El Informe de Amenazas CCN-CERT IA-21/13 puede descargarse en el portal del CERT Gubernamental: www.ccn-cert.cni.es

Riesgos y Amenazas del BYOD, nuevo informe público del CCN-CERT

- **Conocer los riesgos, amenazas y vulnerabilidades existentes en el fenómeno del *Bring Your Own Device* (BYOD) es uno de los principales objetivos de este documento.**
- **Los Informes de Amenazas del CCN-CERT (IA), tanto públicos como de acceso restringido, se enmarcan dentro de la labor que tiene encomendada de divulgación de las mejores prácticas sobre seguridad de la información.**

Madrid, 5 de noviembre de 2013. El **CCN-CERT**, del Centro Criptológico Nacional (CCN), ha hecho público su Informe de Amenazas, **IA-21/13 de Riesgos y Amenazas del *Bring Your Own Device* (BYOD)**, en el que se adentra en este fenómeno que define la posibilidad de que los empleados de una organización usen los dispositivos de los que son propietarios para desarrollar sus funciones profesionales, accediendo al entorno, servicios y datos corporativos. Esta tendencia al alza que, si bien produce beneficios para ambas partes (organización y trabajador), no está exenta de numerosos riesgos y amenazas para los sistemas de información corporativos, así como ciertos condicionantes legales que no pueden pasarse por alto en la Política de Seguridad de un organismo o empresa que decida, conscientemente, permitir la implantación de este concepto en el funcionamiento de su organización.

¿Qué es BYOD?, Oportunidades versus Riesgos, Amenazas y Vulnerabilidades, Mejores Prácticas en la implantación de un sistema BYOD, así como Soluciones MDM (*Mobile Device Management*) son algunos de los apartados de este documento que hace especial referencia a las **Guías CCN-STIC 457** (Herramientas de Gestión de Dispositivos Móviles) y **450** (Seguridad en Dispositivos Móviles).

El Informe hace especial hincapié en la importancia de desarrollar una **Política de Seguridad BYOD**, acompañada de un adecuado **plan de divulgación y sensibilización** para que todos los niveles de la organización (incluidos, por supuesto, los altos directivos) conozcan los riesgos para la seguridad de la información corporativa, sean conscientes de la necesidad de soporte TI para gestionar una diversidad de dispositivos, aplicaciones y software y, sobre todo, tengan muy presente el incremento del riesgo de sufrir ciberataques.

Sobre CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó a finales del año 2006 como el CERT gubernamental/nacional, y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de la Administración y de empresas pertenecientes a sectores designados como estratégicos.

La misión del CCN-CERT es, por tanto, contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a las Administraciones Públicas y a las empresas estratégicas, y afrontar de forma activa las nuevas ciberamenazas.

MÁS INFORMACIÓN

Centro Criptológico Nacional
Argentona, 20
28023 Madrid www.ccn-cert.cni.es
eventos@ccn-cert.cni.es