Nota de actualidad CAP 3/2013

ACTUALIDAD CYBER

CENTRO DE ANÁLISIS Y PROSPECTIVA

En la presente nota de actualidad se enumeran algunas de las cuestiones que vienen acaparando la atención de los medios en las últimas fechas, y especialmente en referencia a las iniciativas que en esta materia se están tomando en Europa y en España

1. Europa

1.1. Centro Europeo de Ciberdelincuencia (EC3)

El 11 de enero de 2013 entró en funcionamiento el nuevo Centro Europeo de Ciberdelincuencia (EC3) para contribuir a proteger a las empresas y a los ciudadanos europeos frente a la ciberdelincuencia.

Las investigaciones sobre los fraudes en línea y sobre los abusos de menores en línea y otros delitos informáticos afectan con frecuencia a cientos de víctimas simultáneamente e implican a sospechosos en diversas partes del mundo. Las operaciones de esta magnitud no pueden llevarse a buen término con la única participación de los efectivos de las policías nacionales.

La actividad del EC3 se centrará en las actividades ilegales en línea de las bandas de delincuencia organizada, especialmente en los ataques dirigidos contra las operaciones bancarias y otras actividades financieras en línea, la explotación sexual infantil en línea y los delitos que afecten a las infraestructuras críticas y a los sistemas de información en la UE.

El Centro también facilitará la investigación y el desarrollo y garantizará el refuerzo de las capacidades de las autoridades responsables de la aplicación de la ley, los jueces y los fiscales; asimismo, llevará a cabo evaluaciones de las posibles amenazas, que incluirán análisis, previsiones de tendencias y alertas tempranas. Con el fin de desmantelar un mayor número de redes de delitos informáticos y de perseguir a un mayor número de sospechosos, el EC3 recopilará y tratará los datos relacionados con la ciberdelincuencia y ofrecerá un servicio de asistencia en materia de ciberdelincuencia a las fuerzas de seguridad de los países de la UE. Además, prestará apoyo operativo a los países de la UE (por ejemplo, contra la intrusión, el fraude, el abuso sexual de menores en Internet, etc.) y aportará conocimientos técnicos, analíticos y de peritaje forense de alto nivel en el marco de investigaciones conjuntas.

La Comisión anunció su intención de crear un Centro Europeo de Ciberdelincuencia en la «Estrategia de seguridad interior de la Unión Europea en acción», adoptada el 22 de noviembre de 2010 por la Comisión. La creación de un Centro Europeo de Ciberdelincuencia (EC3) forma parte de una serie de medidas destinadas a proteger a los ciudadanos de delitos en Internet.

Más información:

https://www.europol.europa.eu/ec3

1.2. Estrategia Europea de Ciberseguridad

La Comisión Europea, junto con la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, ha publicado, el 7 de febrero de 2013, una estrategia de ciberseguridad acompañada de una propuesta de Directiva de la Comisión sobre la seguridad de las redes y de la información (SRI).

La estrategia de ciberseguridad, «Un ciberespacio abierto, protegido y seguro», representa la visión de conjunto de la UE sobre cómo prevenir y resolver mejor las perturbaciones de la red y los ciberataques. El objetivo consiste en impulsar los valores europeos de libertad y democracia y velar por un crecimiento seguro de la economía digital. Se prevén una serie de medidas específicas para reforzar la ciberresiliencia de los sistemas informáticos, reduciendo la delincuencia en la red y fortaleciendo la política de ciberseguridad y ciberdefensa internacional de la UE.

La estrategia articula la visión de la UE sobre la ciberseguridad en torno a cinco prioridades:

- la ciberresiliencia;
- la reducción drástica de la delincuencia en la red;
- el desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (PCSD);
- el desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad;
- el establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales.

La política internacional del ciberespacio de la UE promueve el respeto de los valores europeos esenciales, define las normas sobre comportamiento responsable, impulsa la aplicación al ciberespacio de la legislación internacional vigente, ayudando a los países de fuera de la UE mediante la creación de capacidades de ciberseguridad, y fomenta la cooperación internacional en este ámbito.

La UE ha logrado avances esenciales en la mejora de la protección de los ciudadanos frente a la ciberdelincuencia, entre los que destacan el establecimiento del Centro Europeo de Ciberdelincuencia (IP/13/13), la propuesta de legislación sobre los ataques informáticos (IP/10/1239) y el lanzamiento de una alianza mundial contra los abusos sexuales a menores en línea (IP/12/1308). La estrategia pretende asimismo desarrollar y financiar una red de centros de excelencia sobre ciberdelincuencia para facilitar la formación y la creación de capacidades.

La Directiva sobre la SRI propuesta es un elemento central de la estrategia de conjunto; exigiría a todos los Estados miembros, facilitadores clave de Internet y operadores de infraestructuras críticas —plataformas de comercio electrónico, redes sociales y operadores de servicios de energía, transportes, banca y sanidad— a velar por un entorno digital seguro y fiable en toda la UE.

La propuesta de Directiva prevé un conjunto de medidas, entre las que cabe resaltar las siguientes:

a) los Estados miembros deben adoptar una estrategia de SRI y designar a una autoridad competente en la materia dotada de los recursos financieros y humanos adecuados para la prevención, la gestión y la resolución de riesgos e incidentes de SRI;

b) se creará un mecanismo de cooperación entre los Estados miembros y la Comisión que permitirá difundir alertas tempranas sobre riesgos e incidentes a través de una infraestructura segura, así como cooperar y organizar revisiones por homólogos periódicas;

c) los operadores de infraestructuras críticas de algunos sectores (servicios financieros, transportes, energía y sanidad), los facilitadores de servicios de la sociedad de la información (en particular, tiendas de aplicaciones, plataformas de comercio electrónico, servicios de pagos por Internet, computación en nube, motores de búsqueda y redes sociales) y las administraciones públicas deben adoptar prácticas de gestión de riesgos y comunicar los incidentes significativos de seguridad que se produzcan en relación con sus servicios principales.

La comisaria de la UE responsable de los asuntos de interior, Cecilia Malmström, ha afirmado:

«La estrategia pone de relieve nuestras iniciativas concretas para reducir drásticamente la ciberdelincuencia. Muchos países de la Unión carecen de las herramientas necesarias para rastrear y combatir la delincuencia organizada en Internet. Todos los Estados miembros deben establecer unidades nacionales de ciberdelincuencia efectivas que puedan beneficiarse de la experiencia y el apoyo del Centro Europeo de Ciberdelincuencia (EC3).».

Antecedentes

Los incidentes de ciberseguridad están aumentando en frecuencia y magnitud, son cada vez más complejos y no conocen fronteras. Esos incidentes pueden causar daños graves a la seguridad y la economía. Deben redoblarse los esfuerzos de prevención, cooperación y transparencia en relación con los incidentes en el ciberespacio.

Los esfuerzos previos de la Comisión Europea y de diversos Estados miembros a título individual estaban demasiado fragmentados para poder responder a un desafío que crece día a día.

Datos actuales sobre ciberseguridad

- Se estima que cada día hay 150 000 virus informáticos en circulación y 148 000 ordenadores infectados.
- El Foro Económico Mundial ha estimado en un 10 % la probabilidad de que se interrumpan infraestructuras de información críticas en los próximos diez años, lo que podría causar daños por valor de 250 000 millones de dólares.

- La ciberdelincuencia es responsable de una gran proporción de los incidentes de ciberseguridad. Symantec estima que las víctimas de la ciberdelincuencia pierden a escala mundial alrededor de 290 000 millones de euros al año, mientras que un estudio de McAfee cifra los beneficios de la ciberdelincuencia en 750 000 millones de euros anuales.
- La encuesta del Eurobarómetro sobre ciberseguridad de 2012 reveló que el 38 % de los internautas de la UE ha modificado su comportamiento porque le preocupa la ciberseguridad: el 18 % se inclina menos por comprar en línea y el 15 % se muestra más reacio a utilizar los servicios de banca electrónica. Además, el 74 % de los consultados coincide en que el riesgo de sufrir un ciberdelito ha aumentado, el 12 % ya ha sido víctima de fraude en la red y el 89 % evita divulgar información personal.
- En la consulta pública sobre la SRI, el 56,8 % de los consultados señaló haber sufrido el año pasado incidentes de seguridad en la red con un impacto significativo en sus actividades.
- Entretanto, las cifras de Eurostat revelan que, hasta enero de 2012, solo el 26 % de las empresas de la UE había definido una política formal de seguridad de las TIC.

Más información:

http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

2. España.

2.1. Interior.

Centro Nacional de Excelencia en Ciberseguridad (CNEC).

El CNEC es un centro dependiente del Instituto de Ciencias Forences y de la Seguridad (ICFS) de la UAM dedicado a la formación, entrenamiento, investigación y desarrollo tecnológico de excelencia en materia de ciberseguridad y ciberinteligencia para el incremento de la eficacia de la lucha contra la criminalidad

El CNEC forma parte del proyecto puesto en marcha por la **Dirección General de *Home Affairs* de la Comisión Europea** en 2009.

En julio de 2011 el ICFS optó a este proyecto aunando en su solicitud al Cuerpo Nacional de Policía (Brigada de Investigación Tecnológica), la Guardia Civil (Grupo de Delitos Telemáticos), y al grupo empresarial S21sec.

En la actualidad, el CNEC se encuentra desarrollando cuatro grandes proyectos de formación y entrenamiento:

- Desarrollo de Módulos de Entrenamiento (modalidad presencial y mediante plataforma e_Learning) destinados a las fuerzas de seguridad.
- Implementación de los Módulos de Entrenamiento
- Adaptación a España de los manuales europeos de lucha contra la cibercriminalidad desarrollados por el ECTEG (*European Cybercrime Training & Education Group*)
- Diseño e Implementación de un Programa de Certificaciones para fuerzas de seguridad que permitan acreditar su preparación de forma independiente de la formación recibida y permita dar soporte a análisis y conclusiones en sede judicial. Dicho programa se inspirará en la normativa establecida por la Agencia de Certificaciones de Ciberseguridad del ICFS (ver enlace a la derecha de esta página) Este Programa de Certificaciones no solo se destina a las fuerzas de seguridad españolas, sino también a otros países europeos y de América Latina.

En la actualidad, el CNEC está realizando dos proyectos de investigación y desarrollo cuya finalización está prevista para finales del 2014:

1. Estudio y desarrollo de herramientas de investigación digital para la prevención y lucha contra los delitos tecnológicos
2. Creación del DLAF (*Digital Forensic Laboratory Automation Framework*) un Laboratorio Forense Open Source Automatizado para las fuerzas de seguridad nacionales y europeas.

Más información:

http://cnec.icfs.uam.es/index.htm

2.2. Defensa.

Mando de Defensa del Ciberespacio

El Ministerio de Defensa ha anunciado la creación de este nuevo Mando, que dependerá orgánicamente del Estado Mayor de la Defensa. El ministro de Defensa, Pedro Morenés, lo anunció oficialmente durante el acto de celebración de la Pascua Militar, el pasado 6 de enero.

Según la web Infodefensa (http://www.infodefensa.com/cache_noticias/el-/el-mando-de-ciberdefensa-de-las-fuerzas-armadas-da-sus-primeros-pasos.html), el **Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD)** están dando sus primeros pasos hacia la puesta en marcha efectiva. El **Estado Mayor de la Defensa (EMAD)** ha elaborado ya la Orden de creación y la ha enviado al Ministerio para su análisis y posterior discusión interministerial.

Según dicha fuente, durante su intervención en el Curso sobre Seguridad Nacional y Ciberdefensa organizado por la **Cátedra Isdefe** en la **Escuela de Ingenieros de Telecomunicación** de Madrid los días 21 y 22 de enero, el **capitán de navío Francisco Zea**, jefe de la Sección de Seguridad de la Información CIS del EMAD, señaló que el documento recoge el ámbito de actuación, misión, cometidos, y mando y dependencias del MCCD, cuya creación ordenó el **ministro de Defensa, Pedro Morenés**, en noviembre de 2012.

Zea explicó que este Mando se unirá a las iniciativas que ya están en marcha en las Fuerzas Armadas en el ámbito de la ciberdefensa, como el Centro de Respuesta a Incidentes de las FAS, dirigido a la seguridad de las redes clasificadas, y el Centro de Operaciones de Seguridad de Defensa (COSDEF), para las redes abiertas.

Asimismo, destacó la realización de ciberejercicios anuales y avanzó que el próximo mes de abril se llevarán a cabo unas Jornadas SID (Seguridad de la Información de Defensa).

El capitán de navío también habló del marco doctrinal de la ciberdefensa, en el que se incluyen dos documentos de 2011 –**Visión del JEMAD de la Ciberdefensa Militar** y **Concepto de Ciberdefensa Militar**–, una mención para el impulso de esta área en la **Directiva de Defensa Nacional de 2012** y un **Plan de Acción para la Obtención de la Capacidad de Ciberdefensa**, también de 2012.