RESPUESTA A INCIDENTES DE SEGURIDAD

Manel Medina, Jordi Buch

esCERT-UPC, Setiembre 1996

E-mail: cert@escert.upc.es

Hoy, millones de usuarios se aprovechan de las facilidades de intercambio de datos que ofrecen las redes informáticas. Internet es el ejemplo más famoso. "Usar" está relacionado con "abusar". Millares de usuarios abusan de las facilidades de las redes informáticas por varias razones: crimen, venganza, beneficios o entretenimiento. Se deben tomar medidas de seguridad para proteger datos, ordenadores y redes de ordenadores. El área de los sistemas de información, donde seguridad adquiere una especial importancia, entra en conflicto con las características de las redes de hoy -la facilidad de uso y conectividad.

Para reforzar y proteger la seguridad de la información, hoy las empresas, instituciones responsables de redes formulan políticas de seguridad y designan a personas o equipos para mantenerlas. A nivel de seguridad de redes, en Internet existen equipos de seguridad desde 1988. Estos equipos son conocidos como bajo los nombres de CERT ("Computer Emergency Response Team") o IRT ("Incident Response Team").

EQUIPO DE RESPUESTA A INCIDENTES

Un **equipo de respuesta a incidencias** (IRT) es un equipo de personas que llevan a cabo la gestión del incidente. Los proveedores de red, universidades, compañías, etc pueden disponer de sus propios IRTs o delegar a externos. También se les puede designar como CERTs.

Un CERT español debe tener los mismos objetivos que los otros CERTs Europeos y del resto del mundo. El ámbito de actuación ha de abarcar todo el territorio del Estado Español. esCERT-UPC lo abarca, aunque la red académica, debido a su importancia, dispone de Iris-CERT, en ésta hay una actuación conjunta.

El esCERT-UPC basa su actuación en el análisis, recomendación, formación y asistencia a emergencias. Estos servicios están personalizados y sujetos al secreto profesional. Mediante los análisis y las recomendaciones se realiza una auditoría de carácter periódico, mientras que la formación se lleva a cabo en forma de cursos-seminarios.

PREVENCIÓN

Para la prevención de incidentes, esCERT-UPC ofrece un punto de información que contiene una selección de herramientas de seguridad, artículos variados, avisos de seguridad y cualquier otra información relativa a la seguridad en redes de ordenadores.

La formación también se considera una actividad de prevención. esCERT-UPC ofrece unos seminarios sobre seguridad. En éstos, se trata desde como formular una correcta política de seguridad hasta la configuración de un cortafuegos.

GESTIÓN DE INCIDENTES

Nos referimos a **gestión de incidentes** a cualquier acción correctiva o represiva tomada al ocurrir un incidente. Con esta acción debe ser posible minimizar al máximo los efectos del incidente y localizar su origen con la finalidad de prever los futuros.

El proceso de gestión de un incidente se inicia cuando un afectado contacta con esCERT-UPC. También, esCERT-UPC puede dar un aviso a un posible afectado.

COORDINACIÓN DE INCIDENTES

Muchos incidentes no van a salir del marco de una LAN o institución, mientras que en otros se pueden involucrar a varias instituciones, y por lo tanto varios IRTs. Es en este último caso cuando se hace necesaria una **coordinación de incidentes**. El CERT/CC situado en Pittsburgh, USA es el ejemplo más famoso de centro de coordinación de incidentes. En Australia está el AUSCERT, mientras que en Alemania está el DFN-CERT. En España existe el Rediris-CERT y esCERT-UPC, el primero se ve obligado a asumir el papel de centro coordinador debido a la importancia de la red Rediris, mientras que el segundo actúa como equipo independiente con sede en la Universidad Politécnica de Cataluña y dar servicio tanto a la comunidad académica Interne como al resto.

Es necesaria también una coordinación entre los diferentes CERTs. En 1990 se constituyó **FIRST** ("Forum of Incident Response and Security Teams") para coordinar a la variedad de IRTs de organizaciones comerciales, académicas o gubernamentales. FIRST propicia una rápida coordinación y respuesta a incidentes de seguridad. También facilita el intercambio de información entre sus miembros. Actualmente en España no hay ningún miembro de FIRST, pero se prevé que tanto Rediris-CERT como esCERT-UPC sean reconocidos. Para la coordinación de incidentes, se dispone de una lista de puntos de contacto (POC). La POC contiene los datos de los diferentes responsables de seguridad de las diferentes organizaciones, empresas, etc que disponen de conexión a Internet.