La seguridad de las TIC

La Agenda Digital es uno de pilares de la Estrategia Europa 2020 de la Comisión Europea. En ella se propone explotar mejor el potencial de las tecnologías de la información y la comunicación (TIC) para favorecer la innovación, el crecimiento económico y el progreso.

LUIS MIGUEL GARRIDO
Director de Grandes Cuentas de Administraciones Publicas de Fortinet

Entre las líneas de actuación definidas se encuentra la lucha contra la ciberdelincuencia y la aplicación de medidas relativas a la seguridad de las redes y la información y a la lucha contra los ataques informáticos.

En este marco se crea en 2004 la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), que ayuda a la Comisión Europea y a los estados miembros a prevenir y responder frente a problemas de seguridad en Redes e Información. Desarrolla actividades en 4 áreas: Respuesta ante incidentes (CERT); Protección de infraestructuras críticas (sistemas SCADA, redes interconectadas, cloud computing, botnets,..); Identidad y confianza (eID, Risks and Data Breaches, Privacy and Trust) y gestión de riesgos.

Algunas de estas líneas de actividad están claramente enfocadas a los principales vectores de ataque que se están utilizando en este momento por parte de los ciberdelincuentes, que son:

APTs (Amenazas persistentes avanzadas): ataques dirigidos a un objetivo/organización específica, con un fin muy concreto de robo de información con la que obtener un beneficio económico de algún tipo, que emplean múltiples vectores de ataque (ingeniería social, virus, troyanos, gusanos, exploits zero-day,...) y que son de larga duración y persistentes en el tiempo para que las barreras de seguridad no sean capaces de detectarlos. Aunque hay muchos ejemplos de este tipo de ataques, uno muy relevante y conocido fue el cometido en Operación Aurora, ataque realizado desde China dirigido a compañías de tecnología, de seguridad y contratistas del entorno de Defen-

sa con el fin de ganar acceso y modificar repositorios de código fuente de ciertas compañías

Ataques a aplicaciones Web: aprovechando las vulnerabilidades de las aplicaciones web, que se desarrollan normalmente sin aplicar criterios de desarrollo seguro en el ciclo de vida de las aplicaciones. Esto hace que sean susceptibles a vulnerabilidades tipo XSS (Cross site scripting), inyecciones (de SQL, de comandos, de php, ...), desbordamiento de buffer, malformación el protocolo http o los llamativos defacement, (alterar la imagen de una página Web). En Youtube se pueden encontrar tutoriales para ejecutar este tipo de ataques por parte de casi cualquier tipo de persona.

Ejemplos de este tipo de ataques hay muchos, como robos de tarjetas de crédito de múltiples compañías, los conocidos defacement realizados por Anonymous a Inteco, la DGP, partidos políticos,... También a organizaciones europeas como la OSCE (Organización para la Seguridad y la Cooperación), entre otros.

Ataques DoS: ataques orientados a tumbar un servicio mediante inundación de conexiones. En Abril de 2013 se ha producido el mayor ataque de DDoS registrado hasta la fecha, con picos de 300 Gbps, y que ralentizó las conexiones de internet. El origen estuvo en la inclusión en lista negra por parte de Spamhaus de la empresa de alojamiento Cyberbunker. Numerosos también han sido los ataques de DDoS de Anonymous. En España un ejemplo reciente, también en Abril, ha sido el Congreso de los Diputados, víctima de un ataque de este tipo en el marco de las protestas del 25A.

Ataques a infraestructuras industriales: este es un área realmente crítica, ya que hay en juego vidas humanas. Los sistemas de control de potabilizadoras de agua y depuradoras (muchas veces en manos municipales), de refinerías, centrales nucleares, centrales térmicas, ... son extremadamente sensibles y no siempre están securizados adecuadamente. El ejemplo más relevante y que ha levantado una concienciación importante en las autoridades de todo el mundo fue Stuxnet, una APT dirigida a sabotear los reactores nucleares de Irán. Stuxnet es un gusano capaz de reprogramar autómatas programables y ocultar los cambios realizados.

En España, en el ámbito de las Administraciones Públicas, regulado por el Real Decreto 421/2004, de 12 de marzo, el CNI a través del Centro Criptológico Nacional (CCN) desarrolla diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas. Una de las funciones más destacables del Centro Criptológico Nacional ha sido la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Por otro lado, a raíz de la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, el posterior Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad establece un marco que fija los principios básicos y requisitos mínimos, así como las medidas de protección para implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos. ✱

En España, en el ámbito de las Administraciones Públicas, regulado por el Real Decreto 421/2004, de 12 de marzo, el CNI a través del Centro Criptológico Nacional (CCN) desarrolla diversas actividades directamente relacionadas con la seguridad de las TIC