Grupo de trabajo IRIS-CERT

IRIS-CERT <cert@rediris.es>

17 de mayo de 2001

Actividades de estos GGTT

- Miercoles 9, mañana
  - IRIS-PCA
  - IRIS-CERT
  - Tutorial de seguridad básica
- Miercoles 9, tarde
  - Análisis de ataques (Computer Forensic)
  - DLC sobre Sistemas de detección de intrusos
- Jueves 10
  - Mesa redonda
  - ¿DLC?

Índice

- Resumen de actividad
  - ISPES
  - TI (Europa)
  - Grupos de trabajo
- Estadisticas de incidentes.
- Análisis de los gusanos Unix

ISPES

Reuniones con algunos proveedores de internet para tratar los problemas de coordinación de seguridad.

Buena acogida por parte de los "carriers" mayoritarios en ESPANIX.

Puntos a destacar:

- Los proveedores suelen guardar los logs de llamadas/accesos a la red durante un periodo de 5 años (por motivos fiscales ;-).
- Propuesta de enmmiendas y propuestas sobre correo-e y spam (ver mañana el Grupo de trabajo de IRIS-MAIL
- Proxima creación de un repositorio de puntos de contacto de seguridad de ISP españoles.
- Incorporación de nuevos ISP al grupo de trabajo.

TF-CSIRT

Reuniones de coordinación con otros grupos de seguridad Europeos.

Reunión Barcelona (Enero 2001)

- Grupo de trabajo sobre clasificación (taxonomía de incidentes)
- Grupo de trabajo sobre formato XML de intercambio de incidentes de seguridad
- Propuesta a RIPE de la incorporación de un contacto técnico de seguridad
- Grupo de trabajo sobre formación de Equipos de Respuesta a Incidentes de Seguridad

Proxima reunión a Finales de Mayo en Eslovenia.

Trusted Introduced

Iniciativa para tener centralizada información sobre grupos de seguridad a nivel Europeo y validar la información proporcionada.

http://www.ti.terena.nl

- Categorización de los grupos de seguridad Europeos.
- Aquellos grupos que cumplan una serie de criterios llegan al nivel 2
- Esta valoración es realizada por un equipo independiente

Desde el 23 de Marzo IRIS-CERT obtiene el nivel 2 del TI

Grupos de Trabajo e iniciativas

GTI-AUP: Tras la revisión que se hizo en el plenario de los pasadas JJTT, se esta a la espera de presentar esta política al ministerio.

GTI-SDIR: Nuevo grupo de trabajo sobre sistemas de detección de intrusiones, DLC esta tarde.

Lista CERT-ES: Debate del libro de seguridad en equipos Unix

Grupos de Trabajo

GTI-AUP: Tras la revisión que se hizo en el plenario de los pasadas JJTT, se esta a la espera de presentar esta política al ministerio.

GTI-SDIR: Nuevo grupo de trabajo sobre sistemas de detección de intrusiones, DLC esta tarde.

Lista CERT-ES: Debate del libro de seguridad en equipos Unix

¿Otros DL?

Encuesta

- 11 personas respondieron a la encuesta.
- “Seguridad perimetral” basada en ACL en router
- Bastantes instituciones emplean algún sistema antivirus.
- Desconocimiento de algunas de las listas de RedIRIS
- Poco personal dedicado efectivamente a la seguridad
- Diversidad de S.O.
- Poco empleo de conexiones seguras

Resumen de incidencias de seguridad

Evolución de los incidentes

Incidentes totales desde Noviembre de 2000: 286

Número de incidentes internacionales (tanto origen como destino): 256 (89

- Numero de incidentes con origen internacional: 66 (28%)
- Numero de incidentes con destino internacional: 190 (72%)

Número de incidentes donde están involucradas instituciones afiliadas: 259 (90%)

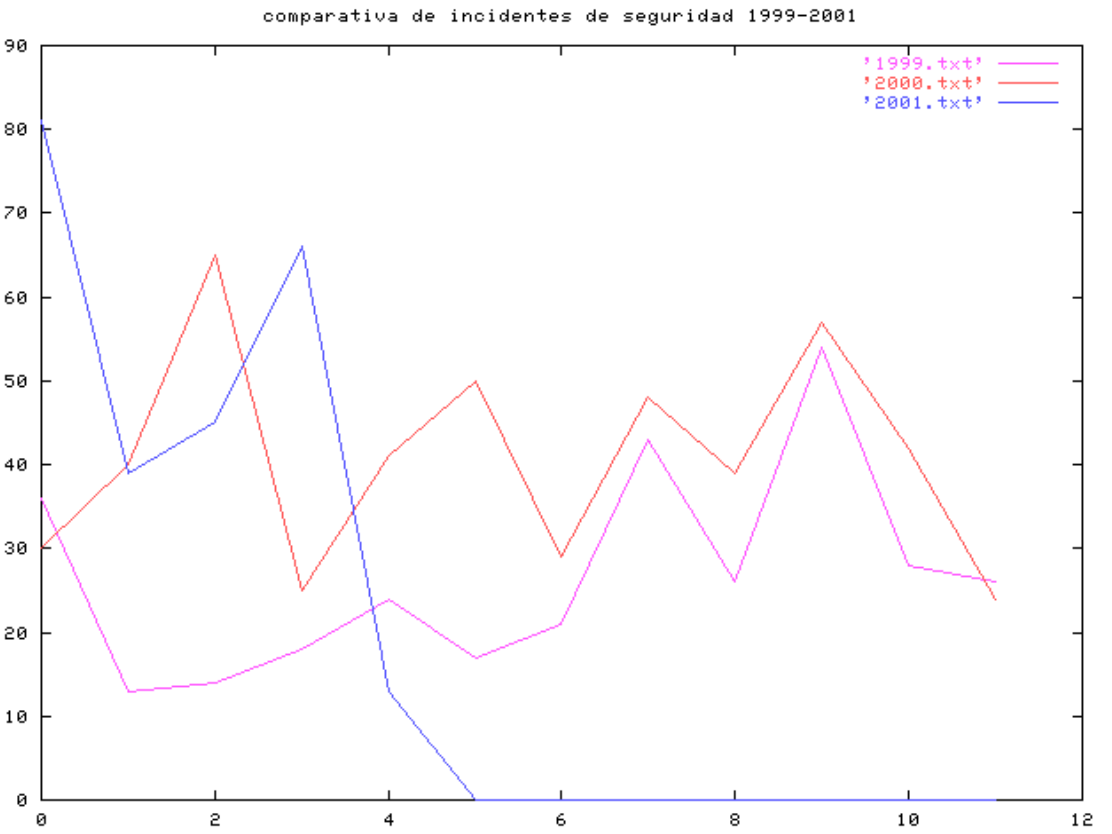
Esto significa que sólo 27 incidente/s involucran a sitios Nacionales no afiliados.

En cuanto al origen de los incidentes, 186 (el 65%) de estos se han originado debido a una queja recibida desde el exterior, mientras que solo 72 (25%) se han generado debidas a un correo recibido desde la institución afiliada

Incidentes por categorias

1. Escaneo de puertos 135 (47%)
2. Acceso a root Vulnerabilidad SO 38 (13%)
3. MAIL SPAM 35 (12%)
4. Otro tipo de incidente 19 (6%)
5. Denegación de servicio con exito 10 (3%)

Evolución incidentes



Comentarios

- Disminuyen los equipos "importantes" de las organizaciones grandes (servidor WWW, correo, etc.)
- Aumentan los incidentes en equipos "aislados": docentes, becarios, etc. no administrados.
- A partir de los primeros gusanos, se genero solo un correo de incidente por máquina origen (bastantes incidentes superaron los 10 correos ;-)
- Hace falta una respuesta más rápida desde los servicios centrales ante este tipo de ataques

EQUIPOS SIN ADMINISTRAR

Incidentes más comunes

- Gusanos de Linux
- Ataques de denegación de servicio (con accesos vía root)
- Escaneos desde el exterior.
- Cambios de páginas WWW (incidentes externos).

¿ PREGUNTAS ?