Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Incidentes de Ciberseguridad

UD04. Plan de respuesta ante incidentes.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Los Procedimientos de Actuación ante Incidentes

INCIBE. Procedimiento Actuación ante Incidentes (CC0)

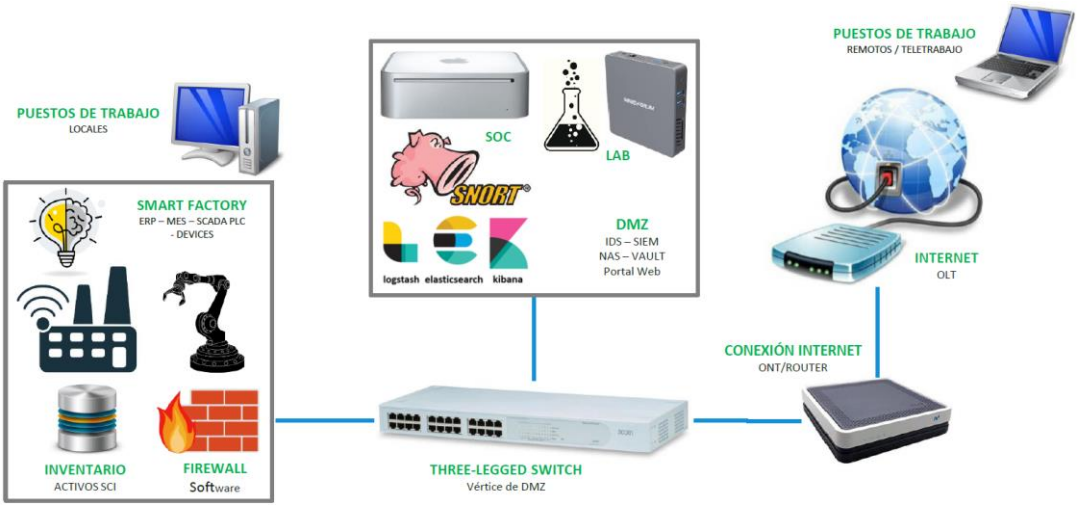
Como hemos estudiado en la Unidad 4, en los momentos iniciales de manifestación de un incidente suele existir un cierto desconcierto en lo relativo a las medidas que se deben tomar, por parte de quién y en qué orden, lo cual suele aumentar la afectación del incidente.

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.

¿Qué te pedimos que hagas?

- ✓ **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 que 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.

Plan de Actuación ante incidentes para Empresa Ficticia SA.

Autor: Juan Antonio García Muelas, juangmuelas@gmail.com

Revisión 2.1, Publicada el 16 de febrero de 2024.

Índice de Contenidos

Plan de Actuación ante incidentes para Empresa Ficticia SA.

Autor: Juan Antonio García Muelas, juangmuelas@gmail.com

Revisión 2.1, Publicada el 16 de febrero de 2024.

Procesos para Identificación, Recopilación de Evidencias y Evaluación Inicial de Incidentes

Identificación de Incidentes

Debe identificar el alcance del daño e intentar realizar las primeras acciones para detener y mitigar la incidencia.

La identificación de un incidente podrá ser activa, observando un incidente en directo, o pasiva, observando ciertos comportamientos anómalos.

Se deberán identificar los activos afectados para poder contener el problema. Imprescindible la comunicación del equipo con las personas involucradas, debiendo recopilar y documentar la mayor cantidad de información que sea posible, para así determinar con mayor eficacia los activos involucrados en el incidente.

Monitorización

- ✓ Implementar un sistema de monitorización de redes y sistemas, formado por:
  - IDS/SIEM para la prevención y detección de intrusiones y anomalías.
  - Firewall para controlar el tráfico entrante y saliente de la red.
  - Software antivirus y antispyware actualizado para detectar y eliminar malware.
  - Herramientas de análisis de logs para facilitar la identificación de eventos sospechosos.

Revisión de logs y alertas

- ✓ Establecer un proceso para la revisión regular de logs y alertas de seguridad:
  - ➢ Definir roles y responsabilidades para la revisión de logs.
  - ➢ Priorizar la revisión de logs de sistemas críticos y sensibles.
  - ➢ Utilizar herramientas de análisis de logs para facilitar la identificación de patrones y actividades sospechosas.

Notificación de incidentes

- ✓ Definir canales de comunicación para la notificación de incidentes:
  - ➢ Implementar un sistema de tickets para centralizar la recepción de informes de incidentes.
  - ➢ Establecer un sistema de alertas para notificar al equipo de respuesta a incidentes.
  - ➢ Definir un plan de comunicación para informar a los empleados y a las distintas partes interesadas.

Análisis de vulnerabilidades y riesgos

- ✓ Realizar análisis periódicos de vulnerabilidades para identificar y mitigar riesgos:
  - ➢ Utilizar las distintas herramientas de escaneo de vulnerabilidades para poder identificar las debilidades del sistema.
  - ➢ Evaluar el impacto potencial de las vulnerabilidades detectadas y priorizar su corrección.
  - ➢ Implementar medidas de seguridad adecuadas para mitigar los riesgos detectados.

Recopilación de Evidencias

Preservación de la cadena de custodia

- ✓ Asegurar la integridad de las pruebas mediante la preservación de la cadena de custodia:
  - ➢ Documentar el proceso de recopilación de pruebas.
  - ➢ Almacenar las pruebas de forma segura y confidencial.
  - ➢ Limitar el acceso a las pruebas al personal autorizado.

Recopilación de pruebas digitales

- ✓ Identificar y recopilar las pruebas digitales relevantes para el incidente:
  - ➢ Captura de imágenes de disco de los sistemas afectados.
  - ➢ Recopilación de logs y archivos relevantes.
  - ➢ Análisis de volatilidad de la memoria.
  - ➢ Recopilación de información de las redes sociales y otras fuentes.

Recopilación de pruebas físicas

- ✓ En caso de ser necesario, recopilar pruebas físicas:
  - ➢ Dispositivos de almacenamiento.
  - ➢ Equipos informáticos.
  - ➢ Documentación en papel.

Documentación del proceso

- ✓ Documentar el proceso de recopilación de pruebas:
  - Detallar las pruebas recopiladas.
  - Describir el método de recopilación.
  - Identificar a las personas que participaron en la recopilación.

Evaluación Inicial del Incidente

Determinación de la naturaleza del incidente

- ✓ Clasificar el tipo de incidente:
  - Malware
  - Phishing
  - DDoS
  - Acceso no autorizado
  - Denegación de servicio
  - Catástrofes naturales
  - Fuga de datos

Evaluación del impacto del incidente

- ✓ Evaluar el impacto del incidente en la empresa:
  - Impacto financiero.
  - Impacto reputacional.
  - Impacto operativo.
  - Pérdida de datos.
  - Interrupción del servicio.

Priorización de la respuesta

- ✓ Priorizar la respuesta al incidente en base a su severidad e impacto:
  - Incidentes críticos: requieren de una respuesta inmediata y la activación del plan de respuesta a incidentes.
  - Incidentes de alta prioridad: requieren de una respuesta rápida y la asignación de recursos adicionales.
  - Incidentes de baja prioridad: pueden ser resueltos con la atención normal.

Notificación a las partes interesadas

- ✓ Notificar a las partes interesadas sobre el incidente:
  - Equipo de respuesta a incidentes.
  - Alta dirección.
  - Clientes o colaboradores afectados.
  - Autoridades o entidades legales (en caso de ser necesario).

Documentación de la evaluación

- ✓ Documentar los resultados de la evaluación inicial:
  - Naturaleza del incidente.
  - Impacto del incidente.
  - Prioridad de la respuesta.
  - Acciones tomadas.

Roles y Funciones en caso de un Incidente de Seguridad

Definición de Roles y Funciones

Equipo de Respuesta a Incidentes (ERI)

- ✓ **Responsable del ERI:** CISO (Chief Information Security Officer)
  - ➢ Lidera la respuesta al incidente y coordina las acciones.
- ✓ **Miembros del ERI:**
  - ➢ CIO (Chief Information Officer):
    - ▪ Soporte técnico y análisis forense.
  - ➢ CTO (Chief Technology Officer):
    - ▪ Análisis de riesgos y medidas de contención.
  - ➢ CSO (Chief Security Officer):
    - ▪ Comunicación interna y externa.
  - ➢ Expertos en seguridad informática:
    - ▪ Soporte técnico especializado.
  - ➢ Personal de TI:
    - ▪ Implementación de las medidas de contención y recuperación.
  - ➢ Representantes legales:
    - ▪ Asesoramiento legal y cumplimiento normativo.

Funciones específicas por rol

Responsable del ERI:

- ✓ Toma de decisiones sobre la respuesta al incidente.
- ✓ Coordina las acciones de los diferentes equipos.
- ✓ Informa a la alta dirección sobre el estado del incidente.

CIO:

- ✓ Realiza el análisis forense para determinar la causa del incidente.
- ✓ Implementa las medidas de contención para evitar la propagación del incidente.
- ✓ Restaura los sistemas afectados.

CTO:

- ✓ Evalúa el impacto del incidente en la empresa.
- ✓ Recomienda medidas de seguridad para prevenir futuros incidentes.

CSO:

- ✓ Informa a los empleados y colaboradores sobre el incidente.
- ✓ Gestiona la comunicación con los medios de comunicación.

Expertos en seguridad informática:

- ✓ Aportan su conocimiento técnico para la investigación del incidente.
- ✓ Recomiendan medidas de seguridad para mitigar el impacto del incidente.

Personal de TI:

- ✓ Implementa las medidas de contención y recuperación.
- ✓ Brinda soporte técnico a los usuarios afectados.

Representantes legales:

- ✓ Asesoran sobre las implicaciones legales del incidente.
- ✓ Ayudan a cumplir con las normativas de protección de datos.

Llamada a filas del equipo

- ✓ El responsable del ERI determina el nivel de severidad del incidente.
- ✓ En función de la severidad, se activa el plan de respuesta a incidentes y se convoca al equipo necesario.
- ✓ Se utilizan diferentes canales de comunicación para notificar al equipo (correo electrónico, llamadas telefónicas, herramientas de mensajería instantánea).

Miembros de alta prioridad a los que se les traslada información preliminar

- ✓ CEO (Chief Executive Officer)
- ✓ COO (Chief Operating Officer)
- ✓ CFO (Chief Financial Officer)
- ✓ CLO (Chief Legal Officer)

Información preliminar:

- ✓ Tipo de incidente y su naturaleza.
- ✓ Impacto potencial en la empresa.
- ✓ Acciones inmediatas tomadas.
- ✓ Pronóstico de la evolución del incidente.

Pasos y Preguntas en la Detección Concreta del Tipo de Incidente

Pasos

Recopilación de información

- ✓ **Identificar la fuente del problema:** ¿Usuario, sistema, red?
- ✓ **Analizar los síntomas:** ¿Mensajes de error, comportamiento inusual, lentitud?
- ✓ **Revisar los logs y alertas:** ¿Eventos sospechosos, actividad inusual?
- ✓ **Consultar con el personal afectado:** ¿Qué han observado? ¿qué acciones han realizado?

Análisis

- ✓ **Correlacionar la información:** Buscar patrones y relaciones entre los datos recopilados.
- ✓ **Evaluar el contexto:** ¿Ha habido cambios recientes en la infraestructura o en las aplicaciones?
- ✓ **Considerar las amenazas conocidas:** ¿Se asemeja el incidente a un ataque conocido?

Preguntas

- ✓ ¿Qué tipo de actividad inusual se ha detectado?
- ✓ ¿Cuándo se observó por primera vez el problema?
- ✓ ¿Cuántos usuarios o sistemas están afectados?
- ✓ ¿Qué medidas se han tomado hasta el momento?
- ✓ ¿Se ha detectado actividad similar en el pasado?

Preguntas para determinar el tipo de incidente:

Malware

- ✓ ¿Se han detectado archivos o procesos sospechosos?
- ✓ ¿Se ha producido un aumento en el uso del CPU o de la red?
- ✓ ¿Se han recibido mensajes de error o alertas de antivirus?

Phishing

- ✓ ¿Se han recibido correos electrónicos o mensajes sospechosos?
- ✓ ¿Los enlaces o archivos adjuntos parecen confiables?
- ✓ ¿Se ha iniciado sesión en sitios web fraudulentos?

DDoS

- ✓ ¿Se ha producido una caída repentina del servicio?
- ✓ ¿Se ha observado un aumento inusual en el tráfico de red?
- ✓ ¿Se han recibido mensajes de error relacionados con la capacidad del servidor?

Acceso no autorizado

- ✓ ¿Se han detectado inicios de sesión inusuales o fallidos?
- ✓ ¿Se han modificado archivos o configuraciones sin autorización?
- ✓ ¿Se han detectado actividades sospechosas en las cuentas de usuario?

Personal a informar:

- ✓ **Equipo de respuesta a incidentes:** Deben ser informados de inmediato para que puedan iniciar la investigación y la respuesta.
- ✓ **Alta dirección:** Deben ser informados sobre la gravedad del incidente y las medidas que se están tomando.
- ✓ **Clientes o socios afectados:** Deben ser informados si el incidente ha impactado sus datos o servicios.
- ✓ **Autoridades o entidades legales:** Deben ser informados si el incidente se sospecha que es un delito.

Contención, Mitigación y Eliminación de Incidentes. Playbook para Ransomware.

Contención

- ✓ **Objetivo:** Limitar el alcance del daño, recopilar evidencias y evitar su propagación.
- ✓ **Acciones:**
  - ➢ Aislar los sistemas afectados: Desconexión de la red, cuarentena de equipos afectados.
  - ➢ Detener la actividad maliciosa: Desactivación de cuentas, eliminación de malware.
  - ➢ Preservar la evidencia: Captura de imágenes de disco, registro de logs.

Mitigación

- ✓ **Objetivo:** Reducir el impacto del incidente en la empresa.

- ✓ **Acciones:**
  - ➢ Implementar medidas de seguridad adicionales: Fortalecimiento de firewalls, actualización de software.
  - ➢ Restaurar los sistemas afectados: Backups, imágenes de disco.
  - ➢ Comunicar a los usuarios y partes interesadas: Informar sobre el incidente, medidas tomadas.

Eliminación

- ✓ **Objetivo:** Eliminar la amenaza de forma permanente y prevenir su recurrencia.
- ✓ **Acciones:**
  - ➢ Eliminación del malware: Eliminación de archivos infectados, limpieza del sistema.
  - ➢ Reparación de las vulnerabilidades: Actualización de software, parcheo de vulnerabilidades.
  - ➢ Aprendizaje del incidente: Análisis de la causa raíz, mejora de la respuesta a futuros incidentes.

Playbook para Ransomware

Investigar, remediar (contener, erradicar), y comunicar en paralelo. La contención es crítica en los incidentes de ransomware, priorice en consecuencia.

Asigne pasos a individuos o equipos para que trabajen simultáneamente, cuando sea posible; este playbook no es puramente secuencial. Utilice su mejor criterio.

Investigar

1. **Determinar el tipo** de ransomware (es decir, ¿Cuál es la familia, la variante o el tipo?)

- ✓ Encuentre cualquier mensaje relacionado. Compruebe:
  - ➢ Las interfaces gráficas de usuario (GUIs) del propio malware.
  - ➢ Archivos de texto o html, que a veces se abren automáticamente tras el cifrado.
  - ➢ Archivos de imagen, a menudo como fondo de pantalla en los sistemas infectados.
  - ➢ Correos electrónicos de contacto en extensiones de archivos encriptados.
  - ➢ Ventanas emergentes después de intentar abrir un archivo encriptado.
  - ➢ Mensajes de voz.
- ✓ Analice los mensajes en busca de pistas sobre el tipo de ransomware:
  - ➢ Nombre del ransomware.
  - ➢ Lenguaje, estructura, frases, material gráfico.
  - ➢ Correo electrónico de contacto.
  - ➢ Formato de la identificación del usuario.
  - ➢ Especificaciones de la demanda de rescate (ej., moneda digital, tarjetas de regalo)
  - ➢ Dirección de pago en caso de moneda digital.
  - ➢ Chat de soporte o página de soporte.
- ✓ Analice los archivos afectados y/o nuevos. Compruebe:
  - ➢ El esquema de cambio de nombre de los archivos encriptados, incluyendo la extensión (`.crypt`, `.cry`, `.locked`) y el nombre base.
  - ➢ Corrupción de archivos frente a encriptación.
  - ➢ Tipos de archivos y ubicaciones específicas.
  - ➢ Usuario/grupo propietario de los archivos afectados.

- Icono de los archivos encriptados.
- Marcadores de archivos.
- Existencia de listados de archivos, archivos clave u otros archivos de datos.

✓ Analice los tipos de software o sistemas afectados. Algunas variantes de ransomware sólo afectan a determinadas herramientas o plataformas.

✓ Subir los indicadores a servicios de categorización automatizados como Crypto Sheriff, ID Ransomware, o similar.

2. Determinar el alcance:

✓ ¿Qué sistemas están afectados?
- Busque indicadores de compromiso (IOCs), como archivos/hashes, procesos, conexiones de red, etc. Utilice protección endpoint/EDR, telemetría endpoint, logs del sistema, etc.
- Comprobar la infección de sistemas similares (ej., usuarios, grupos, datos, herramientas, departamento, configuración, estado de los parches): comprobar herramientas IAM, [herramientas de administración de permisos, servicios de directorio, etc.
- Encontrar comando & control externo (C2), si está presente, y encuentra otros sistemas que se conecten a él: comprobar firewall o logs de IDS, logs de sistemas/EDR, logs DNS, logs de netflow o router, etc.

✓ ¿Qué datos están afectados? (ej., tipos de archivo, departamento o grupo, software afectado).
- Buscar cambios anómalos en los metadatos de los archivos, como cambios masivos en las horas de creación o modificación. Comprobar herramientas de búsqueda de metadatos de archivos.
- Buscar cambios en archivos de datos normalmente-estables o críticos. Comprobar herramientas de monitorización de integridad de archivos.

3. Evaluar el impacto para priorizar y motivar los recursos.

✓ Evaluar el impacto funcional: impacto en la empresa o en la misión.
- ¿Cuánto dinero se pierde o está en riesgo?
- ¿Cuántas (y cuáles) misiones se degradan o están en riesgo?

✓ Evaluar el impacto en la información: impacto en la confidencialidad, integridad y disponibilidad de los datos.
- ¿Qué importancia tienen los datos para la empresa/misión?
- ¿Cuán sensibles son los datos? (ej., secretos comerciales)
- ¿Cuál es la situación reglamentaria de los datos (ej., PII, PHI)?

4. Encuentra el vector de infección. Comprueba las tácticas capturadas en la Initial Access tactic de MITRE ATT&CK. Las especificaciones y fuentes de datos más comunes son:

- Archivo adjunto de correo electrónico: comprobar logs de correo electrónico, dispositivos y servicios de seguridad del correo electrónico, herramientas e-discovery, etc.
- Protocolo de escritorio remoto inseguro (RDP): comprueba resultado de escaneo de vulnerabilidades, configuraciones del firewall, etc.
- Auto-propagación (gusano o virus) (comprueba telemetría del host/EDR, logs del sistema, análisis forense, etc.)
- Infección vía dispositivos extraíbles (gusano o virus)

Remediar

Planificar eventos de remediación en los que estos pasos se lancen juntos (o de forma coordinada), con los equipos apropiados listos para responder a cualquier interrupción.

Considere el momento y las compensaciones de las acciones de remediación: su respuesta tiene consecuencias.

Contención

En situaciones de ransomware, la contención es crítica. Informar de las medidas de contención con los datos de la investigación. Dé mayor prioridad a las cuarentenas y otras medidas de contención que durante una respuesta típica.

Las cuarentenas (lógicas, físicas o ambas) impiden la propagación desde los sistemas infectados y evitan la propagación hacia los sistemas y datos críticos. Las cuarentenas deben ser exhaustivas: incluir el acceso a la nube/SaaS, el inicio de sesión único, el acceso a sistemas como el ERP u otras herramientas empresariales, etc.

- Poner en cuarentena los sistemas infectados
- Poner en cuarentena a los usuarios y grupos afectados.
- Ponga en cuarentena los archivos compartidos (no sólo los conocidos; proteja también los no infectados).
- Ponga en cuarentena las bases de datos compartidas (no sólo los servidores infectados conocidos; proteja también las bases de datos no infectadas)
- Ponga en cuarentena las copias de seguridad, si no están ya protegidas
- Bloquee los dominios y direcciones de comando & control
- Elimine los correos electrónicos vectoriales de las bandejas de entrada.
- Confirme que la protección de enpoints (AV, NGAV, EDR, etc.) está actualizada y activada en todos los sistemas.
- Confirmar que los parches se despliegan en todos los sistemas (priorizando los sistemas, SO's, software, etc.).
- Despliegue de firmas personalizadas en las herramientas de protección de endpoints y de seguridad de la red, basándose en los IOC's descubiertos.

Erradicar

- Reconstruir los sistemas infectados a partir de soportes conocidos como buenos.
- Restaurar a partir de copias de seguridad conocidas y limpias.
- Confirmar que la protección de los endpoints (AV, NGAV, EDR, etc.) está actualizada y activada en todos los sistemas.
- Confirmar que los parches se despliegan en todos los sistemas (dando prioridad a los sistemas, SO's, software, etc.).
- Despliegue de firmas personalizadas en las herramientas de protección de endpoints y de seguridad de la red, basándose en los IOC's descubiertos.
- **Vigilar la re-infección:** considerar el aumento de la prioridad de las alarmas/alertas relacionadas con este incidente.

Comunicar

- ✓ Escalar el incidente y comunicarlo a la dirección según el procedimiento.
- ✓ Documentar el incidente según procedimiento.

- ✓ Comunicarse con los asesores jurídicos internos y externos según el procedimiento, incluyendo discusiones sobre el cumplimiento, la exposición al riesgo, la responsabilidad, el contacto con las fuerzas del orden, etc.
- ✓ Comunicarse con los usuarios (internos)
- ✓ Comunicar las actualizaciones de la respuesta al incidente según el procedimiento.
- ✓ Comunicar el impacto del incidente y las acciones de respuesta al incidente (ej., contención: "¿Por qué está caído el archivo compartido?"), que pueda ser más intrusivo/disruptivo durante los incidentes de ransomware.
- ✓ Comunicar los requisitos: "¿Qué deben hacer y no hacer los usuarios?" Véase "Referencia: Acciones del usuario en caso de sospecha de ransomware", a continuación.
- ✓ Comuníquese con los clientes
  - ➢ Centrarse especialmente en aquellos cuyos datos se han visto afectados.
  - ➢ Genere las notificaciones requeridas en base a las regulaciones aplicables (particularmente aquellas que puedan considerar el ransomware como una violación de datos o que de alguna manera requieran notificaciones (ej., HHS/HIPAA))
- ✓ Póngase en contacto con los proveedore(s) de seguros
  - ➢ Discutir qué recursos pueden poner a disposición, qué herramientas y proveedores apoyan y pagarán, etc.
  - ➢ Cumplir con los requisitos de notificación y reclamación para proteger la elegibilidad.
- ✓ Comuníquese con los organismos reguladores, incluyendo una discusión sobre los recursos que pueden poner a su disposición (no sólo una notificación de tipo repetitivo: muchos pueden ayudar activamente).
- ✓ Considerar la posibilidad de notificar e implicar a las fuerzas del orden.
  - ➢ Aplicación de la ley local.
  - ➢ Aplicación de la ley local a nivel estatal o regional.
  - ➢ Fuerzas de seguridad europeas o nacionales
- ✓ Comuníquese con los proveedores de seguridad y de TI
  - ➢ Notificar y colaborar con los proveedores gestionados según el procedimiento.
  - ➢ Notificar y colaborar con los consultores de respuesta a incidentes según el procedimiento.

Recuperación

- ✓ Poner en marcha un plan de continuidad de la actividad/recuperación de desastres: ej., considerar la migración a ubicaciones operativas alternativas, sitios de conmutación por error, sistemas de respaldo.
- ✓ Recuperar los datos de las copias de seguridad ya limpias en sistemas ya limpios, parcheados y monitorizados (post-erradicación), de acuerdo con nuestra estrategia de copias de seguridad bien-testeadas.
  - ➢ Comprobar las copias de seguridad en busca de indicadores de compromiso.
  - ➢ Considerar la recuperación parcial y las pruebas de integridad de las copias de seguridad.
- ✓ Encuentre y pruebe desencriptadores conocidos para la(s) variante(s) descubierta(s) utilizando recursos como el proyecto ¡No More Ransom!.
- ✓ Considerar el pago del rescate por los activos/datos críticos irrecuperables, de acuerdo con la política interna.
- ✓ Considerar las ramificaciones con las partes interesadas apropiadas.
- ✓ Comprender las implicaciones financieras y el presupuesto.
- ✓ Comprender las implicaciones legales, reglamentarias y de seguros.

- ✓ Comprender los mecanismos (ej., tecnologías, plataformas, proveedores intermedios/intermediarios)

Recursos

Referencia: Acciones de los Usuarios ante la Sospecha de Ransomware

- ✓ Mantenga la calma y respire profundamente.
- ✓ Desconecte su sistema de la red `TODO: incluya pasos detallados con capturas de pantalla, una herramienta preinstalada o un script para facilitar esta tarea ("romper en caso de emergencia"), considere los interruptores de corte de red por hardware`.
- ✓ Haz fotos de tu pantalla con tu smartphone mostrando las cosas que has notado: mensajes de rescate, archivos encriptados, mensajes de error del sistema, etc.
- ✓ Toma notas sobre el problema o los problemas utilizando la aplicación de notas de voz de tu smartphone o con papel y boli. ¡Todo ayuda! Documenta lo siguiente:
  - ➢ ¿Qué has notado?
  - ➢ ¿Por qué pensaste que era un problema?
  - ➢ ¿Qué estabas haciendo en el momento en que lo detectaste?
  - ➢ ¿Cuándo se produjo por primera vez, y con qué frecuencia desde entonces?
  - ➢ ¿Dónde estaba cuando ocurrió y en qué red? (oficina/casa/tienda, con cable/inalámbrica, con/sin VPN, etc.)
  - ➢ ¿Qué sistemas está utilizando? (sistema operativo, nombre de host, etc.)
  - ➢ ¿Qué cuenta utilizas?
  - ➢ ¿A qué datos suele acceder?
  - ➢ ¿Con quién más se ha puesto en contacto en relación con este incidente y qué le ha dicho?
- ✓ Contacta al servicio de asistencia y ser lo más útil posible.
- ✓ Tenga paciencia: ¡la respuesta puede ser perturbadora, pero está protegiendo a su equipo y a la organización! **Gracias**.

Referencia: Acciones del Help Desk ante la Sospecha de Ransomware

- ✓ Mantenga la calma y respire profundamente.
- ✓ Abra un ticket para documentar el incidente, según el procedimiento
  - ➢ Pídale al usuario que tome fotos de su pantalla usando su smartphone mostrando las cosas que notó: mensajes de rescate, archivos encriptados, mensajes de error del sistema, etc. Si es algo que ha notado directamente, haga lo mismo usted.
- ✓ Toma notas sobre el problema o los problemas utilizando la aplicación de notas de voz de tu smartphone o con papel y boli. Si se trata de un informe de usuario, haz preguntas detalladas, incluyendo:
  - ➢ ¿Qué has notado?
  - ➢ ¿Por qué pensaste que era un problema?
  - ➢ ¿Qué estabas haciendo en el momento en que lo detectaste?
  - ➢ ¿Cuándo se produjo por primera vez, y con qué frecuencia desde entonces?
  - ➢ ¿De qué redes se trata? (oficina/casa/tienda, cableada/inalámbrica, con/sin VPN, etc.)
    - ¿De qué sistemas se trata? (sistema operativo, nombre de host, etc.)
    - ¿De qué datos se trata? (rutas, tipos de archivos, archivos compartidos, bases de datos, software, _etc._)
  - ➢ ¿Qué usuarios y cuentas están implicados? (directorio activo, SaaS, SSO, cuentas de servicio, etc.)

- ¿A qué datos suelen acceder los usuarios implicados?
- ¿Con quién más has contactado acerca de este incidente y qué les has dicho?

- ✓ Haz las preguntas de seguimiento que sean necesarias. **Usted es el encargado de responder al incidente, contamos con usted**.
- ✓ Obtenga información de contacto detallada del usuario (domicilio, oficina, móvil), si procede
- ✓ Registre toda la información en el ticket, incluyendo notas manuscritas y de voz
- ✓ Poner en cuarentena a los usuarios y sistemas afectados.
- ✓ Póngase en contacto con el equipo de seguridad y estar preparados para participar en la respuesta según las indicaciones: investigación, remediación, comunicación y recuperación

Información adicional

- ✓ "Identificación de Ransomware para el analista Juicioso", Hahn (12 Jun 2019)
- ✓ Incluyendo su Proyecto No More Ransom! su servicio Crypto Sheriff y su Q&A
- ✓ Servicio ID Ransomware.
- ✓ MITRE ATT&CK Matrix, incluyendo Accesos Iniciales y tácticas de Impacto.

Cierre de Incidencias: Proceso, Documentación, Aprendizaje y Mejora

Proceso de Cierre: Confirmar que el problema está resuelto de forma satisfactoria y no hay generados nuevos problemas.

Verificación de la resolución

- ✓ Asegurar que la amenaza ha sido eliminada y el problema resuelto.
- ✓ Realizar pruebas para confirmar la funcionalidad del sistema.
- ✓ Validar la satisfacción del usuario o cliente.

Documentación del cierre

- ✓ Registrar la fecha y hora del cierre.
- ✓ Detallar las acciones tomadas para resolver el incidente.
- ✓ Incluir la causa raíz del problema, si se ha identificado.
- ✓ Resumir las lecciones aprendidas y las recomendaciones para prevenir futuros incidentes.

Comunicación del cierre

- ✓ Informar al usuario o cliente sobre la resolución del incidente.
- ✓ Brindar detalles sobre las acciones tomadas y las medidas de prevención.
- ✓ Ofrecer soporte adicional si es necesario.

Documentación Asociada

- ✓ **Informe final del incidente:** Detalla el proceso de respuesta, la causa raíz, el impacto y las lecciones aprendidas.
- ✓ **Registro de actividades:** Documenta las acciones tomadas durante la respuesta al incidente.
- ✓ **Capturas de pantalla y logs:** Evidencia del problema y las acciones tomadas.
- ✓ **Comunicaciones:** Registros de las comunicaciones con usuarios, colaboradores y entidades externas.

Aprendizaje y Mejora

Análisis del incidente

- ✓ Identificar la causa raíz del problema.
- ✓ Evaluar la eficacia del plan de respuesta a incidentes.
- ✓ Identificar oportunidades de mejora.

Implementación de mejoras

- ✓ Actualizar el plan de respuesta a incidentes.
- ✓ Implementar medidas de seguridad adicionales.
- ✓ Capacitar al personal sobre las lecciones aprendidas.

Traslado de Información

- ✓ **Equipo de respuesta a incidentes:** Informar sobre el cierre del incidente y las lecciones aprendidas.
- ✓ **Alta dirección:** Informar sobre el impacto del incidente y las medidas tomadas.
- ✓ **Clientes o socios afectados:** Informar sobre la resolución del incidente y las medidas de prevención.
- ✓ **Autoridades o entidades legales:** Informar sobre el cierre del incidente si es necesario.

Webgrafía.

https://www.incibe.es/incibe-cert/guias-y-estudios/guias/guia-nacional-de-notificacion-y-gestion-de-ciberincidentes

https://www.metacompliance.com/es/blog/data-breaches/how-to-write-an-incident-response-plan

https://www.ciberseguridad.eus/empresa-segura/medidas-para-mitigar/plan-de-respuesta-incidentes-de-ciberseguridad

https://www.ibm.com/es-es/topics/incident-response