Grupos de Seguridad

Francisco Jeśus Monserrat Coll

Murcia, 3 de Abril 2006

Índice

- Alguno de historia
- ¿Para qué hace falta un equipo de Seguridad ?
- Funciones que puede cubrir un equipo de seguridad
- Algunos aspectos esenciales
- Referencias.

Equipos de Seguridad

En 1988 , surge el primer “CERT” en la Universidad Carnegie Mellon, después de que la aparición de un gusano de correo electrónico bloqueara Internet.

Este gusano puso en evidencia varios problemas:

- ¿Cómo notificar a los usuarios la existencia de problemas de seguridad ?
- ¿Cómo ponerse en contacto con los responsables de un equipo ?

.....

Pronto se vio que un “CERT” para Internet no era suficiente

La dimensión global de Internet hizo que en pocos años surgieran varios grupos de seguridad:

- Con una ámbito de actuación más específico
  - ACERT, Equipos del sistema de Defensa Estadounidense
- De soporte de productos específicos:
  - Cisco PSIRT, Soporte a productos de la empresa Cisco
- En distintas localizaciones geográficas:
  - IRIS-CERT, Red Académica Española.

Que formaron FIRST (Forum of Incident & Response Team)

Algunas definiciones

CERT/CC

Computer Emergency & Response Team (Coordination Center)

- "CERT" es una marca registrada por la Universidad.
- No hace referencia expresa a aspectos de seguridad

CSIRT

Computer Security Incident & Response Team

- Termino más ajustado a la situación actual.
- Equipo dentro de una organización encargado responder a los problemas de seguridad

Definiciones (II)

Ámbito de actuación (constituencia) :

- ¿A quién da soporte un grupo de seguridad ?

Inicialmente no se definía exactamente:

- “Usuarios” conectados a Internet

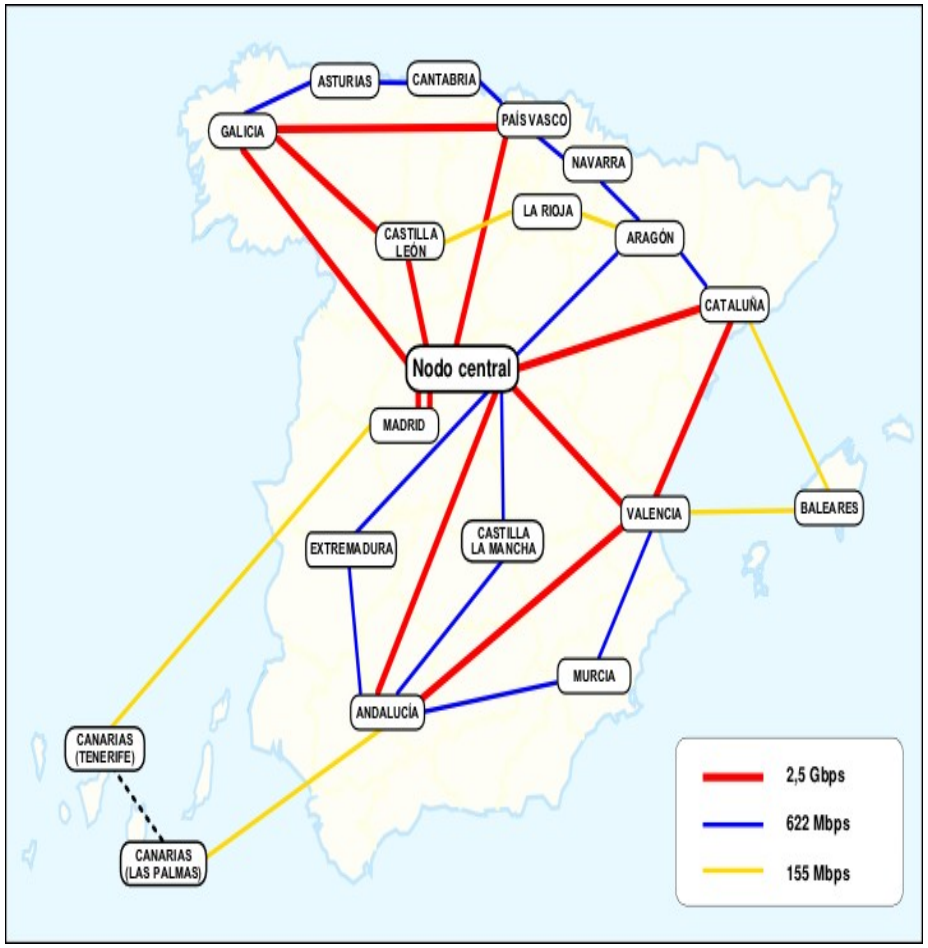
Lo que muchas veces no se ajustaba a la realidad.

- ¿Quién puede “dar soporte” a todos los usuarios de un país ?
- ¿Se tiene autoridad sobre estos usuarios ?

Algunos ejemplos de CSIRT

IRIS-CERT, Red Académica e Investigación Española (RedIRIS)

- Ámbito de actuación:
  - Equipos conectados por RedIRIS (primaria)
  - Punto de contacto con otras redes españolas. (secundario)
- Principales funciones:
  - Solución de problemas de seguridad



IRIS-CERT (II)

Creado en 1995.

Daba soporte limitado a usuarios de Internet en España

- Registro de dominios ".es" por parte de RedIRIS
- Mayor red (1995) IP en España

Soporte limitado a usuarios finales.

- Un contacto de seguridad en cada Universidad/centro I+D conectado a RedIRIS

Además de gestión de incidentes:

- Pilotos de seguridad (PKI)
- Máquinas trampas, IDS, etc.

Algunos ejemplos de CSIRT (II)

CSIRT gubernamentales:

Aparecen a partir del año 2000 para dar soporte a los usuarios de un país:

- Ofrecen servicios de alerta y avisos personalizados en el idioma del país.
- Campañas de concienciación sobre seguridad en internet.
- Coordinación con empresas privadas , proveedores de Internet y otros CSIRT a un nivel nacional.

Algunos ejemplos:

- GOV-CERT, http://www.govcert.nl Holanda,
- ArCERT , http://www.arcert.gov.ar Argentina
- CERT-A, http://www.certa.ssi.gouv.fr (Francia, administración pública)

CSIRT en España

A día de hoy solo existen dos CSIRT en España:

- IRIS-CERT
- EsCERT-UPC

Red.es , E pública española, gestiona un servicio de información sobre virus, http://www.alertaaIntivirus.es

A nivel europeo desde 2005 existe ENISA, agencia europea de seguridad de la información.

Este año se ha credo el Instituto de las telecomunicaciones , INTECO , una de cuyas funciones sera la creación un CSIRT gubernamental en España

¿Para que hace falta un CSIRT ?

Sería la primera pregunta:

- ¿Hay problemas de seguridad que no son solucionados con éxito ?
- ¿se pude hacer algo más ?

- ¿Qué puede hacer un CSIRT ?

¿Quién es la mayor amenaza?

¿Empleados?

- *¿Seguridad h/w & s/w?*
- *¿Firewalls?*
- *¿Anti-virus s/w?*

¿Sabías que?
Datos del DTI indican:*
- *68% han sufrido incidentes maliciosos*
- *Dos terceras partes no tienen políticas de seguridad*
- *57% no tiene plan de contingencia*

¿Clientes/ Estudiantes?

Virus/Worms

LoveBug, CodeRed, Nimda, Slammer,…
Cuestan $1T worlwide
Necesitan del usuario para extenderse
- *Attachments inesperados*
- *Programas innecesarios*

Usuarios descuidados caen

¿Proveedores/Socios?

* UK Department for Trade & Industry Information Security Breaches survey 2004

¿Para qué un CSIRT ?

Para organizar:

2.Autoridad

- ¿Qué puede hacer el equipo y con qué derecho?
- ¿Quién respaldará al equipo cuando las cosas se pongan problemas?

3.Escalamiento

- Ruta jerárquica acordada de antemano
- Para llegar a los directivos, contactos de prensa, administración de riesgos

- Contactos externos (CSIRTs, policía, etc)

2.Usar el esfuerzo de forma efectiva y eficiente

3.Evitar mensajes/acciones contradictorias

Marco de trabajo del CSIRT

Es esencial definir el servicio y prevenir argumentos

Declaración de la Misión

- Liste las actividades que realizará el equipo
- Y que cosas no las hará (y quién las hace)
- Sea realista – Los mejores CSIRTs hacen pocas cosas, pero las hacen bien

Área de trabajo

- A quién le dará el servicio el equipo

Lugar en la organización

Relación con otros equipos

Funciones de un equipo de seguridad

¿Qué es lo que puede hacer un CSIRT ?

¿Qué pude hacer un CSIRT ?

- Manejo de Incidentes
- Alertas y Avisos
- Manejo de Vulnerabilidades
- Manejo de Artefactos
- Anuncios
- Revisión de la Tecnología
- Auditorías/Análisis de Riesgos
- Configuración y Mantenimiento
- Herramientas/Aplicaciones/Infraestructura

- Desarrollo de Herramientas de Seguridad
- Detección de Intrusiones
- Diseminación de Información
- Análisis de Riesgo
- Planeación para la Continuidad de Negocios
- Consultoría de Seguridad
- Construcción de Advertencias
- Educación/Entrenamiento
- Evaluación de Productos

Ninguno Realiza TODO

fuente de CERT-CC (www.cert.org/csirts/)

Distintos servicios

1. **Prevención de incidentes**
   - Advertencias, auditorías, escaneos de puertos/vulnerabilidades, …
2. **Detección de incidentes**
   - Sensores IDS, alertas de firewalls, puntos de contacto, …
3. **Solución de incidentes**
   - Coordinación de incidentes, manejo en sitio, …
4. **Post-procesamiento de incidentes**
   - Castigos (con cuidado), lecciones aprendidas, …
   - Retroalimentación para la prevención de incidentes

Gestión de Incidentes

Es una función esencial para llamarse CSIRT

Puede consistir en cualquiera de:

- Análisis de Incidentes
  - Recolección de evidencia Forense
  - Rastreo/trazado de incidentes
- Respuesta a Incidentes en-sitio
- Apoyo a Incidentes
- Coordinación de Incidentes

Algunos aspectos esenciales

Algunos aspectos esenciales en la creación y funcionamiento de un CSIRT.

- Apoyo de la organización
- Recursos técnicos
- Aspectos de organización.

Apoyo de la organización.

Un CSIRT no es un proyecto que se puede desarrollar sin un apoya directo de las organización a la que da soporte.

- Soporte económico,personal, material, formación etc.
- Responsabilidad y apoyo en las actuaciones del CSIRT.

Ejemplo:

- ¿Qué actuaciones se deben tomar ante una intrusión en un sistema ?
- En caso de de conflictos, entre el CSIRT y otro departamento

¿Cómo se resuelven ?

¿Qué habilidades serán necesarias?

- General: sentido común, comunicación, diplomacia, aprendizaje, trabajo bajo presión, jugador en equipo, integridad, aceptación de errores, solución de problemas, manejo del tiempo,…
- Tecnico: Que corresponda a las actividades que el CSIRT ofrecerá

[Ver artículo del CERT-CC para mayor detalle]

¿Qué validaciones/certificaciones necesita?

- El personal del CSIRT *debe* ser confiable
- Construir la confianza es un proceso largo

Discuta requerimientos de confidencialidad con el equipo y asociados

Apoyo de primer, segundo y tercer nivel

Puede no ser personal de tiempo completo para el CERT

- Puede usar parte del personal existente
- Debe acordar sus deberes y tiempos con los gerentes y el personal
- Las emergencias están por “arriba” de cualquier otra cosa.

Equipos virtuales

- Llame a otros expertos dentro de la organización
- De redes, grupos de sistemas o personal del departamento de IT
- Personal de leyes y PR puede ser esencial

Horas de Operación, etc.

¿Cuándo se proveerá el servicio?

- Horas de Oficina solamente
- Horas Extra (Para emergencias o a nivel más bajo)
- ¿24horas/365días?

¿Cómo se puede contactar al servicio?

- Teléfono: directo o via conmutador
- Sólo e-mail

¿Qué es lo que la organización realmente necesita?

Una vez que se ha definido el servicio, se puede estimar

- Personal requerido
- Experiencia/Habilidad necesaria para proveerlo

¿Qué otros recursos se pueden utilizar?

- Especialistas, mesa de ayuda, legal, prensa etc.
- Acuerdos de trabajo *antes* de las emergencias

¿Qué personal será necesitado para 24x7?

Retención de Personal

- Ofrecer recompensas apropiadas
- Rotación de puestos
- Mantenga el trabajo variado e interesante

El personal del CSIRT manejará material sensible

- Necesita un espacio separado que sea físicamente seguro
- Cuartos, escritorios, lockers necesitan cerraduras
- Computadoras aseguradas, redes y respaldos
- Construya un “lugar seguro” con política de seguridad propia

.

Si se trabaja fuera de horas

- Asegure que el acceso sea posible
- Y que las oficinas sean habitables (comida, agua, calor, etc)

Financiación del CSIRT

El CSIRT debe tener fondos a largo plazo

- No es un proyecto anual que puede detenerse en cualquier momento

Se puede cobrar por los servicios

- Centralizado, por subscripción, por demanda o una mezcla

Planee ser auto-suficiente

- Para servicios internos y externos
- Encuentre servicios que puedan crecer en base a actividades existentes

Publicidad del Equipo

Hágase conocido (fuera y dentro)

- Enlace desde la página Web de Seguridad de la organización
- Utilize conferencias, pláticas, talleres, noticias, etc.
- Vincule Actividades dentro del IRP organizacional

Únase a directorios confiables (para que otros puedan contactarlo)

- Proceso de Acreditación confiable.
- Proceso de membresía de FIRST
- Objeto RIPE IRT

Establezca relaciones de trabajo

- Ej. Con organizaciones de alerta de vulnerabilidades.

Más información

TRANSIT , Training of Network Security Incident Teams Staff, http://www.ist-transit.org

- FIRST y Terena organizan periódicamente cursos de dos días de duración sobre la creación de grupos de seguridad en Europa y latinoamérica.
- Centrados sobre todo en aspectos de organización de un equipo de seguridad.
- Las II Jornadas de seguridad de RedIRIS estuvieron centradas en la creación de grupos de seguridad. http://www.rediris.es/cert/doc/reuniones/fs2004

CERT/CC dispone también de cursos sobre creación de equipos de segurida,d http://www.cert.org

Referencias

- FIRST, **http://www.first.org** agrupa a los distintos grupos de seguridad a nivel mundial , organiza un congreso anual.

- TI, Trusted Introduced, **http://ti.terena.nl**, portal donde aparecen los equipos de seguridad Europeos.

- TF-CSIRT, **http://www.terena.nl/activities/tf-csirt** , reuniones de grupos de seguridad Europeos.

E-COAT, **http://www.e-coat.org** , foro de operadores Europeos.