SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

3.2.2.MF0488_3. Capítulo 2
Parte 3

Proceso de notificación y gestión de intentos de intrusión

JOSÉ PABLO HERNÁNDEZ

8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

En el momento que se tiene confirmada la presencia de un ataque en el sistema, el primer paso a realizar para investigar su procedencia será comprobar si los usuarios que utilizan el sistema en ese momento pueden ser sospechosos y, en caso afirmativo, comprobar cuáles son los sistemas que se están ejecutando y quién los está ejecutando para tener controlados los usuarios que han podido ser causantes del ataque.

8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

Visualizar los usuarios logueados en el sistema.

Visualizar los procesos activos.

Serán indicios de amenaza:

- **Procesos que llevan activos un largo período de tiempo.**
- **Procesos que se inician en horas poco habituales.**
- **Procesos que consumen un nivel elevado de CPU.**
- **Procesos que no están ejecutados desde un terminal.**

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Cuando a pesar de ejercer un control de los usuarios y de los procesos del sistema la incidencia ha ocurrido sin conocer quién la ha provocado, hay una serie de recomendaciones y pasos a tener en cuenta para encontrar indicios y señales que permitan detectar las huellas que el intruso ha podido dejar sin darse cuenta.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Examen de los archivos de registro o logs

Con el examen de los archivos de registro o logs se podrá obtener información sobre conexiones a lugares poco frecuentes, utilización de aplicaciones inusuales y otras actividades sospechosas de intrusión.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Comprobación de los permisos del sistema

Es necesario comprobar los permisos de los usuarios del sistema para detectar si alguno de ellos dispone de permisos para más acciones de las que debería estar autorizado.

Una mala asignación de permisos puede ser causante de incidencias.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Chequeo de los archivos binarios del sistema

Es habitual que los intrusos modifiquen los archivos binarios del sistema para ocultarse e intentar borrar huellas. Por ello se recomienda realizar una profunda revisión de los mismos con el fin de comprobar que no han sufrido ninguna alteración.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Comprobación de los puertos abiertos

Cuando se ha producido una intrusión y el intruso ya no está en el sistema es posible que se haya dejado un puerto de conexión abierto.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Comprobar la existencia de sniffers

Como ya se sabe, los sniffers son programas encargados de monitorizar el tráfico de red.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Comprobar la existencia de servicios no autorizados

Se aconseja comprobar si hay dado de alta en el sistema algún servicio no autorizado.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Comprobar las contraseñas del sistema

Se recomienda realizar una comprobación de todas las contraseñas del sistema para detectar si ha habido alguna modificación no autorizada de las mismas.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Comprobar la configuración del sistema y de la red

Hay que examinar los accesos en los archivos de configuración del sistema y de la red para detectar algún acceso no autorizado que haya podido modificar cualquier propiedad o herramienta del sistema.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Buscar todos los archivos ocultos o poco habituales

Otro modo de comprobar la existencia de amenazas en el sistema es mediante el chequeo de todos sus archivos.

Es muy frecuente que los intrusos se oculten en el sistema mediante archivos ocultos o inusuales en los que puedan ocultar herramientas y aplicaciones que les permitan saltar los sistemas de seguridad del sistema y acceder a archivos comprometidos y/o críticos.

8.1. INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

Examinar todos los equipos de la red local

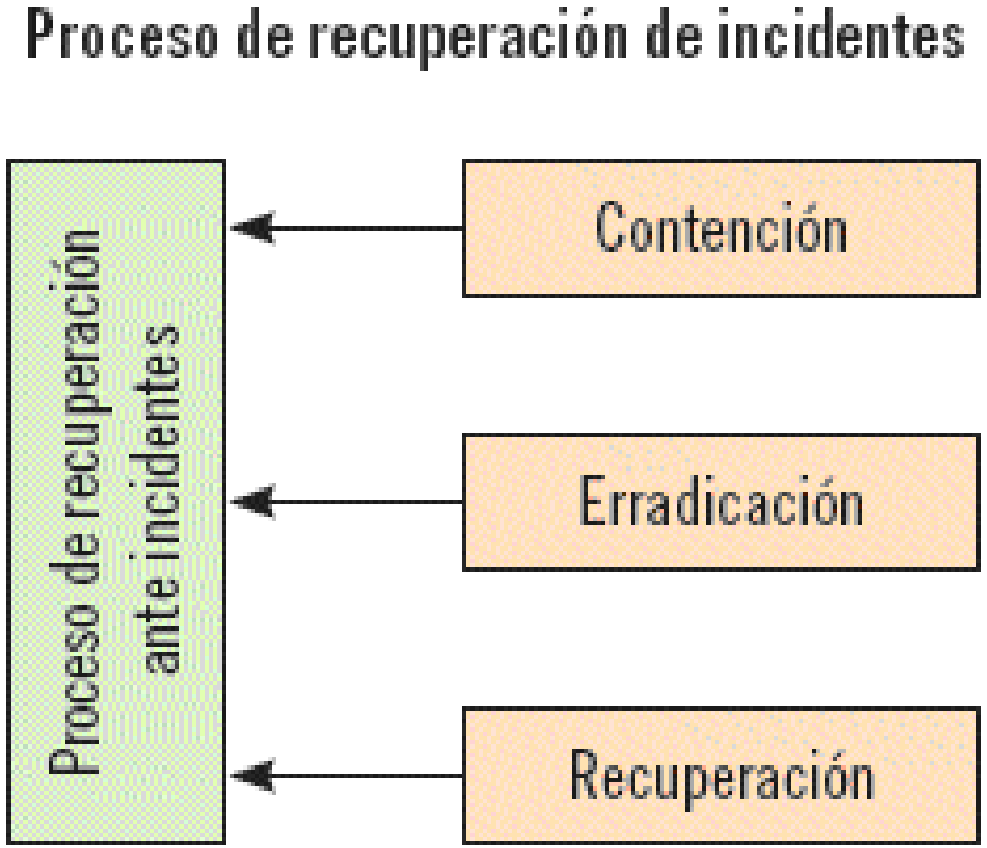
No solo hay que examinar el equipo del que se sospecha que ha podido sufrir un ataque, también se deben examinar todos los equipos que formen parte de su red para comprobar si han sido afectados.

9. PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS

Una vez confirmado y diagnosticado el incidente es el momento de proceder a su resolución y a la recuperación de los sistemas a la situación previa a su aparición.

9. PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS

Esta fase de resolución y recuperación se divide en tres apartados



9.1. EL PLAN DE RECUPERACIÓN ANTE DESASTRES

Se recomienda la implantación y desarrollo de un plan de recuperación ante desastres en el que se establezcan los procedimientos a seguir para la recuperación de la información en caso de incidencias y desastres.

9.1. EL PLAN DE RECUPERACIÓN ANTE DESASTRES

Determinación de las vulnerabilidades que puedan interrumpir el servicio.

Identificación y análisis del coste, imagen y otras consecuencias.

Determinación de las necesidades inmediatas, tanto a medio como a largo plazo, de recuperación del servicio y de los recursos que sean necesarios para ello.

Identificación de las distintas alternativas posibles y selección de las más rentables para facilitar las operaciones de copia de seguridad y de restauración de la actividad a tiempo.

Desarrollo e implantación de planes de contingencia que se encarguen de ejecutar las medidas inmediatas y de largo plazo.

9.1. EL PLAN DE RECUPERACIÓN ANTE DESASTRES

La estructura de un plan de recuperación de desastres debería contener, como mínimo, lo siguiente:

- Plan de trabajo con la planificación de actividades de recuperación de la información.
- Informes de evaluación de la seguridad y la vulnerabilidad de los sistemas.
- Análisis de impacto al negocio.
- Definición de los requisitos de la organización en cuanto a las necesidades de recuperación, el ámbito de aplicación y sus objetivos.
- Plan de desarrollo de la organización en el que se establezcan las normas de recuperación, los responsables de seguridad y las copias de respaldo de la información.
- Programa de pruebas en el que se establezcan las estrategias de la organización para ejecutar pruebas, ensayos y ejercicios con el fin de comprobar la seguridad de sus equipos y sistemas.
- Programa de mantenimiento en el que se establezcan todas las medidas de actualización de sistemas y de aplicaciones de los equipos de la organización.
- Prueba inicial del plan de recuperación de desastres e implantación.

9.1. EL PLAN DE RECUPERACIÓN ANTE DESASTRES

La correcta definición e implantación de un plan de respuesta a incidentes, para terminar, implica numerosos beneficios para las organizaciones.

- Reducción de daños y pérdidas ante la presencia de un incidente.
- Mayor capacidad de protección de los sistemas críticos para la organización.
- Reducción del riesgo de interrupción de la actividad.
- Minimización de la toma de decisiones en caso de detección de incidentes.
- Mejora de la eficiencia general de la organización con la identificación de sus recursos y activos críticos.
- Reducción de las responsabilidades legales que puedan venir ocasionadas por la producción de incidentes.
- Garantía de la fiabilidad de los sistemas reserva de la organización.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Cuando ya se ha llegado a controlar el incidente y se ha conseguido restaurar la situación inicial es el momento de evaluar si procede comunicar los hechos sucedidos a terceros que no tengan que ver con la organización.

En el plan de respuesta a incidentes de las organizaciones se deberían reflejar los aspectos referentes a la comunicación a terceros de las incidencias producidas, los efectos causados, sus causas y las posibles consecuencias que hayan podido suceder.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Asesoramiento

Se recomienda a las organizaciones que intenten asesorarse ante profesionales especializados que evalúen las acciones y decisiones tomadas con el fin de mejorar para futuras incidencias.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Proveedores

Si se ha comprobado que los sistemas de detección y prevención de incidentes han fallado, hay que recurrir a los proveedores de dichas herramientas para que sean conscientes de los fallos de su aplicación.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Comunicación a terceros

Aparte de los proveedores es posible que la incidencia haya afectado a datos y recursos de terceras personas y/o organizaciones.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Fabricantes de software y hardware

En el momento en el que la incidencia ha afectado a algún componente de software o hardware de la organización se recomienda comunicarlo a sus proveedores y fabricantes para que evalúen los daños causados y las posibles consecuencias que puedan aparecer.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Comunicación a terceros perjudicados

No solo hay que comunicar a los terceros cuyos recursos han sido afectados a nivel interno de la organización.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Comunidad general

Cuando la gravedad de la incidencia supone consecuencias graves para la organización e incluso daños y consecuencias perjudiciales para la comunidad, es recomendable comunicar la aparición de dicha incidencia y de las consecuencias de su infección en los sistemas y aplicaciones de una organización y/o usuario particular a través de un plan de comunicación con los medios.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Fuerzas de seguridad

En el caso de haberse producido delito informático por parte del atacante hay que comunicar todo lo sucedido a la policía o agente de seguridad análogo para que recaben todo tipo de pruebas y huellas y conseguir localizarle para que cumpla con los requerimientos legales.

10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

Organismos de respuesta a incidentes

Las organizaciones deben estar en contacto con los organismos de respuesta a incidentes como Cert Inteco en España u otros organismos internacionales.

Ejemplo.

EN SU ORGANIZACIÓN HAN SUFRIDO UN ATAQUE DE ROBO DE DATOS PERSONALES DE CLIENTES QUE PUEDE SER DELITO PARA EL ATACANTE. EN EL PROCESO DE GESTIÓN DE LA INTRUSIÓN, ¿DEBERÍA REALIZAR ALGUNA COMUNICACIÓN A TERCEROS? INDIQUE CUÁLES Y JUSTIFÍQUELO.

Ejemplo. Solución

AL ESTAR AFECTADOS DATOS DE CARÁCTER PERSONAL DE CLIENTES DEBERÍA COMUNICARSE EL ROBO DE DATOS A DICHOS CLIENTES, YA QUE SON LOS PRINCIPALES AFECTADOS DEL ATAQUE.

EN EL RGPD SE ESTABLECE UN PLAZO DE 72 H PARA NOTIFICAR LAS BRECHAS DE SEGURIDAD A LA AEPD Y A LOS AFECTADOS.

POR OTRO LADO, AL CONSIDERARSE DELITO EL ROBO Y UTILIZACIÓN DE DATOS PERSONALES SIN AUTORIZACIÓN DEBERÁ COMUNICARSE DICHO ROBO A LAS FUERZAS DE LA AUTORIDAD PARA QUE BUSQUEN A LOS CULPABLES DEL DELITO Y LES HAGAN PAGAR POR EL DELITO COMETIDO.

11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE

Cuando ya se ha solucionado hay que llevar a cabo una serie de acciones que permitan cerrar el incidente:

- Comprobar con los usuarios que el incidente ha sido solucionado satisfactoriamente.
- Incorporar las acciones y medidas tomadas para la resolución del incidente en la base de datos de su histórico.
- Reclasificar el incidente como “resuelto” o “cerrado”.
- Actualizar la información (en la base de datos de la organización) de las configuraciones del sistema que han intervenido en el proceso de gestión del incidente.
- Cerrar el incidente.

11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE

Es necesario la elaboración de informes :

- Gestión de los niveles de servicio.
- Monitorización del rendimiento del centro de servicios.
- Optimización de la asignación de recursos.
- Identificación de los errores.
- Disposición de información estadística.

11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE

Se recomienda la elaboración de métricas:

- Cantidad de incidentes clasificados temporalmente y por prioridades.
- Ratio en porcentaje de los incidentes (clasificados por prioridades) resueltos en una primera instancia.
- Nivel de cumplimiento de la oferta de servicios a clientes.
- Costes asociados a la aparición y resolución de la incidencia.
- Recursos utilizados para la resolución de la incidencia.
- Nivel de satisfacción de los clientes.
- Tiempos de respuesta y resolución según el impacto y la urgencia de los incidentes.

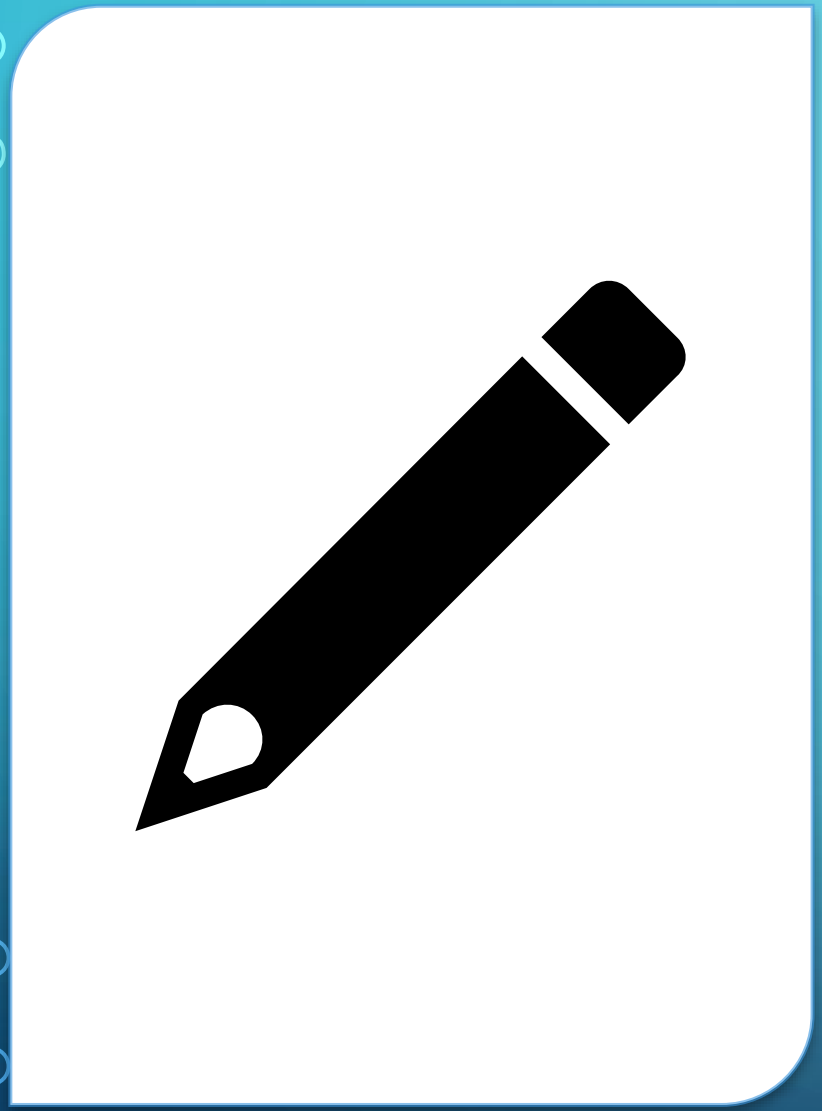
11.1. SOPORTE DE INCIDENTES

Desde que se detecta un incidente hasta que se cierra hay una serie de acciones de soporte que deben llevarse a cabo para tener un control adecuado de su evolución y de todas las acciones realizadas para su resolución y cierre.

11.1. SOPORTE DE INCIDENTES

Pasos de soporte de incidentes	Descripción
Reporte del incidente	Comunicación de las sospechas de incidente a los responsables.
Registro y documentación	Obtención de información adicional y clasificación de la incidencia.
Preparación de la solución	Asignación de tiempos máximos de contención y respuesta.
Aplicación de soluciones mediante software de apoyo	Remisión a los interesados de información referente a la evolución del incidente.
Identificación y solución de problemas	Búsqueda de causa común con incidentes anteriores.
Cierre del incidente con éxito	Comunicación del cierre exitoso del incidente a todos los interesados.

Ejercicios.



3.2.100.1.MF0488_3_EJERCICIOSCAPITULO_2.DOCX.