

Al contrario de lo que se suele abordar en esta sección, se presentan en esta ocasión los proyectos implantados en el mundo -no sólo en un grupo de trabajo universitario- para desarrollar, potenciar y perfeccionar las técnicas de respuesta a incidentes de seguridad en sistemas informáticos. Se comenzará describiendo las actividades más relevantes de las organizaciones oficiales: el grupo de trabajo europeo TF-CSIRT, promovido por TERENA (organización de las redes académicas europeas), y el FIRST, como organización de ámbito internacional, promocionado por CERT/CC y CIAC entre otros. Igualmente, se mencionarán otras iniciativas más incipientes: la EPCI, organización de CSIRTs privados europeos, y el JRC de la Comisión Europea.

La gestión de incidentes de seguridad

El TS-CSIRT y el FIRST centran sus esfuerzos en la formación de equipos de respuesta a incidentes, con el objetivo de que toda máquina conectada a Internet tenga algún día un CSIRT que se haga responsable de la misma. Por otra parte, las nuevas iniciativas comentadas se preocupan más de la prevención de incidentes, como un medio de reducir los riesgos del uso masivo de la red como soporte a las transacciones comerciales y el desarrollo de la sociedad de la información.

TF-CSIRT (<http://www.terena.nl/task-forces/tf-csirt/>)

El TF-CSIRT nació del programa técnico TERENA (<http://www.terena.nl/tech/ToR.html>), con el objetivo de promocionar la colaboración entre los Equipos de Respuesta a Incidentes de Seguridad en Ordenadores (CSIRT's) en Europa.

El término CSIRT empezó a utilizarse a raíz del registro de la "marca CERT" por el CERT/CC (Centro de Coordinación de Equipos de Respuesta a Emergencias de Ordenadores, con sede en la Universidad de Carnegie Mellon en Pittsburg, EE.UU.), en tanto que TF-CSIRT proviene de Task Force-Collaboration of Incident Response Teams, cuya traducción libre podría ser Equipo de Trabajo para la Colaboración de Equipos de Respuesta a Incidentes Informáticos.

Los objetivos del equipo son los siguientes:

- Proporcionar un foro donde intercambiar experiencias e información entre CSIRTs.
- Establecer servicios piloto para la comunidad de CSIRTs europeos.
- Promocionar estándares y procedimientos para respuesta a incidentes informáticos.
- Asistir en la creación de nuevos CSIRTs y en la formación del personal de los CSIRTs existentes.
- Coordinar otras iniciativas comunes.

Conviene aclarar que el TF-CSIRT tomó el relevo de la antigua iniciativa conocida con el nombre de EuroCERT, que a su vez nació del piloto SIRCE, patrocinado por TERENA.

Ante todo, el TF-CSIRT pone en contacto al personal de los distintos CSIRTs. Esta posibilidad de contactar con otros CSIRTs es única y tremendamente fructífera. Si dejamos de lado todas las iniciativas del TF-CSIRT, estos encuentros siguen siendo sumamente útiles para los CSIRTs involucrados.

Sólo la oportunidad de discutir procedimientos de actuación, comentar casos reales, analizar potenciales problemas y, en general, comentar el estado actual de la seguridad informática ya hacen del TF-CSIRT un éxito indiscutible. Si a todo esto le sumamos las múltiples iniciativas coordinadas que surgen, tenemos una combinación excepcional.

Los distintos CSIRTs dependemos unos de otros para poder solucionar efectivamente incidentes con alcance internacional; por ello y en este marco, simplifica muchísimo las cosas conocer en persona a algún representante del resto de CSIRTs.

A pesar de que, de momento, tan sólo se han llevado a cabo cuatro reuniones, ya hay varias iniciativas en marcha. Entre ellas pueden destacarse las siguientes:

- Incident Taxonomy: Best Current Practice Report
- Incident Object Description and Exchange Format (IO-DEF)
- Trusted Introducer for CSIRTs in Europe
- Clearinghouse for Incident Handling Tools
- Training Workshops for New (Staff of) CSIRTs

Incident Taxonomy: Best Current Practice Report

El objetivo de este proyecto es intentar llegar a un consenso entre los distintos mecanismos de clasificación de incidentes existentes. Hay múltiples maneras de clasificar incidentes, lo que supone un problema para la inter-actuación entre CSIRTs.

Por otra parte, iniciativas para crear un registro común de incidentes, del cual se puedan extraer estadísticas para analizar la evolución de los incidentes a nivel europeo, han fracasado debido a los distintos mecanismos empleados para contabilizar incidentes.

Incident Object Description and Exchange Format (IODEF)

Los incidentes de seguridad informática están siendo cada vez más serios y abarcan múltiples CSIRTs o múltiples dominios, involucrando a varios Equipos de Respuesta a Incidentes (IRTs, Incident Response Teams). Cada CSIRT o IRT emplea sus propios sistemas para coordinar estos incidentes; dichos sistemas tienen sus propios formatos y procedimientos y es complejo y costoso en tiempo mover información de un sistema a otro.

Para solventar este problema creciente se está intenta-

do crear un estándar mediante el cual todos los sistemas empleados para coordinar incidentes puedan comunicarse entre sí. Este estándar (IODEF) permitirá en el futuro exportar toda la información relacionada con un incidente a un formato común que posteriormente pueda ser importado de forma automática en el sistema que emplean otros CSIRTs o IRTs para coordinar sus incidentes. De esta forma se agilizará enormemente la coordinación de incidentes que abarquen más de un CSIRT/IRT.

Este proyecto está actualmente muy avanzado y pronto se podrá ver un piloto en funcionamiento. Los objetivos iniciales de este equipo son:

- Redactar un documento en el cual se plasmen los mecanismos empleados para clasificar los incidentes y técnicas de reporting usadas actualmente por los distintos CSIRTs.
- Redactar un documento que refleje los requisitos funcionales de un objeto Incidente.
- Redactar un documento describiendo la relación entre IODEF e IDMEF desarrollado por IETF-WG
- Recopilar una muestra representativa de reports de incidentes.
- Diseñar un modelo de documento XML y DTD para el modelo de datos del IODEF
- Elaborar una guía de uso recomendado del IODEF.

Trusted Introducer for CSIRTs in Europe

Es necesaria la estrecha colaboración entre los distintos CSIRT para poder solucionar incidentes con alcance internacional. Históricamente esta relación de confianza se basaba en las relaciones personales entre múltiples miembros de los distintos CSIRTs existentes. Sin embargo, este modelo, que ha sido útil hasta nuestros días, empieza a resultar poco versátil. Con un número creciente de CSIRTs no se puede seguir basando esta red de confianza en relaciones personales, es necesario un modelo más evolucionado pero que mantenga el nivel de confianza necesario.

La iniciativa del Trusted Introducer (TI) tiene por objetivo dinamizar esta red de confianza. El TI clasifica los CSIRTs existentes en tres niveles: 0, 1 y 2.

Todo CSIRT o IRT del que se tenga constancia adquiere automáticamente el nivel 0; de esta forma se construye una base de datos de equipos de respuesta a incidentes lo más amplia posible. Esta base de datos es de acceso gratuito para toda la comunidad de Internet y proporciona un punto de contacto donde poder comunicar incidentes informáticos. Esta lista puede ser consultada en la siguiente dirección: <http://www.ti.terena.nl/teams/level0.html>

Este registro a pesar de ser sumamente útil no nos proporciona esa red de confianza necesaria. Para ello está el nivel 2. Cuando un CSIRT desea entrar en la red de confianza debe llevar a cabo toda una serie de pasos en los cuales se analizan los procedimientos del equipo, así como los servicios que ofrece. El equipo del TI analiza toda la información proporcionada y si lo considera apto asciende al equipo a nivel 2.

El hecho de que un equipo pertenezca al nivel 2 proporciona al resto de equipos una medida de la seriedad del mismo. Garantiza que sus procedimientos son adecuados y tiene la infraestructura y recursos humanos necesarios para coordinar incidentes y gestionar información sensible de for-

ma segura.

Puede hallarse una lista de los 16 CSIRTs que actualmente pertenecen al Nivel 2 en: <http://www.ti.terena.nl/teams/level2.html>



Figura 1.- El TF-CSIRT nació del programa técnico TERENA con el objetivo de promocionar la colaboración entre los Equipos de Respuesta a Incidentes de Seguridad en Ordenadores (CSIRTs) en Europa.

Clearinghouse for Incident Handling Tools

La idea es crear un repositorio de herramientas y procedimientos empleados por los distintos CSIRTs. Este repositorio constituirá un único punto al cual acudir para tener acceso a las herramientas que todo CSIRT necesita. No sólo se pretende centralizar la ubicación de las herramientas sino que, además, se incorporará una breve descripción de la misma así como una guía de uso.

No se pretende documentar las herramientas, el objetivo es documentar el uso que un equipo de respuesta a incidentes hace de la misma. Junto con este repositorio de

herramientas está pensado incorporar una colección de procedimientos de actuación característicos de los entornos de respuesta a incidentes.

Toda esta información simplificará la creación de nuevos CSIRTs y ayudará en la formación del personal existente. Se trata de un proyecto que todavía está arrancando.

Training Workshops for New (Staff of) CSIRTs

Finalmente, el último de los proyectos que destacamos en este artículo tiene por finalidad construir el material docente necesario para poder constituir nuevos CSIRTs y formar el personal necesario. Se están creando cursos que cubren los siguientes temas:

- Aspectos legales
- Aspectos organizativos
- Aspectos técnicos
- Aspectos de mercado, y
- Aspectos operacionales.

Esta batería de cursos se está terminando estos días y se espera poder impartir un curso piloto en la siguiente reunión del grupo TF-CSIRT para probar la eficacia del material.

En el poco tiempo que lleva en marcha el TF-CSIRT ya se han obtenido grandes resultados, y confiamos en que el equipo seguirá resultando tan efectivo como hasta el momento. Aprovechamos para invitar a aquellos interesados en el mismo a que se pongan en contacto con el esCERT (<http://escert.upc.es>) para obtener más información.

FIRST

El pasado mes de junio se celebró en Toulouse (Francia) el 13º Congreso anual del Forum of Incident Response and Security Teams (FIRST). Fundado en 1990, el FIRST es el principal foro de coordinación de los diferentes CERTs de todo el mundo.

Una de las actividades nucleares del FIRST es, precisamente, la organización de este congreso anual, donde los diferentes equipos de coordinación de emergencias presentan sus propuestas. Este año ha habido una participación importante, tanto por parte de los más de 90 equipos miembros como por parte de candidatos y entidades interesadas, principalmente de Asia.

Fomento en la creación de CSIRTs

Desde el punto de vista organizativo, el principal objetivo del FIRST es fomentar la creación de nuevos equipos de coordinación de emergencias, tanto de ámbito nacional como en grandes corporaciones multinacionales. En este sentido CERT/CC presentó un completo plan de formación destinado a organizaciones que deseen crear un CSIRT (Equipo de respuesta a incidentes de seguridad informática).

Las recomendaciones del CERT/CC para la creación de nuevos CSIRTs son las siguientes:

- Recopilación de información
- Identificación del ámbito de actuación
- Determinar la misión del CSIRT
- Asegurar la financiación necesaria para realizar las operaciones
- Determinar el rango y niveles de servicio
- Determinar la estructura interna del CSIRT y el modelo organizativo
- Crear un plan de puesta en marcha
- Identificar y obtener recursos necesarios de personal y equipamiento
- Desarrollar políticas y procedimientos operativos
- Anunciar el CSIRT, comunicando su misión y los servicios ofrecidos
- Evaluar el plan de puesta en marcha en función de la respuesta

Como medio de presentación de toda esta información para un nuevo CSIRT se recomienda adoptar el estándar RFC 2350.

Obviamente, todos los CSIRTs tienen como objetivo principal la gestión de incidentes de seguridad informática. Normalmente, además ofrecen otro tipo de servicios relacionados con la seguridad informática que permiten mejorar la financiación de la organización, como por ejemplo:

- Emisión de comunicados y alertas
- Publicación y análisis de vulnerabilidades
- Formación a usuarios y administradores de sistemas
- Instalación y configuración de sistemas de detección de intrusos
- Seguimiento de incidentes
- Auditorías y tests de intrusión
- Consultoría de seguridad
- Desarrollo de productos de seguridad
- Análisis de riesgos

Detección de intrusos y Computer Forensics

Desde el punto de vista técnico, el aspecto que despierta mayor interés es el de la detección de intrusos y el llamado "Computer Forensics", es decir el análisis forense de sistemas comprometidos o "muertos".

Las tecnologías disponibles para la prevención de los ataques, como los cortafuegos, están suficientemente maduras y gozan de una amplia difusión, mientras que las herramientas de detección de ataques, igualmente importantes, no han adquirido aún ese grado de madurez.

La detección de intrusos mediante NIDS conlleva unas limitaciones intrínsecas, ya que para funcionar correctamente necesitan capturar todo el tráfico de la red. Normalmente la instalación de NIDS implica un compromiso de seguridad entre permitir o impedir la inspección del tráfico de la red.

En este sentido, los NIDS no pueden actuar en casos de conexiones cifradas, de segmentación de la red o de cualquier otro tipo de medida de seguridad destinada a impedir el sniffing de la red. Por otro lado, por su propia tecnología los detectores de intrusos de red están limitados a comparar los datos con patrones de ataque conocidos o predeterminados.

Dentro del campo de la detección de intrusos el tema más complicado y que centró la última reunión del FIRST fue el del análisis forense de sistemas. Se ha definido el Computer forensics como: "El proceso de identificación, preservación, análisis y presentación de evidencias digitales de tal manera que puedan ser aceptadas en procesos legales".

El análisis presenta unas dificultades añadidas a la detección de intrusos, ya que no sólo es necesario encontrar indicios de un ataque sino que, además, se necesitan aportar evidencias del ataque, de sus consecuencias, de la fecha y hora en que se produjo y, especialmente, de la identidad real del atacante. Además, todas estas evidencias deben ser presentadas de tal manera que puedan ser evaluadas por jueces y abogados, personas con conocimientos informáticos mínimos, y adecuarse a la legislación vigente en cada país.

La búsqueda de evidencias implica un dilema en el proceso de respuesta a incidencias, ya que si se desea conservar las evidencias de la intrusión, no será posible reinstalar o "parchar" el sistema. Si a esto se une el coste de la propia investigación forense, se ve que la presentación de evidencias informáticas en un juicio puede suponer un gasto excesivo para cualquier orga-

nización.

Una vez aceptado el coste de la investigación y de la inmovilización de los recursos se debe proceder con suma cautela, dada la fragilidad de las evidencias informáticas. Cualquier alteración o modificación de los datos puede suponer la invalidación de la evidencia en el juicio.

Los expertos aconsejan realizar una imagen binaria de los discos afectados y montarla en otra máquina, de tal manera que se puedan investigar los datos sin realizar ninguna modificación de los mismos. En la investigación resultará crucial el análisis de los logs o registros existentes en la máquina y la búsqueda de "Artefactos", termino técnico con el que se designa a todo el software aportado por el intruso en la máquina atacada, como rootkits, troyanos o sniffers.

El análisis de los registros (logs) del sistema de una máquina comprometida debe ser analizado con cautela, ya que pueden haber sido alterados fácilmente por el propio atacante, como medio para borrar sus huellas.

Resulta mucho más útil acudir a sistemas externos de gestión de los logs y a sistemas de integridad de ficheros. Sin embargo estas herramientas no siempre están disponibles ya que requieren de una instalación y configuración previas a producirse el ataque. En cualquier caso es necesario mostrar y registrar la fecha y hora de cada evento de tal manera que sea posible recomponer la secuencia de los hechos.

Finalmente es imprescindible presentar la información de tal modo que sea comprensible por los letrados, y que no deje margen a la interpretación.

Por lo tanto el Computer Forensics se basará en cuatro puntos fundamentales: 1. Identificar, 2. Preservar, 3. Analizar, 4. Presentar.



Figura 2.- La iniciativa del Trusted Introducer (TI) tiene por objetivo dinamizar la red de confianza integrada por los CSIRTs existentes, a los cuales clasifica en tres niveles: 0, 1 y 2.

Desde el punto de vista práctico, en las conferencias se presentaron diversas herramientas destinadas a la realización de este tipo de investigaciones, entre la que destacan The Coroner Toolkit, Foundstone Forensics Toolkit y EnCase. Dichas herramientas permiten trabajar con una imagen binaria del disco, acceder de un modo sencillo a todos los registros, realizar búsquedas de palabras clave en todos los archivos y recuperar información supuestamente destruida (Memoria swap, sectores de disco marcados como borrados, sectores defectuosos, etc...)

EPCI (European Private CERT Initiative)

Este grupo “informal” de CSIRTs privados europeos tiene como finalidad el desarrollo de estrategias comunes de financiación de las actividades de los CSIRTs no soportados por las redes académicas o los gobiernos europeos. Entre sus miembros se encuentran organizaciones independientes, como el esCERT-UPC, asociaciones de usuarios de informática, y CSIRTs de multinacionales, como Alcatel, Siemens o BT.

Hasta el momento ha lanzado dos propuestas de proyectos a la Comisión Europea:

– **EISPP (European Information Security Prevention Program)**

Tiene por objetivo fundamental el desarrollo de una metodología común de gestión de la seguridad informática y los incidentes, orientada fundamentalmente a las pymes europeas. Para conseguirlo se están desarrollando bases de datos de vulnerabilidades y contramedidas contra las mismas en varios países europeos.

– **SABEM (Security Assessment Best-practice Methodology)**

Es un proyecto en el que se pretende definir una metodología común para la evaluación de la seguridad de pymes europeas, siguiendo las recomendaciones de ISO-17799 y BS-7799-2. Estas dos normas, cuya aplicación uniforme resulta difícil, dada su ambigüedad, han sido escogidas como punto de referencia para definir una política de seguridad adecuada para pymes.

Además, se estudiarán los aspectos coste/beneficio de la aplicación de una política de seguridad por parte de una pyme, con el fin de encontrar los puntos de equilibrio más adecuados para cada tipo de empresa.

JRC (Joint Research Center)

Es un centro de investigación multidisciplinar ubicado en Ispra (Italia), donde la Comisión Europea desarrolla proyectos “estratégicos” en diversos ámbitos de la ciencia y la tecnología. En los últimos meses han puesto en marcha actividades orientadas a potenciar la seguridad dentro del marco del programa eEurope:

- Protección de datos : establecimiento de un marco para el desarrollo de normas internacionales, tarea asumida por CEN/ISSS (Comité Europeo de Normalización/Information Society Standardization System).
- Privacidad “on-line” . Identificación de las tecnologías disponibles para potenciar la privacidad de los usuarios y las empresas, atentados contra la misma (perfiles de usuario, seguimiento, invasión de la privacidad), identi-

dad virtual, criterios de privacidad a aplicar, etc.

- Confianza y seguridad en el ciberespacio .
- Frenos de la sociedad de la información , entre los que han identificado la protección de la privacidad.
- Cybercrime , para identificar las líneas de investigación a desarrollar en el futuro para contrarrestar el cibercrimen.

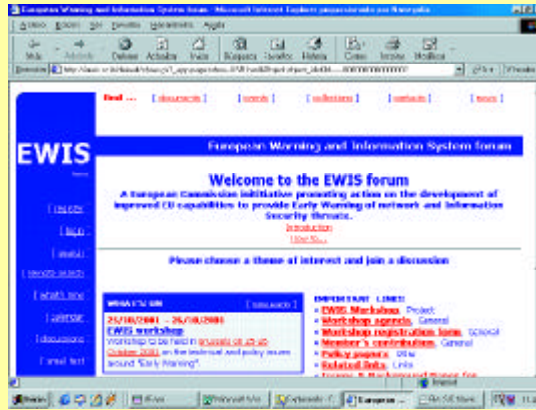


Figura 3.- La EWIS (European Warning and Information System) es una iniciativa para asesorar a la Comisión Europea en el desarrollo de la propia capacidad de la UE para proporcionar alertas “tempranas” de atentados contra la seguridad en la red y los sistemas de información.

EWIS (European Warning and Information System)

La EWIS es una iniciativa para asesorar a la Comisión Europea en el desarrollo de la propia capacidad de la UE para proporcionar alertas “tempranas” de atentados contra la seguridad en la red y los sistemas de información. Pretende confeccionar un “roadmap”, es decir un secuencia de acciones a desarrollar, encaminadas a definir una Política Europea al respecto (<http://ewis.jrc.it/>).

CONCLUSIONES

El desarrollo de sistemas de respuesta a incidentes de seguridad ya es una realidad en el ámbito europeo, a pesar del desprecio con que este objetivo ha sido considerado por la mayoría de las empresas españolas.

Los incidentes de seguridad informática no sólo afectan a los planes de continuidad de operaciones de las empresas, sino que pueden tener consecuencias funestas para las consecuencias de los planes de negocio (robo de información por espionaje industrial, pérdida de credibilidad entre los clientes, etc.) y, además, pueden constituir un delito de negligencia si como consecuencia del mismo se produce una filtración de ficheros de datos personales fuera de la empresa o institución atacada.

Los servicios de inteligencia de los países más desarrollados están utilizando los recursos “sobrantes” de la guerra fría para espiar a las empresas extranjeras que pueden “molestar” al desarrollo de las empresas nacionales, aunque es probable que los últimos atentados terroristas hayan reconducido las “aguas a su cauce” y dichos servicios se concentren nuevamente en investigaciones más orientadas a la “seguridad nacional”.

Por tanto las medidas de protección contra incidentes de seguridad y su adecuada gestión son fundamentales para mantener la “salud” económica de la empresa, y por otra parte, cada día es más fácil obtener la información de otros ordenadores y hay más interés por conseguirla. Prueba de ello son las iniciativas comunitarias para potenciar esta protección no sólo en las grandes empresas, que pueden contar con el apoyo de las grandes consultoras, sino también de las pymes, para las que los costes de subcontratar a una gran consultora son inabordables, y que deberán recurrir a soluciones “pre-fabricadas”, es decir comunes para determinado perfil de empresa u organización. S

- 2 Manel Medina
medina@ac.upc.es
- Óscar Conesa
oconesa@escert.upc.es
- Matías Bevilacqua
matias@escert.upc.es
- EsCERT/UPC
<http://escert.upc.es>