TAREA 04

IMPLEMENTACIÓN DE MEDIDAS DE CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

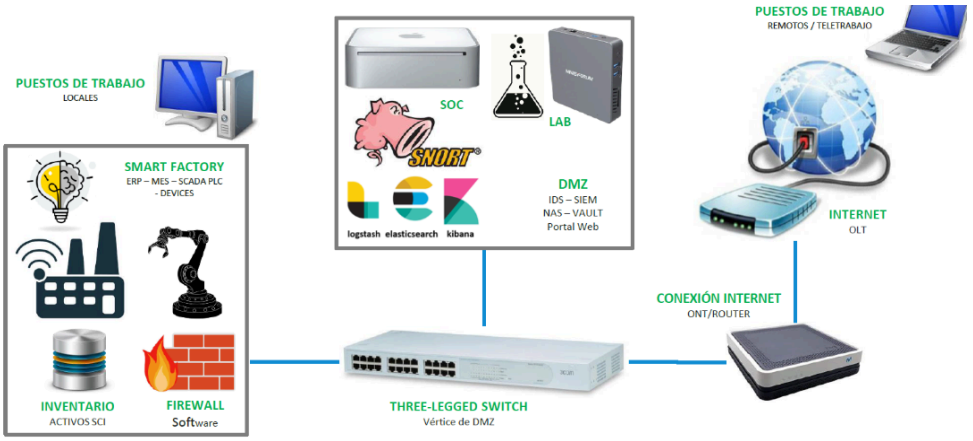
ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

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.