El Centro Criptológico Nacional hace pública la Guía CCN-STIC 827 de Gestión y Uso de Dispositivos Móviles

Cómo utilizar de forma segura los dispositivos móviles

- **Los dispositivos móviles (smartphones y tablets, singularmente) se han convertido en un blanco fácil para los ciberataques, tanto por su uso masivo para fines personales o profesionales, como por la ausencia de medidas de seguridad por parte de los usuarios. Todo ello pese a que requieren medidas adicionales frente a otro tipo de equipos como ordenadores de sobremesa o portátiles.**

- **La Guía está disponible en el portal www.ccn-cert.cni.es, junto con más de 200 documentos de recomendaciones, normas y procedimientos en materia de ciberseguridad.**

Madrid, 4 de junio de 2014.- En el año 2016 se espera que existan en todo el mundo 1.600 millones de dispositivos móviles inteligentes. Este incremento espectacular en su uso, no está siendo acompañado, sin embargo de las medidas de seguridad necesarias (la inmensa mayoría de usuarios no realizan ninguna de las precauciones básicas como contraseñas, software de seguridad o back up de archivos para sus dispositivos móviles). Por este motivo, el **CCN-CERT**, del Centro Criptológico Nacional, **CCN**, adscrito al Centro Nacional de Inteligencia, **CNI**, ha hecho pública su ***Guía CCN-STIC 827 de Gestión y Uso de Dispositivos Móviles*** en la que analiza la problemática derivada del uso de estos equipos, particularmente dentro de las organizaciones. El CERT Gubernamental Nacional ofrece, además, una serie de recomendaciones a tener en cuenta, tanto en el uso personal como profesional de estos dispositivos (y muy especialmente por todas aquellas Administraciones Públicas que deben cumplir con el Esquema Nacional de Seguridad).

Entre los riesgos señalados se encuentran:

- **Movilidad:** su uso en múltiples lugares (organización, domicilio particular, lugares públicos, hoteles…) favorece el extravío o hurto, con el consiguiente acceso no autorizado al dispositivo y/o a la información almacenada o transmitida, instalación de código dañino en las aplicaciones móviles, etc.
- **Contenidos y aplicaciones no confiables**: tanto en su configuracón como en su uso. Descargas fuera de la web o tienda oficial, acceso a contenidos como QR (*Quick Response Codes*), que suelen contener direcciones URL imposible de detectar si son o no maliciosas, etc.

4 de junio de 2014

- **Redes inseguras**: redes públicas o redes privadas comunes, en donde es imposible disponer de mecanismos para controlar la seguridad. Permite ataques de tipo *man-in-the-middle* (intercepción de la comunicación entre dos puntos al modificar los datos en tránsito sin el conocimiento de las partes).
- **Interconexión con otros sistemas** (portátil, ordenador…) para sincronizar cotenidos o con un tercero a través de wi-fi, lo que provoca almacenamiento de datos en ubicaciones no confiables, el intercambio no autorizado de datos o transmisión de infecciones con malware de uno a otro equipo.
- **Servicios de localización** a través de sistemas GPS, en coordinación con otros (redes sociales, navegación, …) lo que afecta a la privacidad del usuario y de su relación con la la organización, facilitando la creación de mapas geográficos de movimientos y de actividad.

Algunas recomendaciones

- Activación de las características de seguridad del propio dispositivo
- Autenticación de acceso al dispositivo y a los recursos corporativos accesibles a través de él.
- No almacenar información sensible o, en su defecto, cifrarla .
- Uso de redes privadas virtuales (VPN), autenticación mutua y desactivación de interfaces de red, no utilizando redes wi-fin inseguras.
- Permitir sólo descargas provenientes de "listas blancas", con los permisos estrictamente necesarios y a través de pasarelas web seguras.
- Sensibilización de usuarios.

Sobre CCN-CERT, CERT Gubernamental Nacional

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 en el año 2006 como el **CERT Gubernamental** español 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 ENS.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es 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 los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN
CCN-CERT
eventos@ccn-cert.cni.es

LinkedIn

4 de junio de 2014