CONSIDERACIONES SOBRE LA DEFINICIÓN DE UN PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD

Álvaro Gómez Vieites
agomezvieites@gmail.com
Profesor de la Escuela de Negocios Caixanova

RESUMEN DE LA PONENCIA

En esta ponencia se analizan los principales aspectos que se deberían tener en cuenta para definir e implantar un Plan de Respuesta a Incidentes de Seguridad en los sistemas informáticos.

Para ello, en primer lugar se revisa la importancia adquirida por la Seguridad de la Información, y se realiza una breve revisión de las principales consecuencias que podría tener para una organización la falta de una adecuada Política de Seguridad de la Información.

Seguidamente, se describen de forma detallada los principales aspectos a tener en cuenta a la hora de definir e implantar un Plan de Respuesta a Incidentes:

1. Constitución de un Equipo de Respuesta a Incidentes.
2. Definición de una Guía de Procedimientos.
3. Detección de un incidente de seguridad.
4. Análisis del incidente.
5. Contención, erradicación y recuperación.
6. Identificación del atacante y posibles actuaciones legales.
7. Comunicación con terceros y relaciones públicas.
8. Documentación del incidente de seguridad.
9. Análisis y revisión “a posteriori” del incidente

Por último, se describirán las prácticas recomendadas por el CERT/CC para mejorar la respuesta de una organización ante los incidentes de seguridad informática.

1. LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

Muchas de las actividades que se realizan de forma cotidiana en los países desarrollados dependen en mayor o menor medida de sistemas y de redes informáticas. El espectacular crecimiento de Internet y de los servicios telemáticos (comercio electrónico, servicios multimedia de banda ancha, administración electrónica, herramientas de comunicación como el correo electrónico o la videoconferencia…) ha contribuido a popularizar aún más, si cabe, el uso de la informática y de las redes de ordenadores, hasta el punto de que en la actualidad no se circunscriben al ámbito laboral y profesional, sino que incluso se han convertido en un elemento cotidiano en muchos hogares, con un creciente impacto en las propias actividades de comunicación y de ocio de los ciudadanos.

Por otra parte, servicios críticos para una sociedad moderna, como podrían ser los servicios financieros, el control de la producción y suministro eléctrico (centrales eléctricas, redes de distribución y transformación), los medios de transporte (control de tráfico aéreo, control de vías terrestres y marítimas), la sanidad (historial clínico informatizado, telemedicina), las redes de abastecimiento (agua, gas y saneamiento) o la propia Administración Pública están soportados en su práctica totalidad por sistemas y redes informáticas, hasta el punto de que en muchos de ellos se han eliminado o reducido de forma drástica los papeles y los procesos manuales.

En las propias empresas, la creciente complejidad de las relaciones con el entorno y el elevado número de transacciones realizadas como parte de su actividad han propiciado el soporte automatizado e informatizado de muchos de sus procesos, situación que se ha acelerado con la implantación de los ERP, o paquetes software de gestión integral.

Por todo ello, en la actualidad las actividades cotidianas de las empresas y de las distintas Administraciones Públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad.

De ahí la gran importancia que se debería conceder a todos los aspectos relacionados con la seguridad informática en una organización. La proliferación de los virus y códigos malignos y su rápida distribución a través de redes como Internet, así como los miles de ataques e incidentes de seguridad que se producen todos los años han contribuido a despertar un mayor interés por esta cuestión.

Podemos definir la Seguridad Informática como "cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema".

Desde un punto de vista más amplio, en la norma ISO/IEC 17799 se define la Seguridad de la Información como la preservación de su confidencialidad, su integridad y su disponibilidad (medidas conocidas por su acrónimo "CIA" en inglés: "*Confidentialy*, *Integrity*, *Availability*").

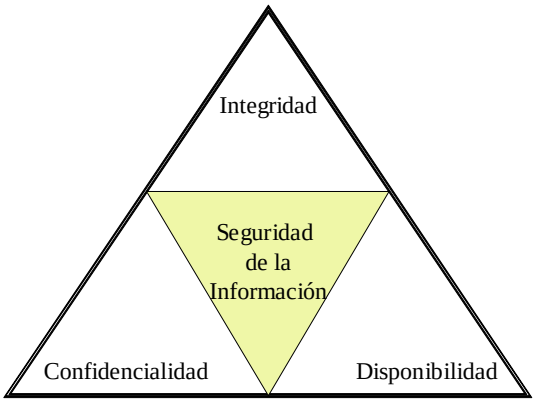

Figura 1: Seguridad de la Información según la norma ISO/IEC 17799

Por "**Incidente de Seguridad**" entendemos cualquier evento que pueda provocar una interrupción o degradación de los servicios ofrecidos por el sistema, o bien afectar a la confidencialidad o integridad de la información.

Un incidente de seguridad puede ser causado por un acto intencionado realizado por un usuario interno o un atacante externo para utilizar, manipular, destruir o tener acceso a información y/o recursos de forma no autorizada. Aunque un incidente también podría ser la consecuencia de un error o trasgresión (accidental o deliberada) de las políticas y procedimientos de seguridad, o de un desastre natural o del entorno (inundación, incendio, tormenta, fallo eléctrico...).

En España, la Ley Orgánica de Protección de Datos define una incidencia como "cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos", en el contexto de los ficheros con datos de carácter personal.

2. POSIBLES CONSECUENCIAS DE LA FALTA DE SEGURIDAD

A la hora de analizar las posibles consecuencias de la ausencia o de unas deficientes medidas de seguridad informática, el impacto total para una organización puede resultar bastante difícil de evaluar, ya que además de los posibles daños ocasionados a la información guardada y a los equipos y dispositivos de red, deberíamos tener en cuenta otros importantes perjuicios para la organización:

- Horas de trabajo invertidas en las reparaciones y reconfiguración de los equipos y redes.
- Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos: coste de oportunidad por no poder utilizar estos recursos.
- Robo de información confidencial y su posible revelación a terceros no autorizados: fórmulas, diseños de productos, estrategias comerciales, programas informáticos…
- Filtración de datos personales de usuarios registrados en el sistema: empleados, clientes, proveedores, contactos comerciales o candidatos de empleo, con las consecuencias que se derivan del incumplimiento de la legislación en materia de protección de datos personales vigentes en toda la Unión Europea y en muchos otros países.
- Posible impacto en la imagen de la empresa ante terceros: pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de

confianza por parte de los clientes y los proveedores, etcétera.

- Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del servicio, pérdida de oportunidades de negocio...
- Posibles daños a la salud de las personas, con pérdidas de vidas humanas en los casos más graves.
- Pago de indemnizaciones por daños y perjuicios a terceros, teniendo que afrontar además posibles responsabilidades legales y la imposición de sanciones administrativas. Las organizaciones que no adoptan medidas de seguridad adecuadas para proteger sus redes y sistemas informáticos podrían enfrentarse a penas civiles y criminales bajo una serie de leyes existentes y decisiones de tribunales: protección de la privacidad y los datos personales de clientes y empleados; utilización de aplicaciones P2P para intercambio de contenidos digitales protegidos por derechos de autor; etcétera.

Según un estudio publicado a principios de 2006 y realizado por la consultora especializada Computer Economics, la creación y difusión de programas informáticos maliciosos a través de Internet (virus, troyanos, gusanos…) ha representado durante esta última década un coste financiero para las empresas de todo el mundo de unos 110.000 millones de dólares.

En otro estudio realizado en esta ocasión por el FBI, se ponía de manifiesto que casi un 90% de las empresas de Estados Unidos habían sido infectadas por virus o sufrieron ataques a través de Internet en los años 2004 y 2005, pese al uso generalizado de programas de seguridad. Estos ataques habían provocado unos daños por un importe medio de unos 24.000 dólares en las empresas e instituciones afectadas. Además, según los propios datos del FBI, cerca de un 44% de los ataques provenían del interior de las organizaciones.

Los nuevos delitos relacionados con la informática y las redes de ordenadores se han convertido en estos últimos años en uno de los mayores problemas de seguridad a escala global. Así, según datos publicados por el Departamento de Hacienda de Estados Unidos a finales de 2005, los delitos informáticos (entre los que se incluyen las estafas bancarias, casos de "*phishing*", pornografía infantil o espionaje industrial) constituyen un lucrativo negocio que genera ya más dinero que el propio narcotráfico. Sólo en Estados Unidos estos delitos, unidos a las consecuencias de la propagación de los virus y de los ataques de denegación de servicio, causan pérdidas anuales superiores a los 50.000 millones de euros.

3. TAREAS A CONSIDERAR EN UN PLAN DE RESPUESTA A INCIDENTES

La definición e implantación de un Plan de Respuesta a Incidentes debería tener en cuenta una serie de actividades y tareas, entre las cuales podríamos destacar todas las que se presentan en la siguiente relación:

- Constitución de un Equipo de Respuesta a Incidentes.
- Definición de una Guía de Procedimientos.
- Detección de un incidente de seguridad.
- Análisis del incidente.
- Contención, erradicación y recuperación.
- Identificación del atacante y posibles actuaciones legales.
- Comunicación con terceros y relaciones públicas.
- Documentación del incidente de seguridad.
- Análisis y revisión "a posteriori" del incidente.

3.1. CONSTITUCIÓN DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

El Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, *Computer Security Incident Response Team*) deberá estar constituido por las personas que cuentan con la experiencia y la formación necesaria para poder actuar ante las incidencias y desastres que pudieran afectar a la seguridad informática de una organización.

Generalmente sólo las grandes organizaciones cuentan con un equipo de personas contratadas para cumplir con esta función. En la mayoría de las organizaciones que no cuentan con un Equipo de Respuesta formalmente constituido, será necesario identificar quiénes son las personas responsables de acometer cada una de las tareas que se hayan definido en el Plan de Respuesta a Incidentes, definiendo claramente

las responsabilidades, funciones y obligaciones de cada persona implicada en dicho Plan.

La organización deberá mantener actualizada la lista de direcciones y teléfonos de contacto para emergencias, para poder localizar rápidamente a las personas clave.

En algunos casos será necesario contratar a las personas con la necesaria experiencia y cualificación profesional (conocimientos técnicos, habilidades de comunicación…). La experiencia es un factor determinante para poder actuar de forma correcta evitando errores a la hora de responder de forma rápida y eficaz ante los incidentes de seguridad.

Asimismo, conviene prestar especial atención a la formación continua de los miembros del Equipo de Respuesta a Incidentes (o de las personas que deban asumir esta responsabilidad si no existe el equipo como tal), contemplando tanto los aspectos técnicos como los aspectos legales (delitos informáticos).

Estas personas deben contar con la dotación de medios técnicos y materiales necesarios para poder cumplir con eficacia su misión. Para comprobar la idoneidad de los medios disponibles, el entrenamiento de los miembros del equipo y las actividades definidas en el Plan de Respuesta a Incidentes, conviene llevar a cabo simulacros de forma periódica en la organización.

3.2. GUÍA DE PROCEDIMIENTOS Y ACTIVIDADES A REALIZAR EN RESPUESTA A UN INCIDENTE

Como parte integrante del Plan de Respuesta a Incidentes, la organización debe definir una guía de actuación clara y detallada con los procedimientos y acciones necesarias para la restauración rápida, eficiente y segura de la capacidad de procesamiento informático y de comunicaciones de la organización, así como para la recuperación de los datos dañados o destruidos.

El objetivo perseguido con la Guía de Procedimientos es conseguir una respuesta sistemática ante los incidentes de seguridad, realizando los pasos necesarios y en el orden adecuado para evitar errores ocasionados por la precipitación o la improvisación.

Una buena Guía de Procedimientos permitirá minimizar los daños ocasionados y facilitar la recuperación del sistema afectado.

Además, esta guía debe completar la adquisición de información detallada sobre cada incidente de seguridad para mejorar los procedimientos de actuación ante futuros incidentes y reforzar la protección actual de los sistemas informáticos de la organización.

Por supuesto, también debe tratar de forma adecuada las cuestiones legales que se pudieran derivar de cada incidente de seguridad, así como los aspectos relacionados con la imagen y reputación de la organización y las relaciones públicas.

3.3. DETECCIÓN DE UN INCIDENTE DE SEGURIDAD

La organización debería prestar especial atención a los posibles indicadores de un incidente de seguridad, como una actividad a contemplar dentro del Plan de Respuesta a Incidentes. Seguidamente se presenta una relación de los principales indicadores de posibles incidentes de seguridad:

- Precursores de un ataque: actividades previas de reconocimiento del sistema informático, como el escaneo de puertos, el escaneo de vulnerabilidades en servidores, el reconocimiento de versiones de sistemas operativos y aplicaciones…
- Alarmas generadas en los Sistemas de Detección de Intrusiones (IDS), en los cortafuegos o en las herramientas antivirus.
- Registro de actividad extraña en los "logs" de servidores y dispositivos de red o incremento sustancial del número de entradas en los "logs".
- Aparición de nuevas carpetas o ficheros con nombres extraños en un servidor, o modificaciones realizadas en determinados ficheros del sistema (librerías, kernel, aplicaciones críticas...), que se pueden detectar mediante herramientas de revisión de la integridad de ficheros.
- Caída o mal funcionamiento de algún servidor: reinicios inesperados, fallos en algunos servicios, aparición de mensajes de error, incremento anormal de la carga del procesador o del consumo de memoria del sistema…
- Notable caída en el rendimiento de la red o de algún servidor, debido a un incremento inusual del tráfico de datos.
- Cambios en la configuración de determinados equipos de la red: modificación de las políticas de seguridad y au-

ditoría, activación de nuevos servicios, puertos abiertos que no estaban autorizados, activación de las tarjetas de red en modo promiscuo (para poder capturar todo el tráfico que circula por la red interna mediante "sniffers"), etcétera.

- Existencia de herramientas no autorizadas en el sistema.
- Aparición de nuevas cuentas de usuario o registro de actividad inusual en algunas cuentas: conexiones de usuarios en unos horarios extraños (por ejemplo, por las noches o durante un fin de semana), utilización de la misma cuenta desde distintos equipos a la vez, bloqueo reiterado de cuentas por fallos en la autenticación, ejecución inusual de determinados servicios desde algunas cuentas, etcétera.
- Informes de los propios usuarios del sistema alertando de algún comportamiento extraño o de su imposibilidad de acceder a ciertos servicios.
- Detección de procesos extraños en ejecución dentro de un sistema, que se inician a horas poco habituales o que consumen más recursos de los normales (tiempo de procesador o memoria).
- Generación de tráfico extraño en la red: envío de mensajes de correo electrónico hacia el exterior con contenido sospechoso, inusual actividad de transferencia de ficheros, escaneo de otros equipos desde un equipo interno…
- Notificación de un intento de ataque lanzado contra terceros desde equipos pertenecientes a la propia organización.
- Desaparición de equipos de la red de la organización.
- Aparición de dispositivos extraños conectados directamente a la red o a algunos equipos de la organización (en este último caso podrían ser, por ejemplo, dispositivos para la captura de pulsaciones de teclado en los equipos).

Conviene tener en cuenta que los ataques informáticos se están volviendo cada vez más sofisticados, por lo que es difícil conseguir detectarlos a tiempo. Incluso existen herramientas que facilitan este tipo de ataques ocultando su actividad y que se pueden obtener de forma gratuita en Internet.

Por otra parte, la gran cantidad de información que se genera en los "logs" y en las distintas herramientas de seguridad puede dificultar su posterior estudio, debido sobre todo a la pérdida de tiempo provocada por los "falsos positivos". Por este motivo, es necesario contar con herramientas y filtros que faciliten la detección y clasificación de los incidentes.

3.4. ANÁLISIS DE UN INCIDENTE DE SEGURIDAD

El Plan de Respuesta a Incidentes debe definir cómo el equipo de respuesta debería proceder al análisis de un posible incidente de seguridad en cuanto éste fuese detectado por la organización, determinando en primer lugar cuál es su alcance: ¿qué equipos, redes, servicios y/o aplicaciones se han podido ver afectados? ¿Se ha podido comprometer información confidencial de la organización o de sus usuarios y clientes? ¿Ha podido afectar a terceros?

Seguidamente, el equipo de respuesta debería determinar cómo se ha producido el incidente: qué tipo de ataque informático (si lo ha habido) ha sido el causante, qué vulnerabilidades del sistema han sido explotadas, qué métodos ha empleado el atacante, etcétera.

Se podría utilizar una "Matriz de Diagnóstico" para facilitar la actuación del equipo en momentos de máximo estrés, evitando que se puedan tomar decisiones precipitadas que conduzcan a errores, constituyendo además un valioso apoyo para el personal con menos experiencia en la actuación frente a incidentes de seguridad.

Síntoma	Código malicioso	Denegación de Servicio (DoS)	Acceso no autorizado
Escaneo de puertos	Bajo	Alto	Medio
Caída de un servidor	Alto	Alto	Medio
Modificación de ficheros de un equipo	Alto	Bajo	Alto
Tráfico inusual en la red	Medio	Alto	Medio
Ralentización de los equipos o de la red	Medio	Alto	Bajo
Envío de mensajes de correo sospechosos	Alto	Bajo	Medio

Tabla 1: Ejemplo de Matriz de Diagnóstico

Asimismo, conviene realizar una valoración inicial de los daños y de sus posibles consecuencias, para a continuación establecer un orden de prioridades en las actividades que debería llevar a cabo el equipo de respuesta, teniendo para ello en consideración aspectos como el posible impacto del incidente en los recursos y servicios de la organización y en el desarrollo de su negocio o actividad principal.

En este sentido, los documentos RFC 1244 y RFC 2196 (del IETF, Internet Engineering Task Force) proponen la siguiente priorización

de las actividades a realizar por parte de un equipo de respuesta a incidentes:

1. Prioridad uno: proteger la vida humana y la seguridad de las personas.
2. Prioridad dos: proteger datos e información sensible de la organización.
3. Prioridad tres: proteger otros datos e información de la organización.
4. Prioridad cuatro: prevenir daños en los sistemas informáticos (pérdida o modificación de ficheros básicos para las aplicaciones y los servidores).
5. Prioridad cinco: minimizar la interrupción de los servicios ofrecidos a los distintos usuarios (internos y externos).

3.5. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Dentro del Plan de Respuesta a Incidentes, el equipo de respuesta debe elegir una determinada estrategia de contención del incidente de seguridad. Una primera opción sería llevar a cabo una rápida actuación para evitar que el incidente pueda tener mayores consecuencias para la organización: apagar todos los equipos afectados, desconexión de estos equipos de la red informática, desactivación de ciertos servicios, etcétera. Esta estrategia de contención es la más adecuada cuando se puedan ver afectados servicios críticos para la organización, se pueda poner en peligro determinada información confidencial, se estén aprovechando los recursos de la organización para lanzar ataques contra terceros o cuando las pérdidas económicas puedan ser considerables.

Una segunda alternativa sería retrasar la contención para poder estudiar con más detalle el tipo de incidente y tratar de averiguar quién es el responsable del mismo. Esta estrategia se puede adoptar siempre y cuando sea posible monitorizar y controlar la actuación de los atacantes, para de este modo reunir las evidencias necesarias que permitan iniciar las correspondientes actuaciones legales contra los responsables del incidente. No obstante, se corre el riesgo de que el incidente pueda tener peores consecuencias para la organización o para terceros (y en este último caso la organización podría ser considerada culpable por no haber actuado a tiempo).

Por otra parte, en algunos tipos de ataque las medidas de contención adoptadas podrían desencadenar mayores daños en los sistemas informáticos comprometidos. Así, por ejemplo, un equipo controlado por un cracker podría estar ejecutando un servicio que se encargaría de realizar "pings" periódicos a determinados servidores o comprobar el estado de las conexiones de red, de tal modo que si se detectase una desconexión del equipo del resto de la red, se desencadenaría otro proceso encargado de eliminar todas las pruebas del disco duro del equipo.

También hay que tener en cuenta que en los ataques de Denegación de Servicio (DoS) puede resultar necesario contar con la colaboración de las empresas proveedoras de acceso a Internet o de administradores de las redes de otras organizaciones para contener el ataque.

Por su parte, la erradicación es la etapa del Plan de Respuesta a Incidentes en la que se llevan a cabo todas las actividades necesarias para eliminar los agentes causantes del incidente y de sus secuelas, entre las que podríamos citar posibles "puertas traseras" instaladas en los equipos afectados, rootkits u otros códigos malignos (virus, gusanos...), contenidos y material inadecuado que se haya introducido en los servidores, cuentas de usuario creadas por los intrusos o nuevos servicios activados en el incidente. También será conveniente llevar a cabo una revisión de otros sistemas que se pudieran ver comprometidos a través de las relaciones de confianza con el sistema afectado.

Por último, la recuperación es la etapa del Plan de Respuesta a Incidentes en la que se trata de restaurar los sistemas para que puedan volver a su normal funcionamiento. Para ello, será necesario contemplar tareas como la reinstalación del sistema operativo y de las aplicaciones partiendo de una copia segura, la configuración adecuada de los servicios e instalación de los últimos parches y actualizaciones de seguridad, el cambio de contraseñas que puedan haber sido comprometidas, la desactivación de las cuentas que hayan sido utilizadas en el incidente, la revisión de las medidas de seguridad para prevenir incidentes similares y la prueba del sistema para comprobar su correcto funcionamiento.

3.6. IDENTIFICACIÓN DEL ATACANTE Y POSIBLES ACTUACIONES LEGALES

Dentro del Plan de Respuesta a Incidentes, la identificación del atacante es necesaria para poder emprender acciones legales para exigir responsabilidades y reclamar indemnizaciones. No obstante, conviene tener en cuenta que generalmente sólo se podrá identificar la máquina o máquinas desde las que se ha llevado a cabo el

ataque, pero no directamente al individuo responsable de su utilización.

La identificación del atacante puede ser una tarea que consuma bastante tiempo y recursos, por lo que no debería interferir en la contención y erradicación del incidente. Algunas organizaciones optan por no perseguir legalmente a los atacantes por el esfuerzo necesario: costes, trámites judiciales, publicación en los medios...

Además, los ataques realizados desde otros países con ciertas lagunas legales en el tratamiento de los delitos informáticos pueden dificultar las reclamaciones judiciales, ya que se complica en gran medida el proceso de extradición de los responsables .

Existen distintas técnicas para determinar la dirección IP del equipo (o equipos) desde el que se ha llevado a cabo el ataque contra el sistema informático: utilización de herramientas como "ping", "traceroute" o "whois"; consulta en los registros inversos de servidores DNS; etcétera.

No obstante, es necesario tener en cuenta una serie de obstáculos que pueden dificultar esta tarea:

- Mediante técnicas de "IP Spoofing" se podría enmascarar la dirección en algunos tipos de ataque.
- El atacante podría estar utilizando equipos de terceros para realizar sus acciones, situación que se produce con bastante frecuente hoy en día.
- El atacante podría haber empleado una dirección IP dinámica, asignada a su equipo por un proveedor de acceso a Internet.
- El equipo del atacante podría estar situado detrás de un servidor proxy con el servicio NAT activo (traducción de direcciones internas a una dirección externa), compartiendo una dirección IP pública con otros equipos de la misma red.

Por este motivo, en muchos casos será necesario solicitar la colaboración de los responsables de otras redes y de los proveedores de acceso a Internet que pudieran haber sido utilizados por los atacantes.

Una tarea que también podría contribuir a la identificación del atacante es el análisis de las actividades de exploración (escaneos de puertos y de vulnerabilidades en el sistema) que suelen anteceder a un ataque, sobre todo si éstas han podido ser registradas por los "logs" de los equipos afectados o por el Sistema de Detección de Intrusiones (IDS).

En cuanto a la ejecución de acciones contra el atacante, se recomienda presentar una denuncia ante las unidades policiales especializadas en este tipo de incidentes o ataques informáticos, para poder emprender de este modo las correspondientes actuaciones policiales y judiciales.

Conviene destacar que si la organización decidiese actuar por su propia cuenta, "tomando la justicia por su mano", es decir, realizar ataques a modo de represalia contra los equipos desde los que aparentemente se está produciendo un intento de intrusión contra sus propios equipos y redes informáticas, esta actuación podría tener graves consecuencias para la organización. Si el atacante ha utilizado técnicas de enmascaramiento (como "IP Spoofing"), la organización podría lanzar un ataque contra equipos y redes inocentes, con las correspondientes responsabilidades legales que se derivan de esta actuación, por lo que podría ser denunciada por las organizaciones propietarias de estos equipos atacados a modo de represalia.

3.7. COMUNICACIÓN CON TERCEROS Y RELACIONES PÚBLICAS

El Plan de Respuesta a Incidentes tiene que contemplar cómo la organización debería comunicar a terceros la causa y las posibles consecuencias de un incidente de seguridad informática.

Así, dentro de este Plan de Respuesta deberían estar previstos los contactos con organismos de respuesta a incidentes de seguridad informática (como el CERT), con las fuerzas de seguridad (Policía o Guardia Civil), con agencias de investigación y con los servicios jurídicos de la organización.

También podría ser necesario establecer contactos con proveedores de acceso a Internet, ya sea el proveedor de la propia organización o el proveedor o proveedores que dan servicio a equipos desde los que se ha originado un ataque contra la organización.

Del mismo modo, en algunos casos sería recomendable contactar con los fabricantes de hardware y/o software que se hayan visto involucrados en el incidente, debido a una vulnerabilidad o una mala configuración de sus productos.

En el Plan de Respuesta a Incidentes también se deben contemplar los contactos con terceros que pudieran haber sido perjudicados

por el incidente de seguridad, como en el caso de que se hubieran utilizado ordenadores de la organización para realizar un ataque contra sistemas y redes de otras entidades. De este modo, se podrían limitar las responsabilidades legales en las que podría incurrir la organización por culpa del incidente de seguridad.

Por otra parte, hay que tener en cuenta el cumplimiento de la normativa existente ya en algunos países, que obliga a la notificación de los incidentes de seguridad a determinados organismos de la Administración, así como a los ciudadanos (generalmente clientes de la organización) que pudieran verse afectados por dicho incidente. En los contactos con los clientes de la organización, el personal debería poder transmitir seguridad y tranquilidad, indicando en todo momento que "la situación está controlada".

Por último, también será conveniente definir un Plan de Comunicación con los Medios: agencias de noticias, prensa, emisoras de radio y TV… Para ello, la organización debería establecer quién se encargará de hablar con los medios y qué datos se podrán facilitar en cada momento. El interlocutor debería estar preparado para responder a preguntas del estilo: ¿quién ha sido el responsable del ataque o incidente?, ¿cómo pudo suceder?, ¿hasta qué punto se ha extendido por la organización?, ¿qué medidas están adoptando para contrarrestarlo?, ¿cuáles pueden ser sus consecuencias técnicas y económicas?, etcétera.

En la comunicación con los medios, la organización debería procurar no revelar información sensible, como los detalles técnicos de las medidas adoptadas para responder al incidente de seguridad, y evitar en la medida de lo posible las especulaciones sobre las causas o los responsables del incidente de seguridad.

3.8. DOCUMENTACIÓN DEL INCIDENTE DE SEGURIDAD

El Plan de Respuesta a Incidentes debería establecer cómo se tiene que documentar un incidente de seguridad, reflejando de forma clara y precisa aspectos como los que se presentan en la siguiente relación:

- Descripción del tipo de incidente.
- Hechos registrados (eventos en los "logs" de los equipos).
- Daños producidos en el sistema informático.
- Decisiones y actuaciones del equipo de respuesta.
- Comunicaciones que se han realizado con terceros y con los medios.
- Lista de evidencias obtenidas durante el análisis y la investigación.
- Comentarios e impresiones del personal involucrado.
- Posibles actuaciones y recomendaciones para reforzar la seguridad y evitar incidentes similares en el futuro.

La Trans-European and Education Network Association (TERENA) ha desarrollado un estándar para facilitar el registro e intercambio de información sobre incidentes de seguridad: el estándar RFC 3067, con recomendaciones sobre la información que debería ser registrada en cada incidente ("*Incident Object Description and Exchange Format Requirements*").

Conviene destacar que una correcta y completa documentación del incidente facilitará el posterior estudio de cuáles han sido sus posibles causas y sus consecuencias en el sistema informático y los recursos de la organización. Por supuesto, será necesario evitar que personal no autorizado pueda tener acceso a esta documentación sensible.

3.9. ANÁLISIS Y REVISIÓN "A POSTERIORI" DEL INCIDENTE

Dentro del Plan de Respuesta a Incidentes se tiene que contemplar una etapa para el análisis y revisión "a posteriori" de cada incidente de seguridad, a fin de determinar qué ha podido aprender la organización como consecuencia del mismo.

Con tal motivo, será necesario elaborar un informe final sobre el incidente, en el que se puedan desarrollar los siguientes aspectos de forma detallada:

3.9.1. Investigación sobre las causas y las consecuencias del incidente:

- Estudio de la documentación generada por el equipo de respuesta a incidentes.
- Revisión detallada de los registros de actividad ("logs") de los ordenadores y dispositivos afectados por el incidente.
- Evaluación del coste del incidente de seguridad para la organización: equipos dañados, software que se haya visto afectado, datos destruidos, horas de personal dedicado a la recuperación de los equipos y los datos, información confidencial comprometida, necesidad de soporte técnico externo, etcétera.

- Análisis de las consecuencias que haya podido tener para terceros.
- Revisión del intercambio de información sobre el incidente con otras empresas e instituciones, así como con los medios de comunicación.
- Seguimiento de las posibles acciones legales emprendidas contra los responsables del incidente.

3.9.2. Revisión de las decisiones y actuaciones del equipo de respuesta a incidentes:

- Composición y organización del equipo.
- Formación y nivel de desempeño de los miembros.
- Rapidez en las actuaciones y decisiones: ¿cómo respondió el personal involucrado en el incidente?, ¿qué tipo de información se obtuvo para gestionar el incidente?, ¿qué decisiones se adoptaron?

3.9.3. Análisis de los procedimientos y de los medios técnicos empleados en la respuesta al incidente:

- Redefinición de aquellos procedimientos que no hayan resultado adecuados.
- Adopción de las medidas correctivas que se consideren necesarias para mejorar la respuesta ante futuros incidentes de seguridad.
- Adquisición de herramientas y recursos para reforzar la seguridad del sistema y la respuesta ante futuros incidentes de seguridad.

3.9.4. Revisión de las Políticas de Seguridad de la organización:

- Definición de nuevas directrices y revisión de las actualmente previstas por la organización para reforzar la seguridad de su sistema informático.

4. PRÁCTICAS RECOMENDADAS POR EL CERT/CC

El CERT/CC (*Computer Emergency Response Team / Coordination Center*) ha propuesto una serie de actividades para mejorar la respuesta de una organización ante los incidentes de seguridad informática. Seguidamente se presenta un extracto con algunas de las principales actividades propuestas por este organismo, agrupadas en tres fases o etapas:

4.1. Preparación de la respuesta ante incidentes de seguridad

- Definición del plan de actuación y los procedimientos para responder a los incidentes, especificando, entre otras cuestiones, a quién se debe informar en caso de incidente o qué tipo de información se debe facilitar y en qué momento (fase del incidente).
- Documentación del plan de actuación y de los procedimientos para responder a los incidentes.
- Comprobación de que el plan de actuación y los procedimientos previstos cumplen con los requisitos legales y las obligaciones contractuales con terceros (como, por ejemplo, exigencias de los clientes de la organización).
- Adquisición e instalación de herramientas informáticas y dispositivos que faciliten la respuesta ante incidentes. Conviene disponer de equipos redundantes, dispositivos de red y medios de almacenamiento para poder recuperar el funcionamiento normal del sistema.
- Verificación de los procedimientos y dispositivos de copias de seguridad.
- Creación de un archivo de discos de arranque y un conjunto de copias con todas las aplicaciones y servicios necesarios para el funcionamiento de los sistemas informáticos, así como de los parches y actualizaciones correspondientes.
- Formación y entrenamiento del personal afectado por este plan y procedimientos de actuación.
- Mantenimiento actualizado de una base de datos de contactos (personas y organizaciones).

4.2. Gestión del incidente de seguridad

- Aislamiento de los equipos afectados por el incidente, realizando además una copia de seguridad completa de sus discos duros.
- Captura y protección de toda la información asociada con el incidente: registros de actividad ("logs") de los equipos y dispositivos de red, ficheros dentro de los servidores, tráfico intercambiado a través de la red, etcétera.

- Catalogación y almacenamiento seguro de toda esta información para poder preservar las evidencias. Convendría disponer de copias de seguridad con la información del estado previo y del estado posterior al incidente de los equipos y sistemas afectados.
- Revisión de toda la información disponible para poder caracterizar el tipo de incidente o intento de intrusión. Análisis detallado de los registros de actividad ("logs") y del estado de los equipos para determinar cuál puede ser el tipo de ataque o incidente, qué sistemas se han visto afectados, qué modificaciones han realizado o qué programas han ejecutado los posibles intrusos dentro de estos sistemas.
- Comunicación con todas las personas y organismos que deberían ser informados del incidente, cumpliendo con lo establecido en las políticas y procedimientos de respuesta a incidentes. Mantenimiento de un registro detallado de todas las comunicaciones y contactos establecidos durante la respuesta ante el incidente.
- Participación en las medidas de investigación y de persecución legal de los responsables del incidente.
- Aplicación de soluciones de emergencia para tratar de contener el incidente: desconectar los equipos afectados de la red corporativa; desactivar otros dispositivos y servicios afectados; apagar temporalmente los equipos más críticos; cambiar contraseñas e inhabilitar cuentas de usuarios; monitorizar toda la actividad en estos equipos; verificar que se dispone de copias de seguridad de los datos de los equipos afectados por el incidente; etcétera.
- Eliminación de todos los medios posibles que faciliten una nueva intrusión en el sistema: cambiar todas las contraseñas de los equipos a los que hayan podido tener acceso atacantes o usuarios no autorizados; revisar la configuración de los equipos; detectar y anular los cambios realizados por los atacantes en los equipos afectados; restaurar programas ejecutables y ficheros binarios (como las librerías del sistema) desde copias seguras; mejorar, si es posible, los mecanismos de registro de la actividad en estos equipos.
- Recuperación de la actividad normal de los sistemas afectados: reinstalación de aplicaciones y servicios, incluyendo los parches y actualizaciones de seguridad; restauración de los datos de los usuarios y las aplicaciones desde copias de seguridad; recuperación de las conexiones y servicios de red; verificación de la correcta configuración de estos equipos.

4.3. Seguimiento del incidente de seguridad

- Identificación de las lecciones y principales conclusiones de cada incidente, recurriendo para ello al análisis "post-mortem" de los equipos afectados por el incidente y entrevistando a las personas implicadas en la gestión del incidente.
- Implementación de las mejoras de seguridad propuestas como consecuencia de las "lecciones aprendidas" en cada incidente: revisión de las políticas y procedimientos de seguridad, realización de un nuevo análisis detallado de las vulnerabilidades y riesgos del sistema, etcétera.

REFERENCIAS BIBLIOGRÁFICAS

S. Barman, Writing Information Security Policies, New Riders Publishing, 2001.

E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, 2004.

J. Chirillo, Hack Attacks Revealed: A Complete Reference, John Wiley & Sons, 2001.

E. Cole, Hackers Beware, New Riders, 2001.

E. Cole, R. Krutz, J. Conley, Network Security Bible, John Wiley & Sons, 2005.

J. Erickson, Hacking: The Art of Exploitation, No Starch Press, 2003.

A. Gómez, Enciclopedia de la Seguridad Informática, Ra-Ma, 2006.

K. Kaspersky, Hacker Disassembling Uncovered, A-LIST Publishing, 2003.

J. Long, Google Hacking for Penetration Testers, Syngress, 2005.

S. McClure, S. Shah, Web Hacking: Attacks and Defense, Addison Wesley, 2002.

J. Mirkovic, S. Dietrich, D. Dittrich, P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms, Prentice Hall, 2004.

RFC's 1244, 2196 y RFC 3067.

R. Russell, Hack Proofing Your Network, Syngress, 2000.

R. Russell, Stealing the Network: How to Own the Box, Syngress, 2003.

J. Scambray, S. McClure, G. Kurtz, Hacking Exposed: Network Security Secrets & Solutions - 2nd Edition, Osborne/McGraw-Hill, 2001.

J. Scambray, M. Shema, Hacking Exposed Web Applications, Osborne/McGraw-Hill, 2002.

M. Shema, Anti-Hacker Tool Kit, Osborne/McGraw-Hill, 2002.

H. Warren, Hacker's Delight, Addison Wesley, 2002.

RESEÑA CURRICULAR DEL AUTOR

Álvaro Gómez Vieites

Ingeniero de Telecomunicación por la Universidad de Vigo. Especialidades de Telemática y de Comunicaciones. Número uno de su promoción (1996) y Premio Extraordinario Fin de Carrera.

Ingeniero Técnico en Informática de Gestión" por la UNED (2004-2006). Premio al mejor expediente académico del curso 2004-2005 en la Escuela Técnica Superior de Ingeniería Informática de la UNED

"Executive MBA" y "Diploma in Business Administration" por la Escuela de Negocios Caixanova.

Ha sido Director de Sistemas de Información y Control de Gestión en la Escuela de Negocios Caixanova. Profesor colaborador de esta entidad desde 1996, responsable de los cursos y seminarios sobre Internet, Marketing Digital y Comercio Electrónico.

Socio-Director de la empresa SIMCe Consultores, integrada en el Grupo EOSA.

Autor de varios libros y numerosos artículos sobre el impacto de Internet y las TICs en la gestión empresarial.