ágoraSIC Centro de Conocimiento en Ciberseguridad

¿Cómo van a evolucionar los ciberataques en 2017?

La revista SIC ha formulado esta pregunta a 107 organizaciones (empresas y centros de servicio públicos y privados), que constituyen el grueso del sector de oferta de Ciberseguridad en España. De sus contestaciones puede deducirse que, además de aumentar las tipologías ya vistas en 2016 y años anteriores, la IoT entra con fuerza como objetivo de los atacantes y con ella sectores hasta ahora no especialmente "trabajados" por la delincuencia.

* Es posible obtener una versión en pdf de este especial rellenando el formulario disponible en www.revistasic.com

CCN
Javier Candau
Jefe del Departamento de Ciberseguridad

1. "Los asociados al **ciberespionaje** (tras las elecciones en EE.UU. algunos de estos ataques han tenido mucho eco mediático aunque los mismos se vienen sufriendo durante años en las AAPP y empresas estratégicas) con actores esponsorizados por estados; los orígenes y la complejidad de los mismos es muy diversa y lamentablemente nuestras organizaciones no están preparadas para responder a los mismos. Además, se espera mayor variedad de ataques sobre plataformas móviles de personas clave en las organizaciones antes mencionadas.

2. Los relacionados con el **cibercrimen**; se espera que incremente su actividad y selectividad hacia objetivos más rentables en la infección mediante variantes de ransomware, variantes de código dañino para medios de pago, la "estafa del CEO" (CEO Fraud) y ataques complejos al sector financiero, denegaciones de servicio distribuidas usando internet de las cosas y venta de servicios a terceros (redes de botnets, herramientas de ataque,…)

3. Los relacionados con **grupos hacktivistas**, tanto de origen nacional como internacional; continuarán los ataques por denegación de servicio y las desfiguraciones. Además, hay que tener en cuenta la permanencia/aparición de identidades con elevadas capacidades técnicas para ejecutar acciones de alto impacto por razones ideológicas y el uso de código dañino para extorsión.

4. Con relación al **ciberyihadismo**, se mantendrá limitado a la propaganda y a la presencia de identidades en redes sociales, así como la realización de ataques no complejos contra objetivos de bajo perfil. Eventualmente se podrían aprovechar errores de la parte defensiva y la asociación o contratación de capacidades relacionadas con el cibercrimen.

Desde el punto de vista defensivo se debe mejorar en la capacidad de vigilancia de las redes ante ataques complejos, en la configuración segura de los dispositivos móviles y su monitorización, en la configuración segura de los dispositivos Internet de las cosas (IOT) y en la vigilancia de los sistemas de control en general (plantas industriales, sistemas de distribución, sistemas de salud, edificios…) pues la seguridad no se ha considerado ni en su diseño ni en su implementación. Es además necesaria incrementar la concienciación de los usuarios en el uso de los dispositivos y los elementos conectados a Internet".