LT06: CUALIFICACION DE INCIDENTES GRAVES FORO ABUSES

Introducción

La gestión y actuación ante incidentes de abusos por parte de las organizaciones que operan en Internet, se está convirtiendo, cada día más, en una tarea indispensable para el buen funcionamiento, tanto de éstas, como de la red en general. Para que esta labor resulte eficaz, es necesaria la coordinación entre organizaciones en materia de gestión de incidentes. Esta coordinación es aún más importante cuando los incidentes a gestionar se pueden definir como incidentes graves, en cuyo caso dicha actuación coordinada debe ser mucho más eficaz.
Este documento recoge una propuesta, a suscribir por los miembros del Foro ABUSES (http://www.rediris.es/abuses/), tanto de cualificación de incidentes graves como de una serie de puntos que sirven como base para una cooperación eficaz en la gestión de dichos incidentes.

Definición de incidentes graves

Se puede definir incidente como cualquier problema relacionado con la seguridad de un sistema informático o red de comunicaciones que permite la comisión de abusos por parte de los usuarios de este sistema o red y en el que se ven involucrados un par origen-destino diferentes.
Dentro de esta definición , y a efectos de este documento, se define como incidente grave todo aquel que pueda causar en el receptor del incidente o en el ISP asociado, un daño de índole moral o económica a corto o medio plazo.
Se consideran incidentes graves, aquellos que cumplen la definición formulada anteriormente y que además pertenecen a una de las siguientes categorías:

- **Phishing**. Término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir de forma ilícita datos personales. Principalmente estos datos están relacionados con claves para el acceso a servicios bancarios y financieros, realizándose esta petición a través de correos electrónicos que facilitan el acceso a páginas web que imitan la imagen o apariencia de una entidad o empresa de reconocido prestigio.
- **SPAM**. Envío de mensajes no solicitados por el receptor, habitualmente de tipo publicitario. Aunque se puede realizar por distintas vías, la más utilizada entre el público en general y la que nos inetersa en esta cualificación, es la basada en el correo electrónico.
- **Malware o programa malicioso**. Programa o archivo, cuyo objetivo es el dañar un sistema informático y que está pues diseñado para insertar en los mismos virus, gusanos, troyanos, etc.., intentando conseguir algún objetivo (desde el más inocuo al mas dañino).
- **Intentos de intrusión**. Cualquier incidente que constituya un intento de acceso (con éxito) a un sistema o red informática ajeno y para el cual no se tiene autorización. Normalmente estos intentos de intrusión de deben a la existencia de vulnerabilidades no parcheadas en los sistemas o redes de comunicación y al uso de passwords débiles.

Procedimientos de detección y cualificación de incidentes graves

La detección de incidentes por parte de un operador, se puede realizar por distintas vías, siendo la más típica la recepción de una denuncia por correo electrónico desde el exterior, ya sea desde un particular, un sistema automático u otro operador. La notificación de un incidente, se puede realizar por otros mecanismos (dependiendo de los habilitados por el operador) entre ellos teléfono, fax, etc..
Además de estos métodos de detección basados en avisos, la detección de posibles

problemas o incidentes graves se puede realizar de forma interna, mediante la utilización de los sistemas de monitorización y alerta implementados en el operador.
Por otro lado, es posible que un operador detecte incidentes, por distintas vías, relativas a IPs que no estén bajo su responsabilidad, pero si bajo la responsabilidad de otro operador adscrito al foro ABUSES. En este caso, deberá ponerse en contacto con los responsables de dichas IPs tan pronto sea posible, utilizando los contactos, tanto públicos como privados disponibles (más información en al siguiente apartado “Procedimientos de notificación”).
Una vez detectada una incidencia, el primer paso a realizar es la verificación de la veracidad de la misma. Una vez comprobada su veracidad, se procederá a su cualificación, utilizando lo niveles de prioridad definidos en el propio operador, teniendo en cuenta que si el problema detectado encaja en la definición dada en el apartado anterior, y se categoriza en una de las categorías anteriores, el incidente será marcado como grave y necesitará pues una atención especial.
Sea cual sea el procedimiento de detección de incidencias graves, la reacción de un equipo abuses antes un incidente de este tipo debe ser diligente, activando todos los mecanismos disponibles y que la legislación española permita, para su resolución en el menor tiempo posible y teniendo en cuenta las recomendaciones dadas en los siguientes apartados de esta propuesta.

Procedimientos de notificación

La notificación de un incidente grave se deberá realizar simultaneamente por dos conductos:

- A través del buzón de abusos habilitado por cada ISP. Así habrá constancia de ese abuso en las bases de datos internas del ISP.
- A través del contacto personal del ISP publicado por el Foro. Se evitará que esas reclamaciones o notificaciones se pierdan en el conjunto de todas las recibidas.

Para permitir una identificación rápida de este tipo de incidentes graves, que por lo tanto necesitan de una atención especial, se deberá incluir en el Asunto del mensaje remitido la referencia **[urgente <tipo de incidencia>]**. Donde <tipo de incidencia> corresponde al tipo de problema a tratar (SPAM, Phishing, Malware, Intrusión).
La notificación, si así lo requiere el caso, se podrá realizar por una vía más rápida, por ejemplo por telefóno, utilizando la información privada publicada en el Foro si está disponible o la pública si ésta no lo está.
Las notificaciones a enviar deberán incluir la prueba del abuso (incluyendo una descripción del problema en cuestión):

- SPAM. Cabecera de correo con fecha, hora, huso horario y cuerpo del correo enviado. Con esto se puede determinar, en el caso de que el ISP disponga de direcciones IP dinámicas, quien utilizaba una IP determinado en el momento del envío del SPAM.
- Phising: Para poder verificar la autenticidad del phising se debe incluir la dirección URL donde está alojada la página fraudulenta. De este manera, se podrá comprobar en todo momento si el phising sigue o no activo y en una dirección IP del ISP.
- Malware: Para los virus que se expanden por correo es necesario saber el Asunto del correo, el fichero adjunto si lo tuviera o cualquier dato que nos permita identificar al virus. Para otro tipo de malware, se debe especificar una descripción del mismo así como cualquier evidencia que permita su identificación, incluyendo si es posible el binario en sí para su análisis y estudio.

- Intentos de Intrusión: Se deberá aportar la línea del LOG del sistema de detección en el que está reflejado la fecha, la hora, el huso horario y la

Efectivamente no he introducido nada en el doc. hasta que no estuviera consensuado con el resto de los participantes.

- puerta utilizada para la intrusión. Los primeros campos permitirán detectar quién utilizba una IP concreta en un momento determinado en el caso de direcciones IP dinámicas.

Todos los operadores que suscriban esta política deben comprometerse a:

- Mantener el asunto del incidente, incorporando su código de seguimiento y manteniendo el código del ISP origen de la denuncia para facilitar las futuras comunicaciones relativas al mismo.
- Confirmar la recepción del incidente, mediente un acuse de recibo.
- Gestionar la incidencia de forma prioritaria, tomando las medidas pertinentes que estén al alcance del operador, informando al origen de la denuncia de las medidas adoptadas, así como actualizando con la información que se disponga hasta su cierre y solución definitiva.
- Poner a disposición de los interesados en cualquier momento cualquier información nueva disponible de que se disponga y que permita acelerar las investigaciones y resolución de los casos.

Aunque lo descrito aquí es de aplicación ante incidentes graves, es más que recomendable que exista coordinación en materia de incidentes entre los ISPs españoles, avisandose de potenciales problemas, fundamentalmente si estos ISPs pertenecen al foro ABUSES.

Definición de tipos de respuesta recomendados ante incidentes graves

Una vez recibida e identificada una notificación de un incidente grave, se debe actuar con diligencia, priorizando su resolución ante otro tipo de incidencias con categorizadas como graves.

Si el caso así lo requiere, se tomarán las medidas de emergencia adecuadas para evitar que el problema se siga produciendo, con el consiguiente perjuicio de los usuarios/ISPs afectados. Estas medidas incluyen:

- SPAM. Bloqueo de las IPs pertinentes a nivel de MTA, firewall o ACL en los routers de acceso, según corresponda. En el caso de que el ataque se origine desde gran cantidad de IPs y no sea posible su filtrado como se recomienda más arriba, será necesario analizar el/los mensaje/s en cuestión para encontrar patrones en los mismos que permitan la elaboración de reglas especificas en lso servidores.
- Phishing. Desactivación o bloqueo de la página fraudulenta (bloqueo a nivel de aplicación Web).
- Malware. Bloqueo de la máquina infectada (firewall, ACLs) para impedir que el malware se siga distribuyendo e infectando nuevas máquinas.
- Intentos de intrusión. Bloqueo de la máquina origen de la intrusión a nivel de firewall o ACL en los routers de acceso.

Una vez tomadas estas medidas de urgencia, es necesario que se realice una investigación exhaustiva del caso (análisis forebse), intentando determinar las causas del mismo, los puntos de fallo aprovechados para conseguir el efecto causado, así como cualquier evidencia que permita determinar el origen real del ataque. Estas investigaciones tienen un doble objetivo; por una parte, investigar estos casos graves con el fin de aprender de la experiencia, lo que nos permitirá asegurar mejor nuestros sistemas en el futuro (siempre que sea posible, la información obtenida por dicha investigación deberá ser compartida en la lista asociada al Foro ABUSES). Por otra parte, un segundo objetivo incluye la detección de cualquier evidencia que permita determinar el origen real del ataque (dirección IP), para proseguir la investigación en dicha dirección.

Si se obtiene información sobre el origen real del ataque, el proveedor deberá ponerse en contacto con los puntos de contacto pertinentes relacionados con dicha red, sobre todo si esa IP pertenece a un ISP en el Foro ABUSES (aunque no sólo en este caso).

Si el incidente ha sido de tal gravedad que fuera necesaria la intervención de las fuerzas de seguridad del estado. La recopilación de evidencias se deberá realizar siguiendo las directrices que marquen dichos cuerpos, para que las evidencias recogidas puedan servir como pruebas ante un posible juicio.

Una vez realizada la investigación, se debe resolver el problema en cuestión, poniendo las medidas apropiadas para que dicho problema no se vuelva a producir.

Si es necesario, y el sistema lo permite, se aconseja la reinstalación de la máquina atacada, para asegurarnos que el agujero ha sido tapado completamente. Esto es especialmente importante cuando el atacante ha conseguido acceso a una cuenta privilegiada y no se puede determinar con seguridad lo que el atacante ha modificado/incluido en la misma.
Dependiendo de la criticidad del sistema comprometido la fase de restauración del servicio/máquina (disponibilidad de sistemas de backup en el caso de los servidores) estará sujeta a determinadas restricciones. En cualquier caso, se debe actuar con diligencia y rapidez, informando convenientemente a las partes implicadas de las medidas adoptadas y la causa del problema detectado.

Mecanismos de automatización (o aceleración) de la respuesta

Aspectos legales

Propuesta de aceptación "universal" entre los operadores de dicha definición

Inclusión en la Política de Uso Aceptable de todos los proveedores (lo que supone la adhesión a las conclusiones)

Adhesión de instituciones/organizaciones (CATA, RED.es, Bancos, etc)

Publicidad