Estrategias de Seguridad en Redes Europeas

Francisco Jesús Monserrat Coll

francisco.monserrat@rediris.es

27 de Mayo, 2004

red.es

Agenda

- Introducción
- El modelo de coordinación en redes Europeas
- Proyectos y actividades resultado de la coordinación
- Acciones Futuras

- Proporciona infraestrura de red y servicios complementarios a la comunidad académica y de investigación española
- Establecida en 1991
- Financiada por el Plan Nacional de I+D+I

Integrada como un departamento con autonomía e identidad propia en el seno de la Entidad Pública Empresarial Red.es

En la actualidad conecta a 233 centros (Universidades, centros publicos de investigación, etc.)

http://www.red.es

Organismo público español encargado del fomento de la sociedad de la información.

- **Reciente creación (2 años)**
- **Agrupa a diversos servicios públicos:**
  - Registo NIC para España.
  - Administración Electrónica
  - Alertas de seguridad http://www.alertaantivirus.es
  - RedIRIS

- Un punto de presencia en cada Comunidad autónomona.
- La gestión a partir de este punto corresponde a cada una de las instituciones

RedIRIS – Servicios

Además de la interconexión y acceso a Internet RedIRIS proporciona diversos servicios a la comunidad científica:

- Coordinación de servicios de Internet
- Celebración de reuniones técnicas con los responsables de las Universidades y Organismos conectados
- Presencia en proyectos Internacionales
- Soporte a grupos de Investigación: listas de correo electrónico, espacio WWW, etc.
- Coordinación de incidentes de seguridad

IRIS-CERT (I)

http://www.rediris.es/cert

- Equipo de atención de incidentes de seguridad de la Red Académica y de Investigación Española (CERT/CSIRT/IRT)
  - Creado en 1995
  - 3 FTE + 1 coordinador técnico

Ámbito de actuación (*constituency*)

- Servicio completo ⇨ Instituciones conectadas a RedIRIS (AS766)
- Servicio limitado ⇨ dominio .es
  - gestión de incidentes y coordinación con otros equipos de seguridad

IRIS-CERT – Servicios Proporcionados (I) -

- Servicios Reactivos
  - *Análisis Forense (sin repercusiones legales)*
  - *Soporte en la Respuesta de Incidentes*
  - *Coordinación con otros equipos de seguridad* ⇨ *dominio .es*
- Servicios Proactivos
  - Observación de tendencias
  - Mantenimiento de herramientas y documentación (WWW/FTP)
  - Enlaces a sitios relevantes de seguridad, otras listas de seguridad y grupos de noticias (en WWW)

IRIS-CERT – Servicios proporcionados -

- Registro de incidentes y generación de estadísticas e informes anuales de actividad
  - http://www.rediris.es/cert/doc/informes/
- Mantenimiento y gestión de una lista de coordinación de seguridad
  - IRIS-CERT@listerv.rediris.es
    - http://www.rediris.es/list/info/iris-cert.es.html

Servicios de Valor Añadido

- Cursos/Ponencias/Presentaciones bajo demanda
  - Grupos de Coordinación de Seguridad dos veces al año
- *Awareness building* (asesoramiento y concienciación de seguridad)

Otros servicios y Grupos de Trabajo

- Gestión y mantenimiento de un Servidor de Claves Públicas PGP ➪ servicio público
  - http://www.rediris.es/keyserver/
- Infraestructura de Clave Pública para la Comunidad RedIRIS (RedIRIS-PKI) ➪ servicio restringido a la comunidad RedIRIS
  - http://www.rediris.es/pki/

- IRIS-CERT puede actuar como punto de contacto entre las instituciones afiliadas y las Fuerzas de Seguridad del Estado
  - Sólo asesoramiento técnico

Relación con la comunidad

- Autoridad compartida

- Es obligatorio disponer de al menos un punto de contacto de seguridad por cada institución afiliada a RedIRIS (servicio completo)
  - Dado por el PER (**P**unto de **E**nlace con **R**edIRIS)
  - Se suscriben a la lista de coordinación de seguridad (IRIS-CERT)
  - Mantenimiento de información de contacto en BBDD interna (LDAP)
- No es obligatorio este punto de contacto para las instituciones con servicio limitado

Relaciones internacionales

- Foros internacionales
  - *TF-CSIRT (Collaboration of Security Incident Response Teams)*

    http://www.terena.nl/tech/task-forces/tf-csirt/

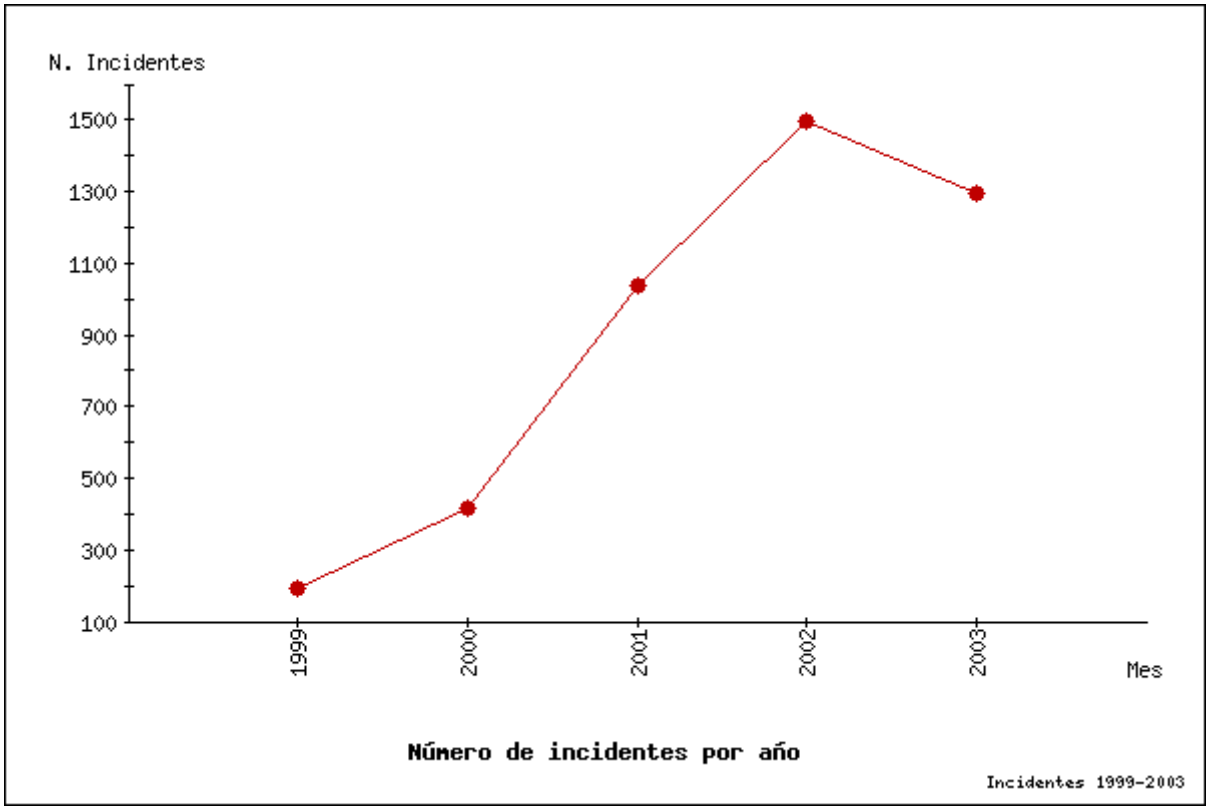
    - CERT-TF (RARE) 1992-1994
    - SIRCE (Security Response Coordination for Europe) 1997-1999
    - CERT-COORD (TERENA) Sep 1999-May 2000
  - FIRST (*Forum of Incident Response and Security Teams*)

    http://www.first.org/

    - 150 equipos miembros de todas las áreas
      - IRIS-CERT es miembro desde 1997
  - Abuse Forum
    - Foro para grupos Abuse e ISPs

Estadísticas 2003 (I)

http://www.rediris.es/cert/doc/informes/2003

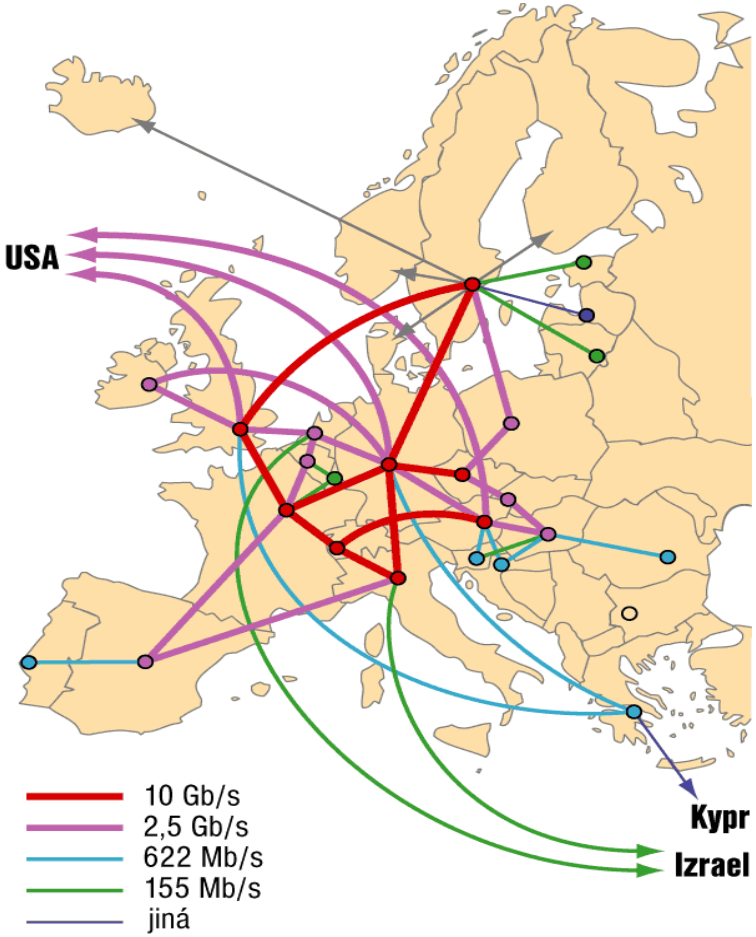


FIRST, http://www.first.org

- Foro de Grupos de Respuesta a incidentes de Seguridad
- Creado formalmente en 1993
- Agrupa a CERT de todo el mundo, con independencia del tipo de Grupo de Seguridad:
  - Proveedores de Internet y redes académicas
  - Grupos de seguridad nacionales
  - Empresas de Seguridad
  - Universidades
  - Etc.

Dos reuniones técnicas al año (miembros) y un congreso

Redes Académicas en Europa



Organización similar en otros países europeos:

- Una red nacional de I+D
- Interconexión de las distintas redes regionales entre si. (Geant)
- Conexión de esta red paneuropea a Internet2 y otras redes de investigación.
- Acuerdos adicionales de conexión de cada red con Carrier y proveedores nacionales.

Coordinación en Europa

DANTE

- Empresa “participada” por las redes academícas
- Encargada de proporcionar interconexión de las distintas redes académicas

TERENA

- Asociación de las redes académicas
- Coordina y apoya diversas inciativas
  - Computación Distribuida (GRID)
  - Midleware (directorios , portales científicos, etc.)
  - Seguridad

Coordinación de Seguridad en Europa

Aprovechando la coordinación a nivel de redes académicas empieza a surgir iniciativas en Europa:

- Reuniones de Grupos de Interés en FIRST
- Reuniones de los precursores de Terena y Dante (1992-1995)
- Congresos comunes.

Gran parte de los grupos de seguridad Europeos hasta el año 1995 eran de redes académicas.

Problema de la coordinación de incidentes en Europa:

- Varias redes académicas, ¿Con quién Contactar ?
- Cuando un incidente involucra a varios redes Europeas, ¿Cómo coordinarlo ?
- Necesidad de fomentar la creación de nuevos CERT

EuroCert

Iniciado como piloto de Terena en Septiembre de 1997 por dos años:

Objetivos:

- Coordinación de incidentes de Seguridad en Europa
- Reducción de la carga de trabajo de los CERT existentes
- Problemas comunes:
  - Zonas Horarias
  - Implicaciones legales
- Punto único de contacto para problemas con Europa
- Financiado por 10 Redes Académicas

EuroCert (II)

Problemas de EuroCert:

- Incremento de Internet,
- Gran parte de los incidentes no involucran a equipos miembros.
- Falta de personal para la gestión de incidentes.

¿Hace falta un “CERT” para toda Europa. ?

- Distintas legislaciones
- Diversos tipos de redes

EuroCert finaliza en el año 1999 por decisión de los organizaciones que contribuían a su mantenimiento.

TF-CSIRT (I)

http://www.terena.nl/tech/task-forces/tf-csirt/

- **Primeras reuniones en Septiembre de 1999. tras la finalización de Eurocert**
- **Necesidad de mantener la coordinación entre grupos de seguridad Europeos.**
- **Aún siendo un proyecto de Terena desde el principio se abre a la participación de otros grupos de seguridad**
  - Proveedores de Internet
  - Grupos de seguridad de los gobiernos
  - Fabricantes
- **Sirve de "incubadora" a proyectos de seguridad que han ido surgiendo.**
  - EISPP
  - Transit
  - eCSIRT.net

TF-CSIRT (II)

Formato:

- Tres reuniones al año
- Abierto a organizaciones ajenas a Terena,
- Reuniones de dos días (ahora tres) en distintos países

Evolución:

- Inicio oficial en Sep 2000
- Incorporación progresiva de nuevos grupos de seguridad
- Puesta en marcha de diversas iniciativas conjuntas
- Mas de 40 grupos de Seguridad en la ultima reunión
- ¿Problemas de crecimiento ?

TI (I)

Trusted Introducer ,http://ti.terena.nl

Primera de las iniciativas puestas en marcha dentro del TI.

Objetivos:

- Creación de un directorio de información de grupos de seguridad Europeos.
- Definir formalmente el cada uno de los grupos de seguridad
- Fomentar la creación de nuevos grupos de seguridad.
- Dos niveles de información

Funciona con un contrato de Terena entre:

- Empresa encargada del TI
- Grupos de seguridad de nivel alto

TI (II)

Acreditación vs Certificación:

- Certificación: Tras una serie de pruebas y requisitos una entidad certifica que se tiene un estado determinado.
- Acreditación: Se comprueba la existencia de determinada información, no su validez.

TI acredita que el CERT se ha definido de acuerdo a una serie de criterios. (RFC 2350)

Tres niveles de grupos:

- 0: se sabe que existe un grupo de seguridad
- 1: Candidato
- 2: Grupo acreditado, ha presentado la información

TI (III)

RFC 2350, Expectation for CSIRT,

Documento que indica que información puede describir un CSIRT

- Nombre del equipo
- Ámbito de actuación (constituence)
- Información de contacto
- Referencias
- Servicios ofrecidos a sus clientes
- Políticas de gestión de información
- Uso de criptografía
- Horarios de trabajo (adicional)
- Personas de contacto

TI (IV)

Proceso de acreditación:

- Se conoce la existencia de un grupo de seguridad y se añade al directorio (nivel 0)
- El grupo solicita su inclusión al nivel 2.
- Se envía la información (paquete de invitación) sobre como definirse (nivel 1)
- El grupo tiene 3 meses para presentar la documentación requerida
- Si se presenta la documentación (y paga la cuota ;-) el grupo pasa a nivel 2

El proceso de acreditación es muy largo, por lo que el TI es mantenido por las aportaciones de los grupos de nivel 2 (720 Euros)

TI (V)

TI proporciona a los miembros de nivel 2, diversos servicios adicionales:

- Listas de coordinación interna
- Acceso a toda la información pública en formato importable a bases de datos
- Mantenimiento de un anillo PGP con la claves de los grupos de seguridad
- Actualización de información en RIPE del objeto IRT

Adicionalmente se buscan nuevos servicios que realice el TI, como resultados de otros proyectos finalizados.

IRT-Object (I)

¿Cómo encontrar el contacto de seguridad para una dirección IP ?

- Registros de Whois,
  - Arin, Estados Unidos http://www.arin.net
  - RIPE, Europa http://ww.ripe.net
  - Lacnic, Latinoamerica, http://www.lacnic.org
  - Apnic, Asia y Oceania, http://www.apnic.org
- Problemas:
  - Información no especifica de seguridad
  - Escasa actualización
  - Direcciones no existentes (SPAM)

IRT-Object (II)

Solución: Crear un nuevo objeto que defina el punto de contacto de seguridad para una dirección IP

- Información de contacto (email, telefono, etc.)
- Claves PGP
- Disponibilidad.

Se define un objeto “IRT” que mantiene esta información y después este objeto se asigna a los rangos IP de los que es responsable.

- Posibilidad de Escalado (IRT “general” y otro más especifico)
- Gestionado directamente por los responsables de los rangos IP o a traves de registros como Trusted Introducer

Incidente de Seguridad típico:

1. Se produce una notificación informal sobre un problema de seguridad.
2. Un IRT crea una alerta de seguridad (correo electrónico) que al final envía a otro CERT indicando:
   - Tipo de ataque
   - Expectativas de respuesta
   - Evidencias
   - Etc
3. El IRT receptor vuelve a procesar esta información para adaptarla a sus necesidades y comunicar el problema al usuario.

IODEF (II)

Como solución surge IODEF (RFC 3067)

- Formato XML para el intercambio de la información
- Completa descripción del incidente de seguridad:
  - Tipo de ataque,
  - Severidad,
  - Evidencias del ataque
  - Etc.

Este objeto se puede incluir de forma automática después por las herramientas de gestión de incidentes de los IRT.

En http://www.ecsirt.net hay información sobre herramientas de manejo de esta información.

European Information Security Promotion Program, http://www.eispp.org

Objetivo: Distribución de información de seguridad a empresas.

- Consorcio de varios grupos de seguridad Europeos.
- Creación de una red de confianza de CERT Europeos para el intercambio de información.

Centrado en la generación de un formato común de definición de avisos de seguridad (XML).

- Varios grupos de seguridad pueden trabajar en el mismo aviso de seguridad.
- Misma estructura y definición de la información.
- Inclusión de referencias a bases de datos de vulnerabilidades externas , CVE, Bugtraq.etc.
- Inclusión en bases de datos.

Transit (I)

Training of Network Security Incident Teams Staff.

http://www.ist-transit.org

Objetivo: Fomentar la creación de nuevos grupos de seguridad en Europa, centrada sobre todo en CSIRT (Respuesta a incidentes de Seguridad)

- Proveedores de Internet
- Redes Académicas
- Empresas de Seguridad

Curso básico sobre:

- Visión General del funcionamiento de un IRT
- Legislación Europea
- Aspectos técnicos (gestión de vulnerabilidades, contactos , etc)

Transit (II)

Financiados por la Unión Europea.

- El alumno solamente paga una parte reducida (alojamiento) del curso.

La documentación ha sido realizada específicamente para estos cursos .

- Disponible la documentación de los cursos.
- Posibilidad de usar los materiales para otros cursos de formación de IRT.
  - No cobrando por ellos.
  - Indicando claramente la autoría del material.
  - Solicitando permiso a la organización de TRANSIT
- En RedIRIS, existe una versión reducida en castellano basada en estos cursos , http://www.rediris.es/cert

eCSIRT.net

The European CSIRT network http://www.ecsirt.net

- **Financiado por la Unión Europea (IST-2001-37558)**
- **Participación de varios grupos de seguridad europeos.**

- **Objetivos:**
  - Recolección de estadísticas de seguridad
  - Creación de una red de alerta temprana
  - Pruebas y ensayos sobre IODEF
  - Definición de un código de conducta

eCSIRT.net (II)

Estadísticas sobre incidentes

- Varios problemas:
  - Interpretación distinta de un mismo incidente de seguridad
  - Falta de mecanismos de recolección automática
- Miden la “carga” de trabajo de los grupos de seguridad.

Estadísticas sobre eventos de seguridad:

- Red de Sensores situados en distintas redes
- Equipos proporcionados por cada organización (y de fuera del proyecto)
- Permiten la correlación de ataques
- Creación de una red de soporte de NTP seguro como soporte

eCSIRT.net (III)

Red de Alerta temprana:

- Definición de mecanismos de alerta:
  - Listas de seguridad encriptadas
  - Sistema telefónico de respaldo
  - Realizadas con éxito pruebas de funcionamiento

IODEF

- Pruebas de intercambio de objetos IODEF
  - ¿Cómo se codifican los mensajes ?
  - Integración en la bases de datos de cada grupo de seguridad
- Desarrollo de herramientas para la creación y manipulación de IODEF.

TF-CSIRT , trabajos en curso (I)

Request Tracker for Incident Response **http://www.bestpracticals.com**

Necesidad de tener una herramienta interna en los CERT para la gestión de los incidentes de seguridad.

RTIR : Modificaciones de RT para adaptarla a la gestión de incidentes de seguridad:

- Busqueda de información sobre direcciones IP
- Creación automática de “incidentes” en base a listados de IP

RTIR se esta empleando por varios grupos de seguridad Europeos, adaptandolo a necesidades comunes:

- Firma / verificación/ encriptación e los mensajes
- Manipulación de los objetos IODEF

Grupo de trabajo dentro de TF-CSIRT sobre RTIR

TF-CSIRT , trabajos en Curso (II)

European Abuse Forum

- **Las diferencias entre grupos de abuse y CERT han ido disminuyendo:**
  - En grandes ISP es distinto.
    - Abuse: Quejas de Acciones realizadas por clientes
    - Cert: Ataques a clientes y sistemas internos
  - Muchas veces es difícil diferenciar:
    - Gusano/Virus que dejan puertas abiertas
    - Máquinas atacadas ,etc

Estas reuniones intentan coordinar a los grupos de abuse y CSIRT

Como Resumen:

- Coordinación a varios niveles:
  - Nacional
  - Europea
- Distintas necesidades pero un problema común
- Unión de esfuerzos
- Participación abierta