Respuesta a incidentes de seguridad de la información

LA MISIÓN PRINCIPAL DEL CCN-CERT ES RESPONDER DE FORMA RÁPIDA Y EFICIENTE ANTE CUALQUIER INCIDENTE DE SEGURIDAD EN LAS ADMINISTRACIONES PÚBLICAS ESPAÑOLAS

CCN-CERT
Centro Criptológico Nacional

Una de las características más destacadas del actual escenario nacional e internacional es, sin duda, el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. De hecho, la expansión de la denominada Sociedad de la Información lleva implícito el que, cada vez más, la información se transmita, se procese y se almacene en algún momento en un sistema. Este hecho, unido a que a través de los sistemas todos somos capaces de manejar una mayor cantidad de información en menos tiempo, ha contribuido a conferir una gran importancia a la información propiamente dicha, que es considerada como un valor en sí misma.

Como tal valor, la información manejada en un sistema pueda estar sometida a distintos tipos de **amenazas**, entendiendo como tal cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica en un sistema de las TIC resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio sistema. Estas amenazas van a introducir, en el manejo de la información, un determinado nivel de **riesgo**. Así, existe riesgo cuando se transmite información por un canal de comunicaciones porque alguien no autorizado podría estar interesado en conocerla (amenaza) y el canal de comunicaciones tiene **vulnerabilidades** (debilidad o falta de control que, llegado el caso, permitiría o facilitaría que una amenaza actuase contra un objetivo o un recurso del sistema). De hecho, conviene reseñar que un canal de comunicaciones es, en la mayoría de los casos, intrínsecamente inseguro.

> Su objetivo principal es "contribuir a la mejora del nivel de seguridad de los sistemas de información en las AA.PP. de España"

También se introduce un nuevo factor de riesgo con la interconexión entre sistemas. Al permitirse que la información sea accesible desde un sistema, aunque físicamente esté almacenado en otro, este acceso se produce, en ocasiones, sin que el propietario de la información tenga conciencia de ello, amenazando la confidencialidad, disponibilidad o integridad de la información. La implantación generalizada de las redes corporativas y el uso de Internet han contribuido a empeorar la situación en este sentido.

De hecho, las amenazas y vulnerabilidades que afectan a los sistemas de información han venido aumentando constantemente en los últimos años, llegando incluso a incrementarse un 55% en los dos últimos años, según datos recogidos por el CCN-CERT.

Respecto a los tipos de riesgos que estas vulnerabilidades implican para nuestros Sistemas de Información, según publica el CERT® Coordination Center, la mayoría de las amenazas recibidas constituyen casos de cibercrimen o ciberdelincuencia, de tal forma que se han convertido en una debilidad

crítica en las naciones occidentales, máxime si tenemos en cuenta que estas amenazas evolucionan continuamente: virus, phising (ataques que utilizan ingeniería social y subterfugios técnicos para robar credenciales de la identidad de consumidores), defacement (cambio de aspecto de un servidor Web, generalmente con fines de protesta, políticos o vandálicos), etc.

Respuesta de las Administraciones Públicas

Precisamente para que las Administraciones Públicas (estatal, autonómica y local) puedan responder de forma adecuada a estos incidentes de seguridad, el Centro Criptológico Nacional creó a principios de este año 2007, su Capacidad de Respuesta a Incidentes de Seguridad, CCN-CERT. De hecho, su objetivo principal es "contribuir a la mejora del nivel de seguridad de los sistemas de información en las AAPP de España", siendo su misión "*ser el centro de alerta y respuesta de incidentes de seguridad, ayudando a las Administraciones a responder de forma más rápida y eficiente ante las amenazas de seguridad que afecten a sus sistemas de información*".

Así pues, y siendo su principal función la respuesta ante incidentes, los procedimientos de gestión de incidentes son clave para ofrecer este servicio del CCN. Entre los aspectos y procedimientos más destacables en el proceso de gestión de incidentes se encuentran los siguientes:

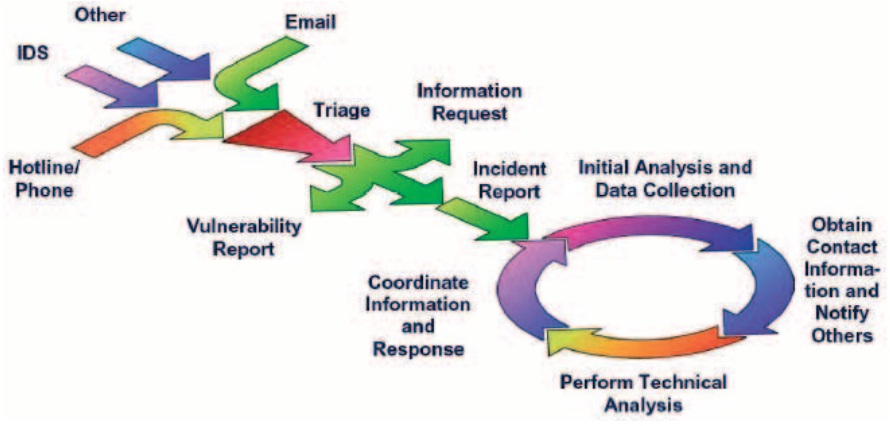
- Recepción y evaluación del incidente (confirmar que se trata de un incidente, si es urgente su resolución, así como un proceso de ordenación, categorización y priorización de los informes entrantes).
- Registro, identificación y análisis de todo lo que vaya sucediendo, automatizando todo lo que sea posible. Esta tarea será esencial, entre otras cosas, para aprender de la experiencia y generar estadísticas e informes de gran valor posterior.
- Notificación inicial y en el momento en que exista una mayor información a todas las personas identificadas como esenciales para la resolución del incidente.
- Escalado por tipo de incidente o nivel de servicio, en función de la nueva información disponible.
- Contención para evitar daños mayores, acordando con los responsables de los sistemas afectados las acciones a tomar para ciertos tipos de incidentes.
- Recopilación de evidencias que permitan una posterior acción legal, en caso necesario.
- Asistencia para la recuperación del sistema y de los datos a un estado seguro y menos vulnerable.

Ataque de Denegación de Servicio

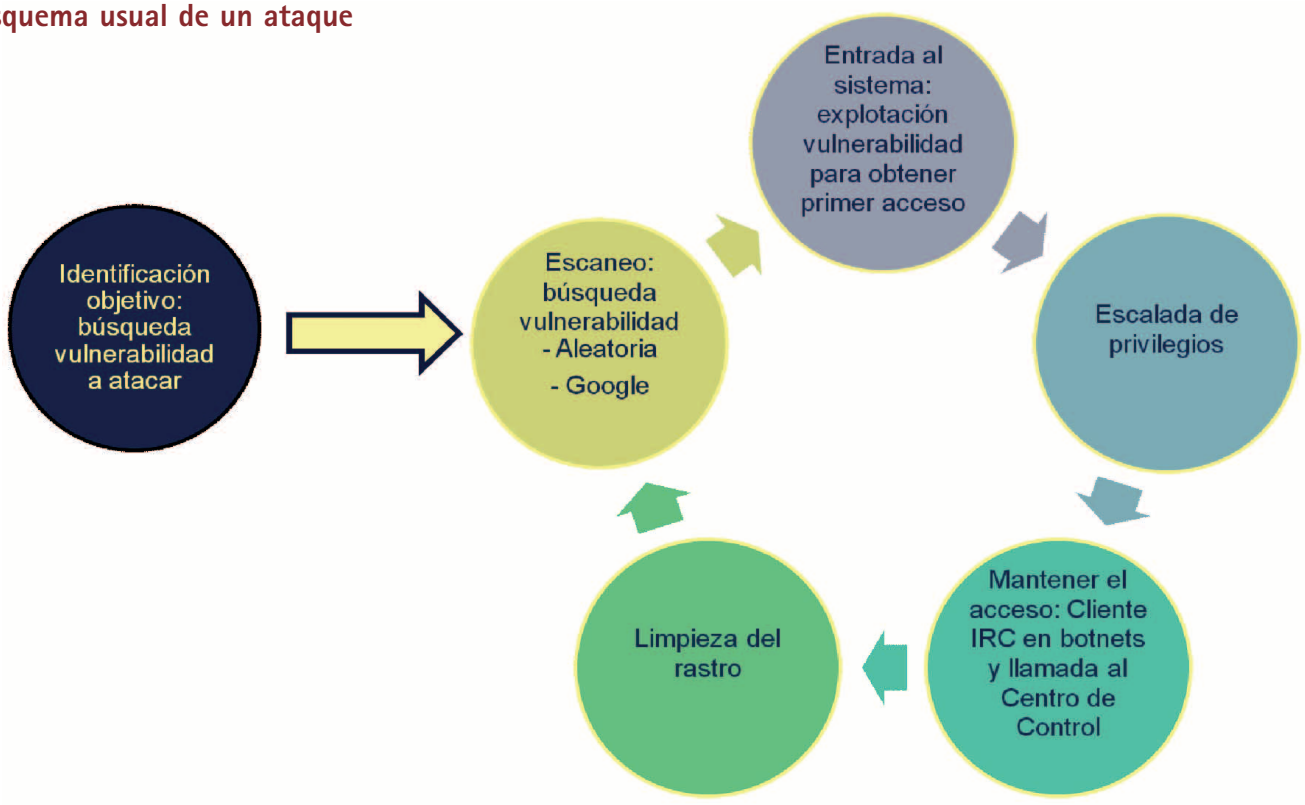
Uno de los tipos de incidente que mayor incremento está teniendo en los últimos tiempos es el denominado Ataque de Denegación de Servicio o DDoS (*Distributed Denial of Service*). Mediante este tipo de ataques se pretende privar intencionadamente a los usuarios legítimos de un recurso o servicio que proporciona un sistema, sobrecargando ese sistema con una avalancha de paquetes de datos desde múltiples fuentes. Los autores del ataque crean normalmente una situación de denegación de servicio (DoS), bien interrumpiendo el canal de comunicación con el servidor (consumiendo su ancho de banda) o bien echando abajo el servidor o reduciendo considerablemente su eficacia. Esto puede conseguirse aprovechando una vulnerabilidad en el servidor o consumiendo sus recursos (memoria, disco duro, etc.).

> Las amenazas y vulnerabilidades que afectan a los sistemas de información han venido aumentando constantemente en los últimos años

Ciclo de vida de un incidente



Esquema usual de un ataque



Los ataques de DDoS suelen estar motivados por distintas causas: extorsión, rivalidad entre empresas o entre países, venganza, combinación con phishing o propaganda.

En este sentido juegan un papel fundamental las denominados BotNets (roBot Networkd); es decir, un grupo de ordenadores comprometidos o infectados (zombis) que utilizan código malicioso y que están, en último extremo, bajo control remoto de un hacker denominado "bot master" o "bot herder".

Los botnets son la principal herramienta para realizar este tipo de ataques puesto que se componen de una gran cantidad de ordenadores (en el orden de miles) que juntos acumulan un ancho de banda que puede inundar los grandes anchos de banda de sus víctimas. Como las botnets están tan dispersas resulta muy difícil conseguir cerrarlas.

El problema radica en la gran dispersión de la botnet (zombis repartidos por todo el mundo) con una gran cantidad de ISPs involucrados, países, idiomas, zonas horarias, etc) y en la gran discreción conseguida por el atacante, que normalmente utiliza un elevado número de máquinas interpuestas entre él y su víctima, así como en la existencia de redes de servicios que facilitan el anonimato del tráfico. En consecuencia, el tiempo necesario para desactivar una botnet es muy elevado y requiere de un gran esfuerzo de coordinación (tratar con diversos proveedores, ...) y un grado de conocimiento muy elevado (tipos de ataque, técnicas de análisis forense de sistemas, etc.).

Por ello, la participación de un CERT en la resolución de este tipo de incidentes (como el CCN-CERT en el caso de ser alguna administración pública española el objetivo del ataque) representa una magnífica ayuda para su resolución dada la coordinación existente entre este tipo de equipos con los del resto del mundo y, además, por el alto perfil de formación que suele caracterizar a sus responsables.

No hay que olvidar, asimismo, que las predicciones apuntan a que durante este año 2007 la cifra de delincuentes informáticos con una motivación de tipo económico irá en aumento. Por tanto, cualquier organización con presencia en Internet, bien sea pública o privada, tiene que ser consciente del incremento del riesgo de este tipo de ataques. De hecho, los planes de seguridad de la información deben tener muy en cuenta este tipo de amenaza, familiarizar a su personal de seguridad con los motivos y los métodos que utilizan los autores de ataques DDoS y mantener, en el caso de la Administración, un contacto directo y fluido con el CCN-CERT para gestionar de forma rápida y eficiente este tipo de incidentes. De lo contrario, estos ataques podrían convertirse en un problema creciente que se escape de nuestro control.