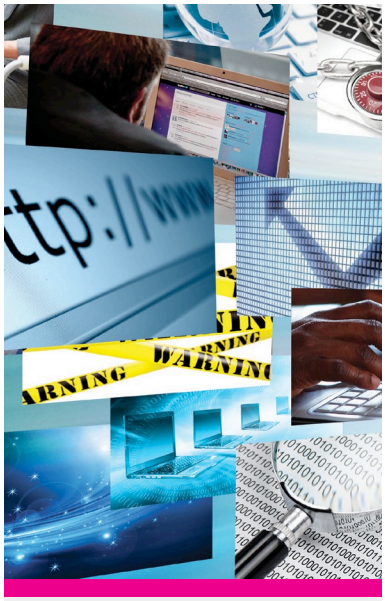
Son pocas las tecnologías que resulten más críticas para el funcionamiento de Internet que el Sistema de Nombres de Dominio (DNS). Las extensiones de seguridad DNS Security Extensions (generalmente conocidas como DNSSEC) permiten a los usuarios tener más confianza en las actividades en línea que se están convirtiendo, cada vez más, en parte de nuestra vida, trabajo, hogar y escuela. DNSSEC actúa como una barrera hermética para los datos de los nombres de dominio, ayudándole a verificar que se está comunicando con el servicio o el sitio web correctos.

¿Qué es DNSSEC?

Antes de que se conecte a un sitio web, su navegador utilizará el DNS para obtener una dirección IP del sitio web que haya escogido. Sin embargo, un atacante podría interceptar su solicitud de DNS y proporcionarle información falsa que le llevaría a un sitio web falso en el que usted podría potencialmente facilitar información personal (por ejemplo, si cree que está accediendo al sitio web de su banco). DNSSEC asegura que usted recibe exactamente la información que publica el propietario del nombre de dominio.

DNSSEC proporciona un nivel de seguridad adicional para que su navegador pueda comprobar y verificar que la información DNS no ha sido modificada. No neutraliza todas las amenazas (nada puede lograrlo), pero proporciona un componente recio para obtener una seguridad adicional de los datos, y no solo en relación con el DNS, sino también en las aplicaciones y servicios relacionados con éste. Por ejemplo, DNSSEC permite el uso del protocolo DANE, que puede añadir un nivel superior de seguridad a los certificados TLS/SSL para el comercio electrónico y garantizar un acceso seguro a los sitios y servicios.

Tenga en cuenta también que DNSSEC NO es exclusivamente para su uso en la web. También puede utilizarlo cualquier otro servicio o protocolo de Internet. Existen ya usos interesantes de DNSSEC con el correo electrónico (SMTP), la mensajería instantánea (IM) y las aplicaciones de voz sobre IP (VoIP).



Acerca de la Internet Society.

Internet Society es una fuente independiente y fiable de información y liderazgo sobre Internet en todo el mundo Con su visión basada en importantes principios y bases tecnológicas, Internet Society promueve el diálogo abierto sobre políticas, tecnología y desarrollo futuro de Internet entre usuarios, empresas, Gobiernos y otras organizaciones. Internet Society trabaja con sus miembros y Capítulos de todo el mundo para permitir la evolución y el crecimiento continuados de Internet para todo el mundo.

Ponga de su parte: Implemente DNSSEC en su(s) Nombre(s) de Dominio.

Al firmar su dominio con DNSSEC entran en juego dos componentes:

1. El registrador de su nombre de dominio necesita poder aceptar los registros de Delegación Firmante (DS) y poder enviarlos a un dominio de nivel superior (TLD), como .com, .org o .net.
2. El proveedor de hospedaje de DNS que opera los servidores de nombres de dominio para su dominio debe ser compatible con DNSSEC y poder firmar (y volver a firmar) sus archivos de zona DNS.

Ciertos registradores desempeñarán ambos papeles para usted. En otras ocasiones, los registros de DNS para su dominio pueden hospedarse en otro proveedor, o también puede hospedarlos usted mismo en sus propios servidores DNS.

Ponga de su parte: Utilice DNSSEC.

Como usuario final, cuenta con varias opciones para verificar que está utilizando DNSSEC:

- Su servidor de DNS local (de su ISP o su red local) puede ejecutar una “validación DNSSEC” y bloquear automáticamente los sitios con firmas DNSSEC incorrectas.
- Como alternativa, puede instalar un servidor validador de DNS en su equipo local.
- Puede añadir soporte de DNSSEC directamente en un navegador web.

Con el tiempo, la validación de DNSSEC estará integrada en los sistemas operativos y será un componente estándar de la infraestructura de redes. Pero hasta que llegue ese momento, estos son los pasos que puede seguir si usted es hábil en las tecnologías y le interesa la seguridad.

Consiga ayuda.

El programa Internet Society Deploy360 Programme proporciona información sobre la implementación de DNSSEC real y de IPv6, entre otros. Deploy360 supera la brecha entre los procesos estándares de IETF (Fuerza de Tareas de Ingeniería de Internet) y la adopción final de esos estándares por parte de la comunidad de operaciones globales. Deploy360 crea y promueve recursos que son fáciles de entender y sencillos de ejecutar por parte de
los profesionales de TI para la implementación de nuevas tecnologías y estándares como IPv6 y DNSSEC.

Visite www.internetsociety.org/deploy360/dnssec para más información, incluyendo la página de “Información básica” y los proyectos específicos que le ayudarán a iniciarse en DNSSEC.