APUNTES 04

IMPLANTACIÓN DE MEDIDAS DE CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

Aumento de Incidentes debido a la Transformación Digital
La Transformación Digital que se está generalizando está produciendo una proliferación masiva de Incidentes de Ciberseguridad, pues no sólo se están digitalizando los particulares y las empresas, sino también los malintencionados y los delincuentes.
Para protegerse frente a esta plaga, se deberán efectuar labores preventivas, labores operativas en caso de la manifestación de un incidente, así como labores de registro y documentación de las lecciones aprendidas, de cara a futuros ataques similares o derivados del detectado.

En esta unidad se darán indicaciones para implementar e implantar las Medidas de Ciberseguridad que permitan prevenir y combatir adecuadamente los incidentes.
Estas medidas estarán compuestas por procedimientos, capacidades, flujos de toma de decisión y mecanismos de restablecimiento de los servicios afectados en cada caso.

1.- PROCEDIMIENTOS DE ACTUACIÓN PARA DAR RESPUESTA, MITIGAR, ELIMINAR O CONTENER INCIDENTES.

A más desconcierto, más afectación
En los momentos iniciales de afectación por un incidente o de detección temprana del mismo, suele existir un cierto desconcierto en lo relativo a las medidas que se deben tomar, por parte de quién y en qué orden.
La afectación de los incidentes es directamente proporcional a dicho desconcierto, por lo que la mejor forma de preverlo y evitarlo es desarrollando Procedimientos de Actuación adecuados.

A pesar de que las medidas de mitigación dependen del tipo de ciberincidente y la afectación que haya tenido, algunas recomendaciones en esta fase son:

- Determinar las causas y los síntomas del ciberincidente para determinar las medidas de mitigación más eficaces. La identificación de la causa raíz suele constituir el 80% del trabajo posterior de análisis del incidente, puesto que en la mayoría de los casos una causa suele llevar aparejado un motivo para el ataque (malicia, burla, hurto, perjuicio para la actividad). Por lo que respecta a los síntomas, también es muy importante detallar todo aquello que se pueda detectar por observación directa o indirecta, puesto que estas trazas casi siempre estarán conectadas con el modus operandi, lo cual aportará también información muy valiosa para el análisis.
- Identificar y eliminar todo el software utilizado por los atacantes. Esta recomendación está ligada a la Filosofía Lean, esto es, pulcritud y orden en todos los escenarios, máxime cuando se trata de malware, cuya funcionalidad no se acaba nunca de conocer del todo y cuyos restos pueden propiciar la reproducción del problema antes o después, bien porque escondan aún más capacidades de ataque, bien porque dejen abiertos canales de entrada desde el exterior. En esta recomendación conviene ser radical, esto es, si se tiene la más mínima sospecha de que pueda quedar algún resto de malware en el sistema, o que pueda haber quedado abierta alguna vía de infección posterior, se deberá recuperar una imagen de respaldo anterior que esté limpia, o bien, se deberá plataformar totalmente la máquina, aunque ello conlleve la pérdida de los últimos movimientos o transacciones efectuadas.
- Recuperación de la última copia de seguridad limpia. Esta recomendación conecta con la anterior, no obstante, figura expresamente por separado porque muchas veces es muy difícil garantizar que una imagen de respaldo anterior no haya respaldado también el malware que ha ocasionado el ataque, o bien, otro malware que pueda estar dormido en su interior, por lo que se deberá disponer de herramientas de análisis de información de respaldo que sean capaces de detectar el máximo número de amenazas potenciales.
- Identificar los servicios utilizados durante el ataque, ya que en ocasiones los atacantes utilizan servicios legítimos de los sistemas atacados. En este sentido, las estadísticas son claras, puesto que el número de ataques que se efectúan utilizando brechas de los sistemas es sensiblemente menor que aquellos ataques que se efectúan a través de servicios legítimos no suficientemente protegidos, o bien, a los que se accede tras un robo de credenciales o usando Fuerza Bruta.
- Por último, se realizará un informe del ciberincidente que deberá detallar su causa y su coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados), así como las medidas que la organización deberá tomar para prevenir futuros ciberincidentes de naturaleza similar. La euforia derivada de vencer o superar un ataque junto con la premura de restaurar los servicios productivos, hace que muchas veces no se detalle adecuadamente la información necesaria para el futuro, o bien, no se estime el impacto en costes o prestación de servicios. La consecuencia inmediata suele ser lamentable, pues muchos ataques exitosos se deben a una repetición de un ataque anterior que no se ha prevenido a pesar de tener la información suficiente. Además, muchos ataques son toscos y se efectúan mediante branches de algún malware anterior que haya tenido éxito en sus propósitos. Este problema se refuerza si no se calcula el coste del ataque, puesto que ante un coste desconocido no se suelen tomar medidas inmediatamente, lo cual provoca que el siguiente ataque similar se efectúe a corto plazo, mientras que si se observa un elevado coste sí que se tomarán medidas adecuadas de prevención cuanto antes.

2.- IMPLANTAR CAPACIDADES DE CIBERRESILIENCIA.

El Concepto de Ciberresiliencia

La ciberresiliencia, es la capacidad para resistir, proteger y defender el uso del ciberespacio frente a los atacantes. Por lo general se suele establecer, desarrollar y medir con base en una escala de niveles.

En general, la mayoría de las empresas están poco preparadas para resistir frente a los ciberataques, debido principalmente a:

- Falta de medidas técnicas para mitigarlos.
- Poca preparación de los sistemas para detener este tipo de ataques.
- Falta de formación o de recursos para hacerles frente.
- Falta de pruebas para evaluar la capacidad real de la organización ante cualquier tipo de ataque externo.

Las organizaciones, deben estar preparadas para dar respuestas rápidas a este tipo de ataques, permitiendo que los servicios que prestan no se vean interrumpidos, y fortaleciendo sus capacidades de identificación, detección, prevención, contención, recuperación, cooperación y mejora continua contra las ciberamenazas.

Durante mucho tiempo, la política de combate de los incidentes de ciberseguridad ha sido completamente reactiva, esto es, sólo se ha combatido de forma puntual los ataques y sólo se han tomado medidas ad hoc para cada variedad de malware. Afortunadamente, en la actualidad quedan pocas dudas de que haya que tomar medidas preventivas de ciberseguridad y de que la política de combate deba ser proactiva, como reza la antigua sentencia del escritor romano Flavio Vegecio: "si vis pacem, para bellum" (si quieres la paz, prepárate para la guerra). En línea con esto, en la mayoría de las empresas existen directivos y políticas específicas para la prevención de incidentes, junto con su correspondiente presupuesto en el plan estratégico.

3.- ESTABLECER FLUJOS DE TOMA DE DECISIONES Y ESCALADO INTERNO Y/O EXTERNO ADECUADOS

La Estrategia de Contención de Incidentes

El conjunto de flujos de decisión y escalado constituyen la denominada Estrategia de Contención de Incidentes de Ciberseguridad. En este marco estratégico se debe contemplar toda la tipología de incidentes, relacionándola adecuadamente con el conjunto de criterios a tener en cuenta para la toma de decisión en cada caso.

Los criterios generales para guiar la toma de decisión podrán ser los siguientes:

- Cuestiones forenses.
- Daño potencial a la organización.
- Hurto de activos y detalle de su valor.
- Premisas para preservar las evidencias, de cara a una investigación posterior.
- Disponibilidad del servicio afectado y tiempo necesario para restablecerlo.
- Tiempo y recursos requeridos para la implementación del marco estratégico.
- Efectividad de la estrategia para la contención total o parcial del incidente.
- Vigencia de la solución aplicada.
- Etc.

Para el diseño de estos flujos es importante tomar como referencia toda la información que sea posible, sin centrarse sólamente en los incidentes acaecidos en la empresa o en empresas próximas o relacionadas. En ese sentido, es fundamental la adhesión a las comunidades del ámbito de la ciberseguridad, sobre todo en lo relativo a la prevención de incidentes.

Lo que suele dar mejor resultado en esta cuestión es abrir un capítulo de Hacking Ético y conectarse con las comunidades relacionadas con el mismo, pues suelen ser muy activas y procuran tener actualizados sus procedimientos y su software en línea con todas las amenazas conocidas a nivel global. Si no es posible contemplar este tema de forma orgánica, creando un área al efecto en la empresa, lo mejor es hacerlo de forma inorgánica, esto es, contratando los servicios de una empresa de Pentesting y Hacking Ético.

La iniciativa más popular en este sentido a nivel global es la de Offensive Security y su distribución Kali Linux, que contiene cientos de paquetes software de código abierto, especializados en ataques muy variados y actualizados a diario.

Así pues, conjugando todas las amenazas conocidas y sus medidas de contención, con las particularidades de cada empresa y su organización, se podrá diseñar flujos coherentes de toma de decisión en lo tocante a la contención de incidentes de ciberseguridad.

4.- TAREAS PARA RESTABLECER LOS SERVICIOS AFECTADOS POR INCIDENTES

La Recuperación frente a un Incidente

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad cuanto antes. Es importante no precipitarse en la puesta en producción de sistemas que se hayan visto implicados en ciberincidentes.

La recuperación de la actividad normal no siempre es posible de forma completa e inmediata. Por ello, es conveniente definir y detallar los niveles de operación de la empresa en su escenario de trabajo habitual, de forma que se sepa cómo actuar para llegar a cada uno de dichos niveles, y qué características del servicio se verán deterioradas total o parcialmente por no estar en el nivel más alto de operación. Esta actividad de definición y caracterización de los niveles de operación también deberá estar recogida en la estrategia de ciberseguridad de la empresa, pues la implementación de dichos niveles puede que no sea estrictamente organizativa y precise desarrollos o configuraciones ad hoc en los sistemas involucrados en la prestación de los servicios.

Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un período de tiempo con medidas adicionales de monitorización. Por lo general, la prisa existente tras un incidente para recuperar el nivel de operación requerido provoca que, en ocasiones, no se tomen todas las precauciones necesarias ni se mantengan las cuarentenas requeridas, a lo cual hay que sumar la dotación de planes de respuesta de emergencia a aplicar en caso de reproducción a corto plazo de un incidente ya identificado y contenido.
Una vez que el ciberincidente está controlado y la actividad ha vuelto a la normalidad, es momento de llevar a cabo un proceso al que no se le suele dar toda la importancia que merece, las lecciones aprendidas, que se basan en la documentación del incidente, como se verá en el apartado siguiente.

5.- DOCUMENTACIÓN DE LOS INCIDENTES.

La Necesaria Reflexión tras un Incidente

Tras un incidente, conviene pararse a reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados a la misma.
La finalidad de este proceso es aprender de lo ocurrido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda repetir, además de mejorar los procedimientos.

La última tarea del proceso de gestión de incidentes consistirá en documentar adecuadamente el ciberincidente detallando lo siguiente:

- Su causa.
- Su coste, por compromiso de información o por impacto en los servicios que se hayan visto afectados.
- Las medidas a tomar para prevenir futuros ciberincidentes similares.

La creación de políticas de Lecciones Aprendidas no es una opción en el campo de la ciberseguridad. Esta recomendación Lean ha probado ya su eficiencia sobradamente cuando se trata de producción, fabricación o prestación de servicio, todos ellos ámbitos acotados en cierta medida. Así pues, dado que en el caso de la ciberserguridad el ámbito no es acotado de ninguna manera, toda la información que se recoja será de utilidad para documentar adecuadamente el problema y evitar su reproducción. Se debe trabajar intensamente en esta cuestión para evitar tropezar dos veces en la misma piedra, pues en algunas ocasiones el coste de estos tropiezos inducidos puede ser muy alto y puede tener incluso responsabilidades disciplinarias por dejación de funciones, omisión de deberes o inacción en general.

6.- SEGUIMIENTO DE INCIDENTES PARA EVITAR UNA SITUACIÓN SIMILAR.

La Cuarentena tras un Incidente

Conviene prestar especial atención a los sistemas atacados durante la nueva puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un periodo de tiempo con medidas adicionales de monitorización, normalmente denominado cuarentena. Para efectuar este seguimiento, la empresa se deberá servir de todos los medios a su alcance, tanto humanos (analistas de ciberseguridad) como técnicos (detección de intrusiones), lo cual equivale en la mayoría de los casos a disponer de un Centro de Operaciones de Seguridad.

En las empresas en que se disponga de un SOC, toda la actividad de ciberseguridad de la empresa estará centralizada, tanto en lo relativo a la detección y combate, como en lo relativo al almacenamiento de datos y a su análisis posterior, máxime si éstos se efectúan durante el período de cuarentena de un sistema tras un ataque ya expurgado.
Como se comentó al principio del módulo, en las dos últimas unidades del mismo se implementará un SOC real fundamental, a partir del cual se podrá trabajar para construir el conocimiento de ciberseguridad de cualquier empresa, escalando el sistema tanto en recursos físicos como en recursos lógicos a medida que se vayan detectando y combatiendo incidentes.

Respuesta
Autoevaluación I: c)
Autoevaluación II: c)
Autoevaluación III: a)
Autoevaluación IV: c)
Autoevaluación V: c)
Autoevaluación VI: b)
TEST I 9/10: 1 c), 2 x), 3 c), 4 c), 5 b), 6 c), 7 c), 8 c), 9 c), 10 c)

Autoevaluación I

¿Qué consecuencias tiene no detallar adecuadamente la información de un incidente?

a) La contaminación de los respaldos con el malware atacante
b) La persistencia del malware dentro del software legítimo
c) La repetición de un ataque anterior que no se ha prevenido, de forma directa o mediante un branch del malware

Autoevaluación II

¿Cuál es la política más recomendable para el combate efectivo contra los incidentes de ciberseguridad?

a) Reaccionar de forma rápida y puntual a cada ataque
b) Tomar medidas preventivas de ciberseguridad
c) La combinación de las dos anteriores

Autoevaluación III

¿Cuál es la mejor estrategia para establecer Flujos de Toma de Decisión y Escalado?

a) Abrir un capítulo de Hacking Ético y conectarse con las comunidades relacionadas con el mismo
b) Contratar los servicios de una empresa de Pentesting y Hacking Ético
c) Cualquiera de las anteriores, en función de los recursos de la empresa

Autoevaluación IV

¿Cuál es el proceso que menos se prioriza durante el restablecimiento de servicios afectados por un incidente?

a) La recuperación de la actividad normal
b) La búsqueda de signos de actividad sospechosa tras la recuperación de la actividad normal
c) Las lecciones aprendidas

Autoevaluación V

¿Qué se debe detallar durante el proceso de documentación de un incidente?

a) Sólo los datos del malware atacante
b) Sólo las consecuencias del ataque
c) Su causa, su coste y las medidas a tomar para el futuro

Autoevaluación VI

¿Cuál es la mejor forma de supervisar un sistema recuperado, durante su período de cuarentena?

a) Disponer de un Sistema de Detección de Intrusiones
b) Disponer de un SOC
c) Disponer de Mecanismos de Respuesta Rápida

TEST I

1- ¿A qué se debe principalmente la repetición de ataques anteriores?:

a) O a. A no actualizar las medidas antimalware.
b) A no documentar adecuadamente la causa y el coste del incidente.
c) A no aplicar medidas preventivas.

3- ¿Cuál de las siguientes cuestiones no es un criterio para la toma de decisión en relación con la contención de un incidente?:

a. Premisas para preservar las evidencias, de cara a una investigación posterior.
b. Daño potencial a la organización.
c. Tiempo de espera online.
d. Hurto de activos y detalle de su valor.

4- La Ciberresiliencia es:

a. La resistencia frente a la repetición de incidentes conocidos.
b. La resistencia a los incidentes recursivos.
c. La capacidad para resistir, proteger y defender el uso del ciberespacio frente a los atacantes.
d. La resistencia informática extrema.

5- La distribución Linux más popular en el área del Hacking Ético es:

a. Fodora.
b. Ninguna de las anteriores.
c. Red Hat.
d. SUSE.

6- ¿En caso de ausencia procedimientos de actuación, qué suele ocurrir en momentos iniciales de afectación por incidente?:

a. Se cortan súbitamente las comunicaciones LAN/WAN.
b. Se levantan inmediatamente todos los escudos antimalware.
c. Por lo general hay un cierto desconcierto en lo relativo a las medidas que se deben tomar.

7- La identificación de la Causa Raiz suele suponer:

a. El 75% del trabajo de análisis.
b. El 10% del trabajo de análisis.
c. El 80% del trabajo de análisis.
d. El 50% del trabajo de análisis.

8- La clave de las Lecciones Aprendidas es:

a. La precisión del análisis del incidente.
b. La calidad de las evidencias recopiladas.
c. La documentación del incidente.
d. La Ciber-Resiliencia de la organización.

9- ¿Cuál es la orientación principal de la política de combate de los incidentes en la actualidad?:
   a. Reactiva.
   b. De análisis forense y lecciones aprendidas.
   c. Proactiva y Preventiva.

10- ¿Cuáles son las principales ventajas de disponer de un SOC?:
   a. El análisis de los datos con posterioridad a una incidencia.
   b. El almacenamiento de datos relevantes en relación con los incidentes. c. Todas las anteriores.
   c. La contralización de la actividad de ciberseguridad de la empresa.

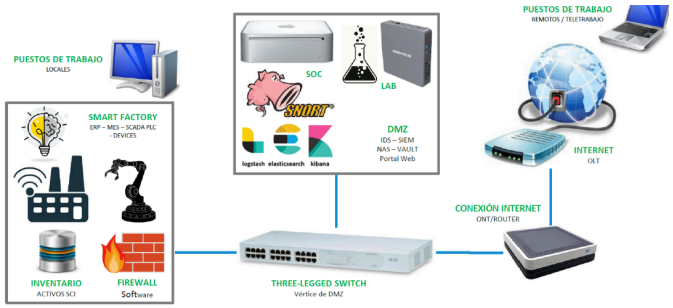
Los Procedimientos de Actuación ante Incidentes

Como hemos estudiado en la Unidad 4, en los momentos iniciales de manifestación de un incidente suele existir un cierto desconcierto en lo relativo a las medidas que se deben tomar, por parte de quién y en qué orden, lo cual suele aumentar la afectación del incidente. Este desconcierto se combate diseñando un Procedimiento de Actuación ante Incidentes. Este procedimiento suele ser de alto nivel y podrá desglosarse en tareas concretas en función del área involucrada en cada caso, o bien, en flujos de decisión y escalado para constituir la Estrategia de Contención de Incidentes de Ciberseguridad.

Introducción: Estructura de la Organización Empresarial.

Dada una empresa como la descrita en la tarea de la unidad de trabajo 1 en la que se sigue el siguiente diagrama de bloques:

Además, esta empresa sigue la siguiente estructura organizativa:



La determinación de la Estructura de la Empresa Ficticia nos permitirá identificar sus áreas de trabajo y las misiones de las mismas , con objeto de saber a qué equipos hay que involucrar en cada momento y cuándo se les debe informar acerca de los incidentes:

- **CEO (Chief Executive Officer): Presidente. Gestión y Dirección administrativa.**
- **COO (Chief Operating Officer): Director de Operaciones.**
- **CFO (Chief Financial Officer): Director de Gestión Financiera.**
- **CMO (Chief Marketing Officer): Director de Actividades Comerciales y de Marketing.**
- **CIO (Chief Information Officer): Director de Sistemas de Información y Desarrollo de Aplicaciones.**
- **CTO (Chief Technology Officer): Director de Tecnología y Estrategia Tecnológica.**
- **CSO (Chief Security Officer): Responsable de Planificación y Estrategia de Seguridad.**
- **CISO (Chief Information Security Officer): Responsable de Ciberseguridad.**
- **CLO (Chief Legal Officer): Responsable del Departamento Jurídico. Es clave para la ciberseguridad.**
- **CDO (Chief Design Officer): Responsable de Diseño.**

Con esta información proporcionada se tiene una idea general de la estructura de la empresa. El grupo de trabajadores de cada departamento y la inclusión de otros posibles departamentos queda a libre elección del alumno.

A continuación, se desglosan en apartados el desarrollo general de un Plan de Actuación ante Incidentes de Ciberseguridad. En este Plan de Actuación no se solicitan detalles a bajo nivel de herramientas a usar, solamente una guía de actuación general.

***Nota: Se debe realizar un único documento con los apartados, pero no en formato pregunta respuesta, sino como un documento de "Plan de Actuación ante incidentes" desarrollado para esta empresa.**

Aunque los recursos adicionales propuestos para consulta y ayuda son documentos de una extensión considerable, este documento no necesita una elevada extensión. La extensión puede estar comprendida entre 7 y 14 páginas contando portada e índice. Esta es una orientación, se pueden realizar entregas de otras extensiones.

Apartado 1: Manifestación y detección del incidente.

Deberás efectuar la siguiente tarea:

Describir procesos para identificación, recopilación de evidencias y evaluación inicial de incidentes.

Apartado 2: Definir los roles de las personas y formación del equipo de respuesta.

Deberás efectuar la siguiente tarea:

Definir qué funciones tendrá asignadas cada rol definido en caso de un incidente. Llamada a filas del equipo en caso de incidente.

Indicar los miembros de alta prioridad a los que se les trasladará información preliminar.

Apartado 3: Concreción del incidente.

Deberás efectuar la siguiente tarea:

Indicar principales pasos o preguntas a realizar para detectar de forma más concreta el tipo de incidente que puede estar sucediendo.

Personal de empresa a los que informar.

Apartado 4: Medidas de actuación ante diferentes tipos de incidentes.
Deberás efectuar la siguiente tarea:
a. Descripción general de las fases de contención, mitigación, o eliminación de los incidentes.
b. Describir de forma concreta estas fases para un tipo específico de incidente (Playbook). Los tipos a elegir son: infección por gusanos, phishing, malware en Windows, DDOS y ransomware.
Apartado 5: Proceso de revisión, documentación y mejora.
Deberás efectuar la siguiente tarea:
Definir el proceso de cierre de la incidencia, la documentación asociada, el aprendizaje adquirido y proceso de mejora.
Traslado de información a las personas o entidades necesarias.
Recursos:
Se trata de un ejercicio teórico de investigación, por lo que sólo hará falta:
Adicionalmente se pueden usar los siguientes recursos auxiliares:
Plantilla traducida al español de "Respuesta a Incidentes" basada en la plantilla creada por el equipo de "Counteractive Security" bajo licencia apache 2.0. Se puede trabajar con la plantilla adaptada al español o directamente con la "Plantilla original en inglés de Counteractive Security".
***Nota: Recurso recomendable para consulta – no entregar tal cual se genera.**
Ejemplo de playbook: Phishing.
Ejemplo de playbook: Malware en Windows.
Ejemplo de playbook: Gusanos.
Vídeo motivacional: Respuesta ante incidentes (Deloitte).
Guía nacional de notificación y gestión de ciberincidentes.
Ciber-resiliencia. Aproximación a un marco de medición.

Plan de actuación ante incidentes de ciberseguridad

Manifestación y detección del incidente. Procesos que van a ayudar a la identificación, recopilación de incidencias y evaluación inicial de incidentes.

Identificación del incidente

1. Monitoreo continuo: utilizar herramientas de monitoreo como IDS (Intrusion Detection System) y SIEM (Security Information and Event Management) para detectar actividades anómalas.
2. Alertas y notificaciones: configurar alertas automáticas para actividades sospechosas. Estas alertas deben ser revisadas por el SOC (Security Operations Center).
3. Reportes manuales: permitir a los empleados reportar incidentes sospechosos a través de un canal de comunicación.

Recopilación de evidencias:

1. Registro de logs del sistema: asegurar que todos los sistemas críticos, recopilen y analicen registros logs detallados de actividades de servidores, aplicaciones y dispositivos de red.
2. Captura el tráfico de la red: utilizar herramientas como snort para capturar y analizar el tráfico de red, pudiendo identificar comunicaciones sospechosas.
3. Tratamiento de incidentes: tomar instantáneas del estado de los sistemas afectados en el momento del incidente, antes de aislar los dispositivos afectados para evitar perder datos o alterar las evidencias.

Evaluación inicial del incidente

1. Análisis previo, realizar un análisis inicial para verificar la existencia del incidente, revisando las alertas y las evidencias.
2. Clasificación del incidente, clasificar el incidente según su severidad y tipo (Malware, phishing, DDos…).
3. Evaluar la gravedad del incidente, basándose en el impacto potencial en la empresa.
4. Notificación, informar a los miembros del equipo de ciberseguridad (al CISO y al CSO) y a la dirección sobre el incidente para una evaluación más detallada.

Definir los roles de las personas y formación del equipo de respuesta.

Especificar funciones asignadas a cada rol en caso de un incidente.

Roles y funciones

1. CISO (Chief Information Security Officer), coordina la respuesta al incidente, la toma de decisiones estratégicas y la comunicación con la alta dirección. Supervisa la implementación de medidas de contención y mitigación.
2. SOC (Security Operations Center), monitorea y analiza las alertas de seguridad, realiza la detección y respuesta inicial, proporciona informes detallados sobre el incidente. Se encarga de coordinar al equipo de TI.
3. Equipo TI, implementa medidas técnicas para contener y mitigar el incidente, realiza análisis forense de los sistemas afectados, asegura la restauración de los sistemas y servicios afectados.
4. Departamento legal (CLO), asegura el cumplimiento de las leyes y regulaciones y proporciona asesoramiento legal (en caso de ser necesario coordina a las autoridades regulatorias).
5. Comunicación (CMO), gestiona la comunicación interna y externa sobre el incidente, prepara comunicados de prensa y declaraciones públicas, informa a los empleados sobre el estado del incidente y coordina con el departamento legal para asegurar la precisión de la información divulgada.

Llamada a filas del equipo:

1. Activación del equipo: el CISO activa el equipo de respuesta ante incidentes tras la evaluación inicial. Se notifica a todos los miembros del equipo de respuesta.
2. Asignación de tareas: cada miembro del equipo recibe tareas específicas según su rol. El SOC coordina las actividades iniciales de detección y análisis, el equipo de TI implementa las medidas de contención y mitigación y el departamento legal, junto con el CMO gestionan la comunicación y el cumplimiento normativo.

Miembros de alta prioridad

1. CEO, recibe información preliminar y actualizaciones regulares. Toma las decisiones críticas sobre la continuidad del negocio y la comunicación externa.
2. CSO, informa sobre la estrategia de seguridad y coordina con el CISO. Supervisa la implementación de la estratégia de respuesta al incidente.
3. COO: asegura la continuidad operativa durante el incidente y coordina con el equipo de operaciones para minimizar el impacto en las actividades diarias de la empresa.

Concreción del incidente

Pasos para detectar de forma más concreta el tipo de incidente

1. Análisis de logs, revisar registros de actividad para identificar patrones específicos del incidente, identificando eventos inusuales registrados y a que usuarios o sistemas involucra.
2. Entrevistar al personal del sistema afectado para poder obtener alguna información extra.
3. Herramientas de análisis, se utilizarán herramientas de análisis forense para examinar sistemas y redes comprometidas. Habrá que averiguar qué vulnerabilidades fueron explotadas y qué tipo de malware puede ser el causante.
4. Consultas con expertos, involucrar a expertos internos o externos para una evaluación detallada. Viene bien saber la opinión de alguien con conocimiento para saber sus recomendaciones y procedimientos adicionales.

Personal de la empresa a informar

1. CISO y CSO, para evaluar y coordinar la respuesta ante el incidente
2. Equipo TI, para implementar las medidas técnicas necesarias.
3. Departamento legal, para asegurar el cumplimiento normativo.
4. Miembros de alta prioridad:
    a. CEO, recibe información preliminar y actualizaciones regulares.
    b. CSO, informa sobre la estrategia de seguridad y coordina con el CISO.
    c. COO: asegura la continuidad operativa durante el incidente.

Medidas de actualización ante diferentes tipos de incidentes.

Descripción general de las fases de contención mitigación o eliminación de los incidentes

La gestión de incidentes de ciberseguridad se estructura en varias fases que permiten una respuesta organizada y efectiva.

1. Detección y análisis, esta fase tiene como objetivo identificar y comprender el incidente lo más rápidamente posible.

Se debe llevar un monitoreo continuo con herramientas como IDS y SIEM para detectar actividades sospechosas en tiempo real.

Tener alertas automáticas para cuando haya eventos inusuales o comportamientos anómalos, que se avise en el momento.

Análisis de logs, revisar el registro de actividad de los servidores, aplicaciones y dispositivos de pred para identificar patrones específicos del incidente.

Capturar el tráfico en red, realizar este tipo de capturas es beneficioso para identificar comunicaciones sospechosas.

Consultar con expertos, involucrar a personas con alto conocimiento puede aportar una evaluación más detallada del incidente.

2. Contención, su objetivo es limitar la propagación del incidente para minimizar su impacto.

Aislamiento de sistemas, desconectar los sistemas afectados de la red para evitar la propagación del incidente.

Bloqueo de accesos, implementar reglas de firewall para bloquear el tráfico malicioso y deshabilitar cuentas comprometidas.

Segmentación de la red, utilizar la segmentación de la red para contener incidentes dentro de una parte específica de la infraestructura.

Medidas temporales, aplicar configuraciones de emergencia para mitigar el impacto.

3. Erradicación, eliminar la causa raíz del incidente y asegurar que no vuelva a ocurrir.

Identificación de la causa raíz, mediante un análisis exhaustivo, identificar como ocurrió el incidente y encontrar la vulnerabilidad.

Eliminar el malware, utilizar herramientas de eliminación adecuadas para limpiar los sistemas afectados.

Actualizar y reconfigurar los sistemas aplicando parches y ajustar configuraciones para corregir las vulnerabilidades

4. Recuperación, restaurar los sistemas y servicios afectados.

Restauración de datos, recuperar los datos de la copia de seguridad, verificando la integridad de la información.

Reconectar los sistemas restaurados a la red y asegurarse de que funcionan correctamente.

Continuar monitorizando los sistemas para detectar cualquier actividad residual.

5. Revisión, analizar el incidente y mejorar los procesos para prevenir futuros incidentes.

Evaluar el impacto del incidente en los sistemas, los datos y las operaciones

Documentación, registrar todos los hallazgos, acciones tomadas y lecciones aprendidas durante la gestión del incidente.

Previsión después del incidente, reunir al equipo para discutir lo ocurrido y extraer lecciones para mejorar futuras respuestas.

Actualizar políticas de seguridad basadas en lo aprendido y además, incluir formación para el personal para mejorar la respuesta ante incidentes.

Playbook para un ataque de phising

Un playbook para un atacante de phishing detalla los pasos específicos a seguir para gestionar este tipo de incidentes de manera efectiva.

1. Detección: identificar correos sospechosos y alertar a los usuarios.

Utilizar filtros de correo electrónico avanzados para detectar y bloquear correos electrónicos sospechosos antes de que lleguen a los usuarios.

Alertas de SIEM, configurar estas alertas para notificar al equipo de seguridad sobre posibles intentos de phishing.

Educar y concienciar a los empleados para que reconozcan correos de phishing y reporten cualquier sospecha al equipo de seguridad.

Utilizar herramientas de análisis de correo para identificar patrones comunes en los correos de phishing.

2. Contención: limitar la propagación del incidente y proteger los sistemas comprometidos

Configurar reglas en el servidor de correo para bloquear correos de posible phishing.

Aislar el sistema comprometido de la red, para evitar la propagación del malware.
Deshabilitar cuentas comprometidas para evitar accesos no deseados.
Implementar reglas de firewall para bloquear las direcciones IP maliciosas (origen correos maliciosos)

3. Erradicación: eliminar el malware instalado y asegurar que no pueda volver a ocurrir.

Utilizar herramientas de antivirus y antimalware para escanear y limpiar los sistemas comprometidos.
Restablecer las credenciales de las cuentas comprometidas.
Aplicar parches y actualizaciones a los sistemas con vulnerabilidades.
Ajustar las configuraciones de seguridad para prevenir futuros incidentes.

4. Recuperación: restaurar los sistemas Y servicios afectados desde las copias de seguridad limpias.

Recuperar los datos y restaurarlos desde las copias de seguridad para asegurar la integridad de la información.
Verificar la integridad de los datos, con pruebas exhaustivas para asegurar que los sistemas restaurados no hayan sido afectados por el incidente.
Reconectar los sistemas restaurados y asegurar que funcionen correctamente.
Monitorear, después del incidente, los sistemas para detectar cualquier actividad residual

5. Revisión, analizar el ataque y mejorar los procesos para prevenir futuros incidentes

Determinar el impacto del ataque en los sistemas, los datos y las operaciones.
Registrar los hallazgos, acciones tomadas y lecciones aprendidas.
Revisión después del incidente, reunir al equipo para discutir lo ocurrido y poner en común las mejoras para futuras respuestas.
Revisión y actualización de políticas de seguridad basadas en las lecciones aprendidas.
Dar formación al personal para capacitarlos ante incidentes y actualizar el procedimiento de respuesta.

Procesos de revisión, documentación y mejora

Proceso de cierre de la incidencia

1. Evaluación del impacto, determinar el impacto en los sistemas, analizando el rendimiento de los sistemas antes y después del incidente. Identificando fallos o interrupciones en los servicios afectados. Verificar el impacto sobre los datos, evaluar si ha habido algún acceso no autorizado y si los datos han estado inaccesibles en algún periodo de tiempo. En el tiempo de inactividad y calcular la pérdida económica causada por el incidente, evaluar el impacto en la reputación y la confianza de la empresa.
2. Documentación, de escribir detalladamente cómo ocurrió el incidente, añadiendo línea de tiempo y eventos clave, anotar las acciones realizadas para erradicar el incidente e incluir las evidencias recopiladas durante la información (logs, tráfico de red…). Analizar e identificar la causa raíz y como se explotaron las vulnerabilidades, analizar la efectividad de la respuesta y las áreas a mejorar.
3. Revisión después del incidente, reunir al equipo para discutir lo ocurrido y extraer lecciones. Medir el tiempo de inactividad y su efecto en las operaciones diarias, calcular pérdidas financieras directas e indirectas causadas por el incidente, evaluar el impacto en la reputación de la empresa y la confianza de los clientes. Proponer recomendaciones específicas para mejorar la seguridad en próximas ocasiones.

Procesos de mejora

1. Revisión de políticas, actualizar las políticas de seguridad basadas en las lecciones aprendidas.
2. Capacitar al personal dándoles formación para la respuesta ante incidentes.
3. Actualización de herramientas, implementar nuevas herramientas o mejoras existentes.

Traslado de información a las personas o entidades necesarias.
Respecto al Personal Interno:

- CEO: Informar sobre el impacto estratégico y las decisiones tomadas.
- CSO: Coordinar la estrategia de seguridad general y las mejoras necesarias.
- CISO: Detallar las acciones de ciberseguridad y las lecciones aprendidas.
- CTO: Gestionar la recuperación técnica y las actualizaciones de sistemas.
- COO: Asegurar la continuidad operativa y minimizar interrupciones futuras.
- CFO: Evaluar el impacto financiero y gestionar los recursos necesarios.
- CLO: Asegurar el cumplimiento legal y gestionar posibles repercusiones legales.

Respecto al Personal Externo:

- Proveedores de Servicios: Informar sobre el incidente y coordinar acciones para mitigar cualquier impacto en los servicios proporcionados.
- Autoridades Legales: Notificar a las autoridades competentes según los requisitos legales y regulatorios.
- Clientes Afectados: Comunicar a los clientes afectados sobre el incidente, las acciones tomadas y las medidas para prevenir futuros incidentes.

El plan proporciona una guía clara y estructurada para la detección, la respuesta y la gestión de incidentes de ciberseguridad en la empresa, asegurando una respuesta eficaz y coordinada.