Plan de respuesta a incidentes para Company Grupo1

Autor: Grupo 1, Grupo1@grupo1.com

Revisión 001, Publicado 01 Apr 2024

Abstract

Este plan de respuesta a incidentes está basado en el plan conciso, directivo, específico, flexible y gratuito disponible Github de Counteractive Security's y discutido en www.counteractive.net

Fue revisado por última vez el 30 Mar 2024. Fue probado por última vez en 31 Mar 2024.

Contents

Plan de respuesta a incidentes para Company Grupo1

Autor: Grupo 1, Grupo1@grupo1.com

Revisión 001, Publicado 01 Apr 2024

Este plan de respuesta a incidentes está basado en el plan conciso, directivo, específico, flexible y gratuito disponible en Github de Counteractive Security y discutido en www.counteractive.net

Fue revisado por última vez el 30 Mar 2024. Fue probado por última vez en 31 Mar 2024.

Evaluar

1. **Mantenga la calma y la profesionalidad.**
2. Reúna la información pertinente, *por ejemplo*, alarmas, eventos, datos, suposiciones, intuiciones (**observar**).
3. Considerar las categorías de impacto, a continuación (**orientar**), y determinar si hay un posible incidente (**decidir**):
4. Iniciar una respuesta si hay un incidente (**actuar**). En caso de duda, inicie una respuesta. El responsable de gestión de incidentes y el equipo de respuesta pueden ajustarse tras la investigación y la revisión.

Evaluar el impacto funcional

¿Cuál es el impacto directo o probable en su trabajo? (*por ejemplo*, operaciones comerciales, empleados, clientes, usuarios)

- Degradación o fracaso del trabajo/negocio: **incidente!**
- Ninguno: evalúe el impacto de la información.

Evaluar el impacto de la información

¿Cuál es el impacto directo o probable sobre sus datos/información, en particular los sensibles? (*por ejemplo*, información personal, datos de propiedad, financieros o sanitarios)

- Información a la que se ha accedido, cogido, cambiado o borrado: **incidente!**
- Ninguno: gestión a través de canales no relacionados con incidentes (por ejemplo, un ticket de soporte).

Cada miembro del equipo está facultado para comenzar este proceso. Si ves algo, dilo.

Iniciar la respuesta

Nombrar el incidente

Cree una frase simple de dos palabras para referirse al incidente -un nombre en clave- que se utilizará para el archivo y el canal del incidente.

Reunir el equipo de respuesta

1. **No** discutir el incidente fuera del equipo de respuesta.
2. Inicie y/o únase al chat de respuesta en MS Teams.
3. Iniciar y/o unirse a la llamada de respuesta en +34 956895623 y/o ms.teams.tld/Grupo1.
4. Preferible usar la llamada de voz, el chat y el intercambio seguro de archivos sobre cualquier otro método.
5. **No** utilizar el correo electrónico principal si es posible. Si el correo electrónico es necesario, utilícelo con moderación o use Grupo1Alter@grupo1.com. Encripte los correos electrónicos cuando cualquier participante esté fuera del dominio grupo1.com.
6. **No** usar SMS/texto para comunicar el incidente.
7. Invite al personal de turno/guardia a la llamada y al chat de respuesta.
    - Invitar a las personas de dirección que esten interesadas y a los asesores jurídicos lo antes posible.
8. OPCIONAL:_ Establecer una sala de colaboración en persona (“sala de guerra”) para la solución de incidentes complejos o graves.

Referencia: Estructura del equipo de respuesta

- Equipo de Mando
  - Incident Commander
  - Incident Commander-Adjunto
  - Escriba
- Equipo de enlace
  - Enlace interno
  - Enlace externo
- Equipo de operaciones
  - Expertos en la materia (SME) para sistemas
  - SME para equipos/unidades de negocio
  - SME para Funciones Ejecutivas (*por ejemplo*, Legal, RRHH, Finanzas)

Referencia: Información de contacto del equipo de respuesta

Rol del equipo de respuesta	Información de contacto
Localizador del Incident Commander	{INCIDENT_COMMANDER_PAGER_NUMBER}}
Url del Incident Commander	grupo1.com/ic-page
Lista del Incident Commander	grupo1.com/ic-roster
Lista del equipo de seguridad	grupo1.com/sec-roster
Lista del equipo SME	grupo1.com/sme-roster
Lista de ejecutivos	grupo1.com/exec-roster

Establecer el ritmo de batalla

Realizar la primera llamada de respuesta

1. Realice la llamada inicial utilizando la estructura de llamada de respuesta inicial
2. Siga las instrucciones del Incident Commander. Si el Incident Commander de turno/de guardia no se une a la llamada **dentro de 20 minutes** y usted es un Incident Commander capacitado, tome el mando de la llamada.
3. Siga las instrucciones correspondientes a su función.
4. Siga la llamada y el chat, y comente según corresponda. Si no es un SME, comunique las aportaciones a través del SME de su equipo si es posible.
5. **Mantenga la llamada y el chat activos durante todo el incidente para una comunicación basada en eventos.**
6. Programe actualizaciones **cada 4 Horas** sobre la comunicación activa.

Referencia: Estructura de la llamada de respuesta inicial

- Incident Commander (IC): Mi nombre es [NOMBRE], soy el Incident Commander. He designado a [NOMBRE] como adjunto y a [NOMBRE] como esccriba. ¿Quién está en la llamada?
- ESCRIBA: [Toma asistencia]

- IC: [Si falta personal clave] Adjunto, por favor llame a [PERSONAL FALTANTE].
- IC: [Hace preguntas para comprender la situación, los síntomas, el alcance, el vector, el impacto y el calendario del reportador del incidente, los SME aplicables para los sistemas y las unidades de negocio].
- SMEs: [Responde brevemente a las preguntas del IC].
- IC: [Si se trata de un incidente]:
  - En este momento, el resumen del incidente es el siguiente: [reitera el resumen]. El equipo de investigación estará dirigido por [NOMBRE], el equipo de reparación estará dirigido por [NOMBRE] y el equipo de comunicación estará dirigido por [NOMBRE]. Ellos coordinarán la composición del equipo y me informarán. Los miembros del equipo, por favor, informen a su jefe de equipo correspondiente.
  - ¿Qué medidas de investigación, corrección o comunicación se han tomado ya? [esta debería ser una lista corta, pero tiene que salir ahora]
  - Esta llamada y el chat permanecerán activos y disponibles hasta el cierre del incidente, por favor, utilícelos para todas las comunicaciones relacionadas con el incidente. Proporcione actualizaciones de estado en tiempo real en el chat, si es posible. ¿Hay alguna pregunta o aportación restante? [responde a las preguntas]
  - Líderes de equipo, por favor procedan con sus acciones planeadas. Nos reuniremos de nuevo en [UPDATE_TIME] para discutir el estado. Gracias.
- IC: [Si esto no es un incidente]: En este momento, estos hechos no alcanzan el nivel de un incidente. Me coordinaré directamente con el reportador del incidente para las acciones de seguimiento. Gracias por su tiempo.

Referencia: Etiqueta de la llamada

- Únase tanto a la llamada como al chat.
- Mantenga el ruido de fondo al mínimo.
- Mantenga su micrófono silenciado hasta que tenga algo que decir.
- Identifícate cuando te unas a la llamada; di tu nombre y tu función (por ejemplo, “Soy el SME del equipo x”).
- Habla con claridad.
- Sea directo y objetivo.
- Mantenga conversaciones/discusiones cortas y al grano.
- Comunicar cualquier preocupación al Incident Commander (CI) en la llamada.
- Respetar las limitaciones de tiempo impuestas por el Incident Commander.

Realizar la actualización de la respuesta

- Llevar a cabo actualizaciones programadas utilizando la estructura de llamada de actualización cada 4 Horas.

- Ajustar la frecuencia según sea necesario.
- Coordinar las actualizaciones independientes (*por ejemplo*, ejecutivas, legales) según sea necesario, pero con la menor frecuencia posible.

Referencia: Estructura de la llamada de actualización de la respuesta

- Incident Commander (IC): Desde la última actualización programada, el resumen del incidente es el siguiente:
  - [Impacto]
  - [Vector]
  - [Actualización del resumen]
  - [Actualización de la línea de tiempo]
- IC: Equipo de investigación, por favor proporcione una breve actualización
  - LÍDER DE LA INVESTIGACIÓN: [Actividades de investigación o "nada que informar"]
  - ¿Cuál es su plan de investigación recomendado?
  - ¿Qué acciones de investigación necesitan ser asignadas o aprobadas? [escuchar, obtener consenso, encargar/aprobar]
- IC: Equipo de remediación, por favor proporcione una breve actualización
  - Líder de remediación: [Actividades de remediación o "nada que informar"]
  - ¿Cuál es su estrategia de corrección recomendada? ¿Objeciones fuertes? [escuchar, obtener el consenso, asignar/aprobar]
  - ¿Qué acciones de corrección necesitan ser asignadas o aprobadas?
- IC: Equipo de comunicación, por favor, proporcione una breve actualización:
  - COMMUNICATIONS LEAD: [Actividades de comunicación o "nada que informar"]
  - ¿Cuál es su estrategia de comunicación recomendada? ¿Objeciones fuertes? [escuchar, obtener consenso, encargar/aprobar]
  - ¿Qué acciones de comunicación necesitan ser asignadas o aprobadas?
- IC: Esta llamada y el chat permanecerán activos y disponibles hasta el cierre del incidente, por favor, utilícelos para todas las comunicaciones relacionadas con el incidente. Si es posible, proporcione actualizaciones del estado en tiempo real en el chat. ¿Hay alguna pregunta o aportación restante? [responde a las preguntas]
- IC: Líderes de equipo, por favor procedan. Nos reuniremos de nuevo en [] para discutir el estado. Gracias.

Supervisar el alcance

- Supervisar el alcance de la respuesta para asegurarse de que no excede el ámbito de control del Incident Commander.
- Si un incidente es lo suficientemente complejo y hay suficientes intervinientes, considere la posibilidad de crear subequipos.

Crear Sub-Equipos

- En la preparación de incidentes complejos, se predefinen tres subequipos: Investigación, Remediación y Comunicación, generalmente responsables de esas funciones de respuesta.
- Crear un puente de llamadas y un chat para cada subequipo.
- El Incident Commander designará a los líderes de los equipos, que dependen del IC, y a los miembros de los equipos, que dependen de su líder. *Los líderes de equipo no tienen que estar formados como Incident Commanders, pero es preferible que tengan alguna experiencia de liderazgo.*
- El Incident Commander puede ajustar el propósito o el nombre de los subequipos según sea necesario.
- Si desea cambiar de equipo, pregunte a su **líder de equipo actual**. **No** preguntar al Incident Commander, o al líder del otro(s) equipo(s). Utilice la cadena de mando.

Incidente dividido

Si un incidente resulta ser dos o más incidentes distintos:

- Establezca un nuevo archivo de incidentes.
- Haga un seguimiento y coordine la investigación, la reparación y la comunicación en el archivo correspondiente.
- Considere la posibilidad de establecer subequipos para cada incidente.
- **Mantener un Incident Commander de alto nivel**, para coordinar los activos de baja densidad y alta demanda y mantener la unidad de mando.

Preparación

Antes de empezar con las etapas previas, es necsario que el personal de la empresa reciba formación en ciberseguridad a través de por ejemplo, reuniones, cocienciación... Esto puede llevar a aprender a identificar los patrones, analizar los registros y regsitros de actividad, y cómo bloquear cuentas de usuarios, y más... A continuación, se detallan algunas prácticas que sirven para preparar a los empleados:

- Entender a cómo acceder a los regsitros del sistema y cómo utilizar el visor de eventos.
- Adquirir la habilidad para bloquear los puertos de servicios que están siendo objeto de ataques.
- Aprender a informar la detección de patrones sospechosos para que las decisioses que se tomen sean las más rápidas y efectivas antes los posibles ataques.
- Conocer el procedimiento para bloquear cuentas de usuario sospechosas.

Es muy importante que los empleados estén al tanto de los diferentes tipos de ataques que se podrían enfrentar o toparse y que comprendan las consecuencias

que puede tener en la empresa. Además, deben de tener en cuenta las señales de alerta que puede indicar que un ataque está en curso, como cambios en el rendimiento del sistema o dispostivos y/o mensajes de errores inesperados.

Los empleados también deben recibir instrucción sobre las mejores prácticas de seguridad, como la creación y el uso de contraseñas seguras, la importancia de mantener el software actualizado y la conexión solo a redes confiables. Es esencial que entiendan la importancia de proteger la información de la empresa y estén al tanto de las medidas de seguridad necesarias para hacerlo.

Se recomienda llevar a cabo simulaciones de ataques para ayudar a preparar a los empleados para que sepan cómo responder adecuadamente en caso de que ocurra de forma real.

Investigar

Investigar, Remediar y comunicar en paralelo, utilizando equipos separados, si es posible. El Incident Commander coordinará estas actividades. Notifique al Incident Commander si hay pasos que el equipo debe considerar.

Crear el archivo del incidente

1. Cree un nuevo archivo de incidentes en grupo1.com/docu/grupo1 utilizando el nombre del incidente. Utilice este archivo para el almacenamiento seguro de documentación, pruebas, artefactos, *etc.*.
    - Proporcionar un almacenamiento digital seguro.
    - Proporcionar un intercambio de archivos seguro.
    - Obtener almacenamiento físico.
    - Compartir la ubicación del archivo del incidente en la llamada y el chat.
2. Documente el impacto funcional y de la información, si se conoce (véase Evaluar).
3. Documentar el vector, si se conoce (*por ejemplo* web, correo electrónico, medios extraíbles).
4. Documente el resumen del incidente: un breve resumen del vector, el impacto, la investigación y la situación de la reparación, si se conoce.
5. Documente la línea de tiempo del incidente, incluyendo la actividad del atacante y la actividad de la respuesta.
6. Documente los pasos de investigación, reparación y comunicación. Documente las actividades de forma independiente para que puedan combinarse y reutilizarse, si es posible.
7. Registre la información significativa, como: **Pruebas**, con la hora de recogida, la fuente, la cadena de custodia, *etc.*.
    - **Sistemas afectados**, con el modo y el momento en que se identificó el sistema, y el resumen del efecto (_por ejemplo, tiene malware, datos a los que se ha accedido).

    - **Archivos de interés**, como el malware o los archivos de datos, con el sistema y los metadatos.
    - **Datos accedidos y tomados**, con nombres de archivos, metadatos y hora de presunta exposición.
    - **Actividad significativa del atacante**, como inicios de sesión y ejecución de malware, con la hora del evento.
    - **Indicadores de compromiso (IOC)** basados en la red, como direcciones IP y dominios.
    - **Indicadores de compromiso basados en el host**, como nombres de archivos, hashes y claves de registro.
- **Cuentas comprometidas**, con el alcance del acceso y la hora del compromiso.

Recoger las pistas iniciales

1. Entrevistar a los reportadores del incidente.
2. Recoger los datos de apoyo iniciales (*e.*, alarmas, eventos, datos, suposiciones, intuiciones) en el archivo del incidente.
3. Entrevistar a lo(s) SME con experiencia en el dominio o el sistema, para comprender los detalles técnicos, el contexto y el riesgo.
4. Entrevistar a lo(s) SME de la unidad de negocio afectada, para comprender el impacto de la misión/negocio, el contexto y el riesgo.
5. Asegúrese de que las pistas son relevantes, detalladas y procesables.

Referencia: Lista de recursos de respuesta

Recurso	Ubicación
Lista de información crítica	grupo1.com/cil
Lista de activos críticos	grupo1.com/assets
Base de datos de gestión de activos	grupo1.com/assets/DB
Mapa de red	grupo1.com/network+map
Consola SIEM	siem.grupo1.com
Agregador de registros	grupo1.com/logs

Actualizar el plan de investigación y el archivo del incidente

1. Revisar y perfeccionar el impacto del incidente.
2. Revisar y refinar el vector del incidente.
3. Revisar y perfeccionar el resumen del incidente.
4. Revisar y perfeccionar la línea de tiempo del incidente con hechos e inferencias.
5. Crear hipótesis: qué puede haber ocurrido y con qué seguridad.
6. **Identificar y priorizar las preguntas clave** (lagunas de información) para apoyar o desacreditar las hipótesis.

- Utilizar la matriz ATT&CK de MITRE o un marco similar para desarrollar preguntas.
  - ATT&CK for Enterprise, incluyendo enlaces a los específicos de Windows, Mac y Linux.
  - ATT&CK Mobile Profile para dispositivos móviles.
- Utilizar palabras interrogativas como inspiración:
  - **¿Cuándo?**: primer compromiso, primera pérdida de datos, acceso a x datos, acceso a y sistema, etc.
  - **¿Qué?**: impacto, vector, causa de origen, motivación, herramientas/explotaciones utilizadas, cuentas/sistemas comprometidos, datos atacados/perdidos, infraestructura, COIs, etc.?
  - **¿Dónde?**: ubicación del atacante, unidades de negocio afectadas, infraestructura, etc.?
  - **¿Cómo?**: compromiso (explotación), persistencia, acceso, exfiltración, movimiento lateral, etc.?
  - **¿Por qué?**: objetivo, momento, acceso a x datos, acceso a y sistema, etc.
  - **¿Quién?**: atacante, usuarios afectados, clientes afectados, etc.?

7. **Identificar y priorizar los dispositivos y estrategias testigo** para responder a las preguntas clave.
   - Consultar los diagramas de la red, los sistemas de gestión de activos y la experiencia de las SME
   - Consultar la Lista de recursos de respuesta)
8. Consulte los playbook de incidentes para conocer las preguntas clave, los dispositivos testigos y las estrategias para investigar las amenazas comunes o muy dañinas.

El plan de investigación es fundamental para una respuesta eficaz; impulsa todas las acciones de investigación. Utilice el pensamiento crítico, la creatividad y el buen juicio.

Referencia: Táctica del atacante a la matriz de preguntas clave

Táctica del atacante	La forma en que los atacantes ...	Posibles preguntas clave
Reconocimiento	... aprender sobre los objetivos	¿Cómo? ¿Desde cuándo? ¿Dónde? ¿Qué sistemas?
Desarrollo de recursos	... construir infraestructuras.	¿Qué sistemas?
Acceso inicial	... entrar	¿Cómo? ¿Desde cuándo? ¿Dónde? ¿Qué sistemas?
Ejecución	... ejecutar código hostil	¿Qué malware? ¿Qué herramientas? ¿Dónde? ¿Cuándo?

Táctica del atacante	La forma en que los atacantes ...	Posibles preguntas clave
Persistencia	... quedarse en el sistema	¿Cómo? ¿Desde cuándo? ¿Dónde? ¿Qué sistemas?
Escalada de Privilegios	... obtener acceso de mayor nivel	¿Cómo? ¿Dónde? ¿Qué herramientas?
Evasión de la defensa	... esquivar la seguridad	¿Cómo? ¿Dónde? ¿Desde cuándo?
Acceso a credenciales	... obtener/crear cuentas	¿Qué cuentas? ¿Desde cuándo? ¿Por qué?
Descubrimiento	... aprender nuestra red	¿Cómo? ¿Dónde? ¿Qué saben?
Movimiento lateral	... moverse	¿Cómo? ¿Cuándo? ¿Qué cuentas?
Recogida	... encontrar y reunir datos	¿Qué datos? ¿Por qué? ¿Cuándo? ¿Dónde?
Mando y control	... herramientas y sistemas de control	¿Cómo? ¿Dónde? ¿Quién? ¿Por qué?
Exfiltración	... tomar datos	¿Qué datos? ¿Cómo? ¿Cuándo? ¿Dónde?
Impacto	... romper cosas.	¿Qué sistemas o datos? ¿Cómo? ¿Cuándo? ¿Dónde? ¿Cómo de malo?

Consulte la página MITRE ATT&CK para obtener más información e ideas.

Crear y desplegar indicadores de compromiso (IOC)

Haga hincapié en los indicadores **dinámicos y de comportamiento** junto con las huellas digitales estáticas.

- Crear IOCs basados en pistas iniciales y análisis.
- Cree IOCs usando un formato abierto soportado por sus herramientas (*por ejemplo*, STIX 2.0), si es posible.
- Utilice la automatización, si es posible.
- **No** desplegar "feeds" de IOCs no relacionados y no curados, ya que pueden causar confusión y fatiga.
- Considerar todos los tipos de IOC:
  - IOC basados en la red, como direcciones IP o MAC, puertos, direcciones de correo electrónico, contenido o metadatos del correo electrónico, URLs, dominios o patrones PCAP.
  - IOC basados en el host, como rutas, hashes de archivos, contenido o metadatos de archivos, claves de registro, MUTEXes, autoejecuciones o artefactos y permisos de usuarios.

  - IOCs basados en la nube, como patrones de registro para despliegues SaaS o IaaS
  - IOCs de comportamiento (a.ka., patrones, TTPs) tales como patrones de árbol de procesos, heurística, desviación de la línea base y patrones de inicio de sesión.
- Correlacionar varios tipos de IOC, como indicadores basados en la red y en el host en los mismos sistemas.

Identificar los sistemas de interés

1. Validar si son relevantes.
2. Categorizar la(s) razón(es) por la(s) que son "de interés": tiene malware, acceso por cuenta comprometida, tiene datos sensibles, etc. Trátelas como "etiquetas", puede haber más de una categoría por sistema.
3. Prioriza la recogida, el análisis y la reparación en función de las necesidades de la investigación, el impacto en el negocio, *etc.*

Recogida de pruebas

- Priorizar en base al plan de investigación
- Recoger datos de respuesta en vivo utilizando velociraptor.
- Recoger los registros relevantes de los sistemas (si no forman parte de la respuesta en vivo), agregadores, SIEM o consolas de dispositivos.
- Recoger la imagen de la memoria, si es necesario y si no forma parte de la respuesta en vivo, utilizando winpmem.
- Recoger la imagen del disco, si es necesario, utilizando sumuri.

- Recoger y almacenar las pruebas de acuerdo con la política, y con la cadena de custodia adecuada. ‘

Considere la posibilidad de recopilar los siguientes artefactos como evidencia, ya sea en tiempo real (*por ejemplo*, a través de EDR o un SIEM) o bajo demanda:

Ejemplo de artefactos útiles

- Procesos en ejecución
- Servicios en ejecución
- Hashes ejecutables
- Aplicaciones instaladas
- Usuarios locales y de dominio
- Puertos de escucha y servicios asociados
- Configuración de resolución del sistema de nombres de dominio (DNS) y rutas estáticas
- Conexiones de red establecidas y recientes
- Clave de ejecución y otra persistencia de la ejecución automática
- Tareas programadas y trabajos cron
- Artefactos de ejecución pasada (por ejemplo, Prefetch y Shimcache)

- Registros de eventos
- Política de grupo y artefactos WMI
- Detecciones antivirus
- Binarios en ubicaciones de almacenamiento temporal
- Credenciales de acceso remoto
- Telemetría de conexiones de red (por ejemplo, netflow, permisos de cortafuegos)
- Tráfico y actividad de DNS
- Actividad de acceso remoto, incluido el Protocolo de Escritorio Remoto (RDP), la red privada virtual (VPN), SSH, la informática de red virtual (VNC) y otras herramientas de acceso remoto
- Cadenas de identificadores de recursos uniformes (URI), cadenas de agentes de usuario y acciones de aplicación del proxy
- Tráfico web (HTTP/HTTPS)

Analizar las pruebas

- Priorizar basándose en el plan de investigación
- Analizar y clasificar los datos de la respuesta en vivo
- Analizar la memoria y las imágenes de disco (es decir, realizar análisis forenses)
- Analizar el malware
- *OPCIONAL:* Enriquecer con investigación e inteligencia
- Documentar nuevos indicadores de compromiso (IOCs)
- Actualizar el archivo del caso

Ejemplo de indicadores útiles

- Comportamiento inusual de autenticación (*e.*, frecuencia, sistemas, hora del día, ubicación remota)
- Nombres de usuario con formato no estándar
- Binarios no firmados que se conectan a la red
- Balizamiento o transferencias de datos significativas
- Solicitudes de línea de comandos PowerShell con comandos codificados en Base64
- Actividad excesiva de RAR, 7zip o WinZip, especialmente con nombres de archivo sospechosos
- Conexiones en puertos no utilizados previamente.
- Patrones de tráfico relacionados con el tiempo, la frecuencia y el recuento de bytes
- Cambios en las tablas de enrutamiento, como la ponderación, las entradas estáticas, las pasarelas y las relaciones entre pares.

Iterar la investigación

Actualizar el plan de investigación y repetir hasta el cierre.

Remediar

Investigar, Remediar y Comunicar en paralelo, utilizando equipos separados, si es posible. El Incident Commander coordinará estas actividades. Notifique al Incident Commander si hay pasos que el equipo debe considerar

Actualización del plan de remediación

1. Revise el archivo del incidente en grupo1.com/docu/grupo1 utilizando el nombre del incidente
2. Revise los playbook aplicables.
3. Revise la lista de recursos de respuesta.
4. Considere qué tácticas del atacante están en juego en este incidente. Utilice la lista de MITRE ATT&CK (*i.*, Persistencia, Escalada de Privilegios, Evasión de la Defensa, Acceso a Credenciales, Descubrimiento, Movimiento Lateral, Ejecución, Recolección, Exfiltración y Mando y Control), o un marco similar.
5. Desarrollar remedios para cada táctica en juego, en la medida en que sea factible teniendo en cuenta las herramientas y los recursos existentes. Considere remedios para Proteger, Detectar, Contener, y Erradicar cada comportamiento del atacante.
6. Priorizar en base a la estrategia de tiempo, el impacto y la urgencia.
7. Documentar en el archivo de incidentes.

Utilice marcos de seguridad de la información (infosec) como inspiración, pero **no utilice la reparación de incidentes como sustituto de un programa de infosec con un marco apropiado.** Utilícelos para complementarse.

Protección

> "¿Cómo podemos evitar que la táctica X se repita o reducir el riesgo? ¿Cómo podemos mejorar la protección futura?"

Utilice lo siguiente como punto de partida para la corrección de la protección:

- Parchear las aplicaciones.
- Parchee los sistemas operativos.
- Actualice las firmas de IPS de la red y del host.
- Actualizar las firmas de protección de puntos finales/EDR/antivirus.
- Reducir las ubicaciones con datos críticos.
- Reducir las cuentas administrativas o privilegiadas.
- Habilitar la autenticación multifactor.
- Reforzar los requisitos de las contraseñas.
- Bloquear los puertos y protocolos no utilizados en los límites del segmento y de la red, tanto entrantes como salientes.
- Poner en lista blanca las conexiones de red para los servidores y servicios críticos.

Detección

> "¿Cómo podemos detectar esto en los nuevos sistemas o en el futuro? ¿Cómo podemos mejorar la detección y la investigación en el futuro?"

Utilice lo siguiente como punto de partida para la corrección de detecciones:

- Mejorar el registro y la retención de los registros del sistema, en particular de los sistemas críticos.
- Mejorar el registro de las aplicaciones, incluidas las aplicaciones SaaS.
- Mejorar la agregación de registros.
- Actualizar las firmas de IDS de la red y del host utilizando IOC.

Contención

> "¿Cómo podemos evitar que esto se extienda o se agrave? ¿Cómo podemos mejorar la contención en el futuro?"

Utilice lo siguiente como punto de partida para la corrección de la contención:

- Implementar listas de acceso (ACL) en los límites de los segmentos de la red.
- Implementar bloqueos en el límite de la empresa, en múltiples capas del modelo OSI.
- Desactivar o eliminar el acceso de las cuentas comprometidas.
- Bloquear direcciones IP o redes maliciosas.
- Bloquee los dominios maliciosos.
- Actualizar las firmas de IPS y antimalware de la red y el host mediante COI.
- Retirar de la red los sistemas críticos o comprometidos.
- Póngase en contacto con los proveedores para obtener ayuda (por ejemplo, proveedores de servicios de Internet, proveedores de SaaS).
- Poner en lista blanca las conexiones de red para los servidores y servicios críticos.
- Matar o deshabilitar procesos o servicios.
- Bloquear o eliminar el acceso de proveedores y socios externos, especialmente el acceso privilegiado.

Erradicar

> "¿Cómo podemos eliminar esto de nuestros activos? ¿Cómo podemos mejorar la erradicación en el futuro?"

Utilice lo siguiente como punto de partida para la remediación de la erradicación:

- Reconstruir o restaurar los sistemas y datos comprometidos a partir de un estado bueno conocido.
- Restablecer las contraseñas de las cuentas.
- Eliminar cuentas o credenciales hostiles.
- Borrar o eliminar malware específico (¡difícil!).

- Implementar proveedores alternativos.
- Activar y migrar a ubicaciones, servicios o servidores alternativos.

Elegir el momento de la reparación

Determine la estrategia de plazos -cuando se llevarán a cabo las acciones de remediación- involucrando al Incident Commander, a los SME y propietarios del sistema, a los SMEs y propietarios de la unidad de negocio, y al equipo ejecutivo. Cada estrategia es apropiada en diferentes circunstancias:

- Elija la reparación **inmediata** cuando sea más importante detener inmediatamente las actividades del atacante que seguir investigando. Por ejemplo, una pérdida financiera en curso, o un fracaso de la misión en curso, una pérdida de datos activa, o la prevención de una amenaza significativa inminente.
- Elija una reparación **retrasada** cuando sea importante completar la investigación o no alertar al atacante. Por ejemplo, el compromiso a largo plazo de un atacante avanzado, el espionaje corporativo o el compromiso a gran escala de un número desconocido de sistemas.
- Elija la remediación **combinada** cuando las circunstancias inmediatas y retardadas se apliquen en el mismo incidente. Por ejemplo, la segmentación inmediata de un servidor o red sensible para cumplir con los requisitos reglamentarios mientras se investiga un compromiso a largo plazo.

Ejecutar la remediación

- Evaluar y explicar los riesgos de las acciones de remediación a las partes interesadas.
- Implementar inmediatamente aquellas acciones de remediación que afecten poco o nada al atacante (a veces llamadas “acciones de postura”). Por ejemplo, muchas de las acciones de protección y detección anteriores son buenas candidatas.
- Programar y asignar acciones de remediación de acuerdo con la estrategia de tiempo.
- Ejecute las acciones de corrección en lotes, como eventos, para lograr la máxima eficacia y el mínimo riesgo.
- Documentar el estado de ejecución y el tiempo en el archivo de incidentes, especialmente para las medidas temporales.

Iterar la remediación

Actualizar el plan de remediación y repetir hasta el cierre.

Comunicar

- Investigar, Remediar y Comunicar en paralelo, utilizando equipos separados, si es posible. Notifique al Incident Commander si hay pasos que el equipo debe considerar

Toda comunicación debe incluir la información más precisa disponible. Muestre integridad. No comunicar especulaciones.

Comunicación Interna

Notificar y actualizar a las partes interesadas

- Comunicarse con las partes interesadas como parte de las llamadas iniciales y de actualización, así como a través de actualizaciones basadas en eventos en la llamada y el chat.
- Coordinar las actualizaciones independientes (*e.*, ejecutivas, legales) según sea necesario, pero con la menor frecuencia posible, para mantener el foco en la investigación y la reparación.
- Concéntrese en la mejor evaluación del vector, el impacto, el resumen y los aspectos más destacados de la línea de tiempo, incluidos los pasos de remediación. No especule.

Notificar y actualizar la organización

- **No** notifique o actualice al personal que no responde hasta que el Incident Commander lo autorice, en particular si existe el riesgo de una amenaza interna.
- Coordine las actualizaciones de los equipos o de toda la organización con los ejecutivos y la dirección de la empresa.
- Concéntrese en la mejor evaluación del vector, el impacto, el resumen y los aspectos más destacados de la línea de tiempo, incluidos los pasos de remediación. No especule.

Crear Informe de Incidentes

- Tras el cierre del incidente, capture la información en el archivo del incidente para su distribución utilizando el formato en grupo1.com/templates. **Si los informes de vector, impacto, resumen, línea de tiempo y actividad están completos, esto puede ser totalmente automatizado.**
- Distribuir el informe de incidentes a lo siguiente: grupo1.com/reports/recibidos.

Comunicar al exterior

Notificar a los reguladores

- **No** notifique ni ponga al día al personal que no ha respondido hasta que el Incident Commander lo autorice.

- Notificar a los organismos reguladores (por ejemplo, HIPAA/HITRUST, PCI DSS, SOX) si es necesario y de acuerdo con la política.
- Coordinar los requisitos, el formato y los plazos con el legal@grupo1.com.

Notificar a los clientes

- **No** notifique o actualice al personal que no responde hasta que el Incident Commander lo autorice.
- Coordine las notificaciones a los clientes con marketing@grupo1.com.
- Incluya la fecha en el título de cualquier anuncio, para evitar confusiones.
- No utilice tópicos como "nos tomamos la seguridad muy en serio". Céntrese en los hechos.
- Sea honesto, acepte la responsabilidad y presente los hechos, junto con el plan para prevenir incidentes similares en el futuro.
- Sea lo más detallado posible con la línea de tiempo.
- Sea lo más detallado posible en cuanto a la información que se vio comprometida y cómo afecta a los clientes. Si estábamos almacenando algo que no debíamos, sé honesto al respecto. Saldrá a la luz más tarde y será mucho peor.
- No hablemos de las partes externas que podrían haber causado el problema, a menos que ya lo hayan hecho público, en cuyo caso enlazaremos con su información. Comunícate con ellos de forma independiente (ver Notificar a los proveedores)
- Publique la comunicación externa lo antes posible. Las malas noticias no mejoran con el tiempo.
- Si es posible, contacte con los equipos de seguridad internos de los clientes antes de notificar al público.

Notificar a los proveedores y socios

- **No** notifique o actualice al personal que no responde hasta que el Incident Commander lo autorice.
- Si es posible, póngase en contacto con los equipos de seguridad internos de los proveedores y socios antes de notificar al público.
- Céntrese en los aspectos específicos del incidente que afectan o implican al proveedor o socio.
- Coordine los esfuerzos de respuesta y comparta la información si es posible.

Notificar a las Fuerzas de Seguridad

- **No** notifique o actualice al personal que no responde hasta que el Incident Commander lo autorice.
- Coordinar con boss@grupo1.com y legal@grupo1.com antes de interactuar con las fuerzas del orden.
- Póngase en contacto con las fuerzas del orden locales en https://www.policianacional.es/contacto.
- Póngase en contacto con el FBI en https://www.fbi.gov/contact-us o a través del Internet Crime Complaint Center (IC3).

- Póngase en contacto con los operadores de los sistemas utilizados en el ataque, sus sistemas también pueden haber sido comprometidos.

Contactar con el servicio de asistencia de respuesta externa

- Póngase en contacto con Counteractive Security para que le ayude a evaluar el riesgo, la gestión de incidentes, la respuesta a los mismos y el apoyo posterior al incidente.
- Póngase en contacto con rrpp.grupo1.com para que le ayude con las relaciones públicas y la comunicación externa.
- Póngase en contacto con ciberalberti.com para obtener ayuda con el seguro cibernético.

Compartir Inteligencia

- Comparta los IOCs con Infragard si procede.
- Comparta los IOCs con su ISAC de servicio a través de https://en.wikipedia.org/wiki/Information_Sharing_ si procede.

Recuperación

La recuperación suele estar dirigida por las unidades de negocio y los propietarios de los sistemas. Tome medidas de recuperación sólo en colaboración con las partes interesadas pertinentes.

1. Poner en marcha un plan de continuidad de negocio/recuperación de desastres: Por ejemplo, considerar la migración a ubicaciones operativas alternativas, sitios de conmutación por error, sistemas de copia de seguridad.
2. Integrar las acciones de seguridad con los esfuerzos de recuperación de la organización. # Playbook

Los siguientes playbooks capturan los pasos comunes de investigación, remediación y comunicación para determinados tipos de incidentes.

Playbook Ataque DDoS

Comenzaremos con saber lo que es un ataque DDoS: es un tipo de ciberataque en el que múltiples sistemas comprometidos, a menudo distribuidos en diferentes ubicaciones geográficas, se utilizan para inundar un objetivo específico, como un servidor o una red, con un gran volumen de tráfico de datos. El objetivo de este ataque es abrumar los recursos del sistema objetivo, como el ancho de banda de red, la capacidad de procesamiento o la memoria, de manera que el servicio se vuelva inaccesible para los usuarios legítimos.

Los motivos detrás de los ataques DDoS pueden variar, desde el sabotaje, la extorsión o la competencia desleal hasta el activismo político o social.

Pasos de Respuesta ante Incidentes

Si tu organización es víctima de un ataque de DoS o DDoS, los siguientes pasos pueden ayudar en la contención, remedio y recuperación del sistema:

Paso 1: Identificar el Ataque

• Verificar que el tráfico sospechoso sea realmente un ataque de DDoS revisando los registros del sistema y los datos de tráfico de red.
o Asegurarse de que la pérdida de servicio no se deba a otros factores como un fallo interno del servidor o una interrupción del proveedor de servicios de Internet/Cloud.
o Verificar si la organización está esperando un gran volumen de tráfico (es decir, lanzamiento de un nuevo servicio o producto, promociones por tiempo limitado, etc.)
• Identificar los activos críticos como servidores y bases de datos que están siendo atacados:
o Obtener las direcciones IP de los sistemas siendo atacados.
o Obtener el diagrama de red para los sistemas atacados.
o Identificar los servicios que el sistema proporciona (es decir, Servidor Web, DNS, Servidor de Correo, etc.)
• Identificar el tipo de ataque de DDoS (Volumétrico, Amplificación, Syn Flood, Protocolo, etc.)
o Obtener más detalles sobre los paquetes maliciosos (capa OSI, Número de Puerto de Destino, Protocolo de Comunicación, etc.)

Paso 2: Contener el Ataque

• Identificar si el ataque de DDoS explota un servicio particular (es decir, ICMP) o está atacando un puerto específico.
* Deshabilitar ese servicio o cerrar el puerto si no son esenciales para la operación del sistema atacado. * Obtener las direcciones IP de los paquetes entrantes de DDoS e implementar control de acceso para bloquear esas direcciones IP.
* Implementar limitación de velocidad para restringir el número de paquetes que pueden ser enviados desde una sola dirección IP.
* Verificar si los proveedores de servicios de Internet o Cloud pueden proporcionar a la organización algún tipo de defensa contra DDoS:
o Limpieza de tráfico / Canal Limpio
o Sinkholing (Bloqueo de direcciones IP maliciosas conocidas)
o Enrutamiento nulo (Implementar como último recurso)
• Desviar el tráfico y cambiar las operaciones a servidores alternativos, si los hay.

Paso 3: Adquirir Evidencia Forense para el Análisis de la Causa

La recopilación de evidencia forense proporcionará información sobre la naturaleza del ataque, incluido el tipo de ataque DDoS, la fuente del tráfico de ataque, el impacto del ataque y los tipos de sistemas atacados. Analizar los datos para determinar la causa raíz del ataque e identificar cualquier vulnerabilidad que pueda haber sido explotada.

Los tipos de evidencia forense a recopilar incluyen:
• Registros de tráfico de red de firewalls, routers, conmutadores y otros dispositivos de red para identificar la fuente y el tipo de tráfico involucrado en el ataque.
• Registros del sistema de servidores y otros sistemas para identificar cualquier actividad inusual o problemas de rendimiento.
• Datos de flujo de red para analizar el volumen y la dirección del tráfico, e identificar cualquier patrón o anomalía.
• Capturas de paquetes para analizar el contenido del tráfico de red e identificar cualquier carga maliciosa o exploits.

Paso 4: Reforzar tus Sistemas

El endurecimiento del sistema puede ayudar a proteger sitios web y redes contra ataques DDoS y es crucial para garantizar que el sitio web permanezca disponible y accesible para usuarios legítimos. Aquí hay algunos pasos para endurecer los recursos web:
• Usar firewalls de aplicaciones web (WAFs) para filtrar el tráfico de direcciones IP o rangos maliciosos conocidos.
• Implementar limitación de velocidad para restringir la cantidad de tráfico que puede ser enviado al sitio web desde una única fuente o dirección IP.
• Desplegar balanceadores de carga para distribuir el tráfico entrante entre múltiples servidores, evitando que un único servidor sea sobrecargado por un ataque DDoS.
• Mantener los dispositivos de red actualizados con el firmware más reciente y los parches de seguridad para abordar las vulnerabilidades conocidas.
• Revisar y actualizar las configuraciones de firewall y seguridad de red para limitar el acceso a sistemas y proteger contra tráfico no autorizado.
• Realizar segmentación de red para separar los activos críticos de los servidores de cara al público.
• Suscribirse a un servicio de protección contra DDoS ya sea de proveedores de servicios de Internet o Cloud.

Paso 5: Notificar a los Interesados e Informar sobre el Incidente

• Notificar a los clientes, proveedores y empleados sobre posibles caídas del sistema o dispositivos de red comprometidos.

• Se recomienda encarecidamente informar el caso a SingCERT a través de su Formulario de Reporte de Incidentes, ya que la información podría ayudar a alertar y asistir a otras personas y organizaciones.
• Si hay pérdida(s) monetaria(s) o actividad criminal involucrada, puedes presentar un informe policial. # Explotación de Aplicaciones de Cara al Público (T1190): ## Fase de Identificación ### Monitoreo de la aplicación: • Configura y utiliza herramientas de monitoreo de aplicaciones para detectar comportamientos anómalos. • Establece alertas para notificaciones inmediatas cuando se detecten comportamientos sospechosos. ### Análisis de logs: • Revisa regularmente los logs de la aplicación y del servidor. • Busca patrones o actividades sospechosas como múltiples intentos de inicio de sesión fallidos, solicitudes de URL desconocidas, etc. ### Clasificación del incidente: • Determina el tipo de explotación basándote en los datos recogidos. • Clasifica el incidente en consecuencia para ayudar a informar las acciones de respuesta. ### Determinación del alcance: • Identifica las aplicaciones afectadas y los datos comprometidos. • Determina cuántos usuarios o sistemas se ven afectados. ### Evaluación del impacto: • Evalúa el impacto funcional en la empresa o objetivo empresarial. • Considera el impacto en la confidencialidad, integridad y disponibilidad de los datos. ### Identificación del vector de ataque: • Comprueba las tácticas en la Initial Access tactic de MITRE ATT&CK. • Identifica cómo el atacante ganó acceso a la aplicación o sistema. ## Fase de Mitigación ### Análisis de vulnerabilidades: • Identifica y analiza las vulnerabilidades que fueron explotadas. • Utiliza herramientas de análisis de vulnerabilidades para ayudar en este proceso. ### Parcheo de vulnerabilidades: • Aplica parches o actualizaciones para corregir las vulnerabilidades identificadas. • Si no hay parches disponibles, considera otras mitigaciones como firewalls, listas de control de acceso, etc. ### Fortalecimiento de la seguridad: • Implementa medidas adicionales de seguridad para proteger la aplicación contra futuras explotaciones. • Esto puede incluir la implementación de autenticación de dos factores, la mejora de las políticas de contraseñas, la capacitación de los usuarios en seguridad, etc. ## Fase de Contención ### Aislamiento de la aplicación: • Aísla la aplicación afectada para evitar que la explotación se propague a otras partes del sistema. • Esto puede implicar la desconexión de la aplicación de la red o la colocación de la aplicación en una red separada. ### Bloqueo de tráfico malicioso: • Utiliza firewalls o sistemas de detección y prevención de intrusiones para bloquear el tráfico malicioso. • Configura las reglas para bloquear el tráfico de las direcciones IP o los dominios asociados con el ataque. ## Fase de Erradicación ### Eliminación de componentes maliciosos: • Elimina cualquier componente malicioso introducido en el sistema a través de la explotación. • Esto puede implicar la eliminación de malware, la desactivación de cuentas de usuario comprometidas, etc. ### Restauración de la aplicación: • Restaura la aplicación a un estado seguro utilizando copias de seguridad limpias. • Asegúrate de que las copias de seguridad no estén comprometidas antes de restaurarlas. ## Fase de Recuperación ### Pruebas de la aplicación: • Realiza pruebas exhaustivas para asegurarte de que la aplicación funciona correctamente y de que la amenaza ha sido eliminada. •

Esto puede implicar pruebas de funcionalidad, pruebas de rendimiento, pruebas de seguridad, etc. ### Restauración de la operación normal: • Una vez que estés seguro de que la amenaza ha sido eliminada, restaura la operación normal de la aplicación. • Monitoriza de cerca la aplicación para detectar cualquier signo de actividad maliciosa recurrente. ## Fase Post-Incidente ### Análisis post-mortem: • Realiza un análisis post-mortem para identificar las lecciones aprendidas y mejorar los futuros playbooks de respuesta a incidentes. • Esto puede implicar la revisión de los procedimientos de respuesta, la identificación de áreas de mejora, la actualización de la formación en seguridad, etc. ### Actualización de políticas y procedimientos: • Actualiza las políticas y procedimientos de seguridad en función de las lecciones aprendidas. • Esto puede implicar la actualización de los playbooks de respuesta a incidentes, la mejora de las políticas de seguridad, la implementación de nuevas medidas de seguridad, etc. ## Recursos • Herramientas de monitoreo de aplicaciones: Estas herramientas pueden ayudarte a detectar comportamientos anómalos en tus aplicaciones. • Herramientas de análisis de logs: Estas herramientas pueden ayudarte a analizar los logs de tus aplicaciones y servidores para identificar posibles signos de explotación. • Herramientas de seguridad: Estas herramientas (como firewalls, sistemas de detección y prevención de intrusiones, software antivirus y antimalware) pueden ayudarte a proteger tus aplicaciones contra explotaciones. # Playbook Manipulación de Datos

La manipulación de datos esta ahora mismo, a la orden del día, debido a que su objetivo como tal es el de modificar y/o debilitar la confianza en la autenticidad de la información. Incluso gracias a estas manipulaciones, proporcionan oportunidades para llevar a cabo ataques destructivos.

La información errónea, la desinformación y la información maliciosa constituyen lo que CISA define como "actividades de información". Los actores maliciosos utilizan MDM (Master Data Management) para generar caos, confusión y división. Estos agentes criminales buscan interferir y debilitar nuestras instituciones democráticas y la unión nacional.

Tras esto explicado, este playbook se usará con el objetivo de hacer un conjunto de pasos detallados para guiar la respuesta a incidentes relacionados con la manipulación no autorizada o maliciosa de datos.

Paso 1: Identificar el Ataque

- Identificar cualquier señal de manipulación de datos. La detección temprana del impacto es muy importante, por lo que se recomienda la configuración de sistemas de monitoreo y detección de intrusiones, así como la capacitación del personal para reconocer signos de actividad sospechosa.
- Confirmar la autenticidad de la manipulación de datos y determinar su alcance preliminar. Es importante validar la naturaleza del incidentes y asegurarse de que no sea un falso positivo antes de tomar medidas adicionales.

Paso 2: Contención y Mitigación

- Contención Inicial: Aislar las áreas afectadas y tomar medidas para evitar una mayor propagación de la manipulación de datos. Si se contiene rápidamente, podría ayudar en la limitación del impacto del incidente y evitar que se propague a otros sistemas o áreas de la red.
- Preservación de Evidencia: Documentar y preservar evidencia relacionada con la manipulación de datos para su análisis forense posterior. La persevación adecuada de la evidencia es crucial para las investigaciones posteriores y posibles acciones legales.
- Recolección de Información: Recopilar información sobre el incidente, incluidos los tipos de dafectados, los posibles vectores de ataques y los sistemas comprometidos. La recopilación de información ayuda a comprender mejor la naturaleza y el alcance del incidente, lo que facilita la respuesta y la recuperación.

Paso 3: Investigación y Análisis

- Análisis Forense: Realizar un análisis forense exhautivo de los sistemas afectados para identificar la causa raíz del incidente y determinar cómo se manipularon los datos. El análisis forense proporciona información crítica para comprender cómo ocurrió el incidente y qué medidas tomar para evitar futuras manipulaciones de datos.
- Identificación de Responsables: Determinar quién o qué está detrás de la manipulación de datos, ya sea un error humano, un acceso no autorizado o un ataque malicioso. Identificar a los responsables ayudaría a tomar las medidas adecuadas y a prevenir incidentes en el futuro.

Paso 4: Recuperación y Restauración

- Restauración de Datos: Restaurar los datos afectados desde copias de seguridad verificadas y limpias. La restauración de datos es crucial para restaurar la integridad y la disponiblidad de la información afectada por la manipulación.
- Revisión de Procedimientos: Revisar y actualizar políticas, procedimientos y controles de seguridad para prevenir futuras manipulaciones de datos. La revisión de procedimientos ayuda a identificar lagunas en la seguridad y a implementar medidas preventivas efectivas.

Paso 5: Comunicación y Notificación

- Comunicación Interna y Externa: Notificar a las partes interesadas internas y externas sobre el incidente y sus implicaciones, incluyendo la alta dirección, los empleados y, si es necesario, las autoridades reguladoras y los clientes afectados. La comunicación transparente ayuda a mantener la confianza de los stakeholders y a mitigar el impacto reputacional del incidente.

Paso 6: Lecciones Aprendidas y Mejoras Continuas

- Revisión Post-Incidente: Realizar una revisión detallada del incidente para identificar lecciones aprendidas y áreas a mejorar en los procesos de seguridad. Estas revisiones son fundamentales para fortalecer la postura de seguridad de la organización y prepararse mejor para futuros incidentes.
- Capacitación y concienciación: Proporcionar capacitación y concienciación adicional al personal sobre la importancia de la seguridad de los datos y las mejores prácticas para prevenir la manipulación no autorizada de datos. La educación continua del personal es esencial para manetner una cultura de seguridad sólida y prepararlos para identificar y responder adecuadamente a incidentes de seguridad. # Playbook Disk wipe ## ¿Qué es un ataque disk wipe? Un disk wipe es un tipo de ciberataque en el cual los datos almacenados en los discos duros u otros dispositivos de almacenamiento de una computadora son eliminados de manera deliberada y generalmente irreversible. ## Pasos de respuesta frente al incidente Si tu organización ha sufrido un ataque por disk wipe, sigue los siguientes pasos para enfrentarlo: ### Paso 1: Confirmar el Incidente
- Verificar la autenticidad del incidente de borrado de disco mediante la revisión de registros de sistema, alertas de seguridad y reportes de usuarios afectados.

- Descartar otras posibles causas de pérdida de datos, como errores de hardware o fallos de software.
  ### Paso 2: Evaluar el Alcance
- Determinar el alcance del borrado de disco, identificando los sistemas y dispositivos afectados.
- Investigar la extensión del daño, incluyendo la cantidad de datos perdidos y la criticidad de la información afectada.

Paso 3: Aislar los Sistemas Afectados

- Desconectar los sistemas afectados de la red para evitar una mayor propagación del incidente.

- Preservar la evidencia forense desconectando los dispositivos de almacenamiento y evitando cualquier actividad que pueda sobrescribir los datos restantes.

Paso 4: Recopilar Evidencia Forense

- Capturar imágenes forenses de los discos afectados y otros medios de almacenamiento pertinentes para su análisis.

- Recolectar registros de eventos, registros de sistema y cualquier otra información relevante para determinar la causa y el alcance del borrado de disco.

Paso 5: Analizar la Causa Raíz

- Realizar un análisis forense exhaustivo para identificar la causa raíz del borrado de disco, incluyendo posibles actividades maliciosas o errores humanos.

- Investigar cualquier indicio de acceso no autorizado, malware o actividades sospechosas en los sistemas afectados.

Paso 6: Restaurar Datos desde Copias de Seguridad

- Identificar y restaurar los datos afectados desde las copias de seguridad más recientes disponibles.
- Verificar la integridad de los datos restaurados para asegurar que se recuperen de manera precisa y completa.

Paso 7: Mitigar Riesgos Futuros

- Implementar medidas de seguridad adicionales para prevenir futuros incidentes de borrado de disco, como controles de acceso más estrictos, monitoreo continuo y auditorías de seguridad regulares.
- Realizar revisiones de políticas de seguridad y procedimientos de respaldo para mejorar la resiliencia y la capacidad de recuperación ante posibles amenazas.

Paso 8: Notificar a las Partes Interesadas

- Informar a las partes interesadas relevantes, incluyendo a la alta dirección, equipos de TI y usuarios afectados, sobre el incidente de borrado de disco y las medidas tomadas para mitigar sus efectos.

- Proporcionar orientación y apoyo a los usuarios afectados para ayudarlos a recuperar cualquier dato crítico perdido durante el incidente. ### Paso 9: Seguir las Políticas y Regulaciones Aplicables

- Cumplir con las políticas internas de la organización y las regulaciones externas, como la notificación obligatoria de brechas de datos según lo requieran las leyes de privacidad y protección de datos aplicables. ### Paso 10: Documentar y Aprender

- Documentar detalladamente el incidente de borrado de disco, incluyendo hallazgos forenses, acciones tomadas y lecciones aprendidas.

- Realizar una revisión post-incidente para identificar áreas de mejora en la preparación y respuesta ante incidentes de seguridad de la información.

Playbook: Compromiso de identidad y acceso

Relación con el MITRE

Matriz de MITRE

Uno de los peligros que se ha podido detectar, es la vulnerabilidad de la identidad y acceso de los usuarios de la empresa, específicamente las credenciales de acceso para poder alcanzar información privilegiada entre otro tipo de actividades nocivas.

La vulnerabilidad de credenciales puede llevar a multitud de problemas, obteniendo acceso a niveles críticos de la empresa, a información privilegiada, e incluso si los permisos lo permiten, instalar malware dentro de los ordenadores a los que tenga acceso de manera remota.

La manera en la que se puede llegar a acceder a estas cuentas, lo más habitual es el phishing, siendo ejecutado por el mismo usuario a través de un correo malicioso o link malicioso cuando navegan por las redes, pudiendo hacer que se instale en el ordenador o máquina, además de poder intentar hacer que otros usuarios puedan ser afectados por ese mismo.

¡Investiga, remedia (contención, erradicación), y comunicación en paralelo!

Investigación

1. Lo primero es revisar las credenciales del usuario que se cree que ha sido vulnerado, para comprobar hasta que punto puede acceder en el sistema.
2. Revisar si no ha sido una falsa alarma, contactando con la persona dueña de las credenciales.
3. Una vez descubierto que las credenciales han sido comprometidas, preguntar al usuario sobre puntos posibles que haya podido comprometerse la seguridad, desde si ha abierto correos extraños, a si ha descargado nuevo software. También se debe revisar el puesto de trabajo por si hay anomalías.
4. Una vez descubierto el método que se usó para comprometer las credenciales, revisar si hay posibilidad de otras víctimas.
5. Revisar si los afectados tenían información sensible en sus cuentas asociadas o en el equipo, y usar los logs para determinar su último acceso.

Remedio

Contención

- Despojar al usuario comprometido de todo permiso y desactivarlo.
- Pasar a resetear todas las contraseñas asociadas al usuario.
- Activar el multi-factor donde sea posible.
- Desactivar login remoto del usuario.

- Revocar todo token de autenticación de los usuarios afectados.
- Si una organización externa ha sido detectada en la investigación, avisar a dicha organización del compromiso de seguridad.
- Siguiendo el paso anterior, bloquear el dominio para evitar recibir más notificaciones o emails de dicha organización.
- Si se ha detectado malware, se debe preservar una muestra de ese malware y analizarla.
- Aislar todos los sistemas infectados, sin apagar a menos que sea absolutamente necesario. Preservar los sistemas para investigaciones forenses posteriores.
- Bloquear todos los Indicadores de Compromiso asociado al sistema de email, firewall y otros sistemas de seguridad.

Erradicación

- Preservar artefactos, sistemas y copias de seguridad relevantes acordado a la sensibilidad y escala del incidente, dado que puede ser importante para análisis forenses futuros.
- Preservar cualquier dato volatil que pueda ser recogido durante las fases anteriores.
- Una vez preservado todo lo anterior, reemplaza o reconstruye los sistemas.

Recuperación

- Restaurar los sistemas afectados con una copia de seguridad limpia, de antes de la infección si es posible.
- Para aquellos que no puedan ser restaurados con una copia de seguridad, reconstruye las máquinas con una imagen limpia o desde el inicio.
- Remediar toda vulnerabilidad y debilidades identificadas en la investigación.
- Resetear contraseñas de todas las cuentas afectadas o crear cuentas de reemplazo y dejar las cuentas afectadas desactivadas de manera permanente.
- Continuar la monitorización de actividad maliciosa a este incidente por un periodo de tiempo prolongado.

Referencias: Recursos de recuperación

Comunicación

Adicionalmente a todo lo anterior, se debe tener esto en cuenta:

1. Mantener una comunicación constante entre los equipos.
2. Mantener actualizados a los usuarios afectados de la evolución de la investigación.
3. Al final de la investigación, hacer una reunión para resumir todo lo acontecido y cómo mejorar la seguridad.

Recursos

1. “Plantilla”
2. “Informacion sobre Credenciales Comprometidas en un Playbook”

Información Adicional

Playbook: Phishing

Antes, de explicar, como tomaremos medidas sobre el Phishing, explicaremos, lo que es:

Phishing: Estafa cibernética en la cual el atacante intenta conseguir toda información secreta o confidencial de los usuarios por medio de suplantación de identidad.

El phishing es una forma de fraude, que se va haciendo más frecuente y a la larga, puede tener consecuencias graves, como, por ejemplo, robo de identidad, pérdida financiera, entre otros...

Paso 1: Identificación

1. Identificar a que persona o personas han sufrido el phishing.
2. Comprobar las direcciones de correo y el de correo para verficar la procedencia.
3. Notificar a la empresa sobre cualquier correo, formulario o llamada sospechosa, para realizar una acción rápida.
4. Recopaliar toda la información sobre el incidente, como se ha producido el ataque, como las consecuencias que ha tenido el ataque.
5. Notificar tanto al equipo de seguridad como a los usuarios afectados, para realizar los remedios necesarios para que no se vuelva a repetir este tipo de ataque.

Paso 2: Fase de Contención

Evaluación de la situación

- Obtener toda la información posible del ataque, guardando los datos del coreeo malicioso y/o telefono malicioso.
- Tomar evidencias, como capturas de pantalla del correo o de cualquier enlace malicioso.
- Analizar el contenido del mensaje, por si hay algún riesgo adicional, como un archivo adjunto no autorizado....
- Realizar un análisis forense de los mensajes y métodos usados de los atacantes.
- Examinar los registros de correo electrónico, servidores web y/o cualquier otro registro o archivo relevante.
- Determinar el alcance del incidente.

- Documentar y reunir todas las pruebas disponibles.
- Realizar copias de seguridad de la evidencia recopilada para un futuro análisis y referencia.

Contención

- No descargar ni ejecuar ningún archivo adjunto.
- Tratar de contactar con el que envió el mensaje con un medio alternativo conocido, empleando datos de contacto confiables

Paso 3: Fase de Mitigación

- Una vez recopilada y analizada la información obtenida, deben de tomarse las medidas para gestionar el incidente.
- Alertar a la organización sobre la existencia de una posible campaña de un phishing predemitado, para avisar a todos los trabajadores y usar las pautas a seguir ante este ataque.
- Identificar y bloquear los sitios web, direcciones IPs y/o direcciones de correo utilizados en el Phishing, para evitar la propagación.
- Interactuar con los proveedores de servicios de correo y sitios web sobre el incidente y solicitar las medidas correspondientes.
- En función del medio el cual se ha sufrido el ataque:
  - Bloquear las llamadas provenientes del número sospechoso, el cúal se hizó el Phishing.
  - Filtrar la dirección de correo o IP de origen del servidor de donde provienen los emails sospechosos.
  - En caso de que un usuario de la organización haya ejecutado o abierto un archivo adjunto, aislar el dispositivo y notificar al equipo para que se realice labores de investigación y desinfección.

Paso 4: Fase de Recuperación

- Si se dispone de un equipo legal, coordinarse con el para tener en cuenta sobre las posibles conseguencias legales y de la reputación de la empresa.
- Determinar las posibles consecuencias económicas.
- Realizar una revisión exhaustiva de las medidas de seguridad existentes.

Paso 5: Fase Post-Incidente

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando el motivo de porque ha pasado, como se ha desarrollado el control de la gestión sobre el ciber incidente y todos los problemas asociados a la misma. Se trata de este paso, aprender de lo sucedido, para que no vuelva a pasar.

Paso 6: Lecciones aprendidas

- Realizar una revisión post-incidente para identificar las lecciones aprendidas y las áreas de mejora en las políticas.
- Porporcionar charlas de concienciación sobre la seguridad a los empleados para aumentar la conciencia sobre los riegsos asociados, además de brindar pautas para identificar y evitar dichos mensajes.

Información adicional

1. 10 consejos práctivos para prevenir el phishing
2. Cómo reconocer y evitar las estafas de phishing

Playbook: Ransomware

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

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

Fase de Identificación

En la fase de identificación y detección se ha de clasificar el incidente para determinar una serie de puntos sobre el ransomware:

- Determinar el tipo de ransomware
- **Determinar el alcance:** Sistemas infectados, datos afectados.
- **Evaluar el impacto:** Evaluar el impacto funcional en la empresa o objetivo empresarial, sobre la confidencialidad, integridad y disponibilidad de los mismos.
- **Encontrar el vector de ataque:** Comprobar las tácticas en la Initial Access tactic de MITRE ATT&CK

Esta identificación puede ser pasiva o activa, si está ocurriendo en el momento (activa) o si estamos observando ciertos comportamientos extraños (pasiva). En cualquiera de los dos casos, identificar los activos afectados es crucial para el problema.

Durante esta fase es fundamental la comunicación del equipo con las personas involucradas, recopilando y documentando con la mayor claridad posible la información aportada, para así determinar con mayor precisión los activos involucrados.

Métodos de ataque más comunes según MITRE ATT&CK:

- Archivos adjuntos de correo electrónico.
- Enlaces maliciosos incrustados en el correo electrónico.

- Vulnerabilidades del navegador web.
- Propagación a través de malware.
- Dispositivos USB portátiles infectados con malware.
- Protocolo RDP poco seguro.

El equipo de respuesta a incidentes deberán implementar métodos consistentes de evaluación y priorizar eventos de ransomware para determinar las escaladas requeridas.

Fase de Mitigación

Actividades encaminadas a erradicar y limpiar o desinfectar las computadoras afectadas. Implementar medidas para evitar la reinfección. Eliminar determinados componentes, tales como malware, cuentas comprometidas, identificar y mitigar todas las vulnerabilidades que fueron explotadas. Este proceso de erradicación del evento en la red, mediante herramientas tecnológicas o manualmente dependiendo del impacto y complejidad de la situación.

Es fundamental erradicar la causa raíz que provocó la brecha de seguridad para que a futuro no vuelva ser explotada. Hasta que esta fase esté completa en su totalidad no se puede volver los sistemas a su normalidad por el riesgo que representa.

Fase de Contención

En situaciones de Ransomware, la contención es fundamental. 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 impiden la propagación desde los sistemas infectados y evitan la propagación hacia los demás sistemas y datos críticos.

Si no ha sido posible ninguna acción de mitigación inicial:

- Tomar una imagen forense del sistema y una captura de memoria de una muestra de dispositivos afectados (por ejemplo, estaciones de trabajo, servidores, servidores virtuales y servidores en la nube). Recopilar cualquier registro relevante, así como muestras de cualquier binario de malware "precursor" y observables asociados o indicadores de compromiso.
- Conservar la evidencia que es de naturaleza altamente volátil, o limitada en retención, para evitar la pérdida o la manipulación.
- Consulte en la comunidad de ciberseguridad incluso si las acciones de mitigación son posibles, con respecto a los posibles descifradores disponibles, ya que los investigadores de seguridad pueden haber descubierto fallas de cifrado para algunas variantes de ransomware y liberado descifrado u otros tipos de herramientas.

Para continuar con los pasos para contener y mitigar el incidente:

- Orientarse bajo una guía confiable para la variante de ransomware en particular y seguir los pasos recomendados para identificar y contener los sistemas o redes afectados.
- Deshabilitar la ejecución de binarios de ransomware conocidos, esto minimizará el daño y el impacto en los sistemas.
- Identificar los sistemas y las cuentas involucradas, Esto puede incluir cuentas de correos electrónicos.
- 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
- Contener los sistemas asociados que puedan usarse para acceso no autorizado adicional o continuo, para evitar filtración de credenciales.

Fase de erradicación

- Revisar las propiedades de archivos cifrados o notas de rescate para identificar usuarios específicos.
- Revisar los registros de eventos RDP, para comprobar las conexiones de red se han realizado correctamente.
- Revisar el registro de seguridad de Windows, los eventos SMB y los registros relacionados que puedan identificar eventos de autenticación o acceso.
- Ejecutar un software de captura de paquetes como Wireshark en el servidor afectado para identificar direcciones IPs involucradas en la escritura activo o cambio de nombre de los archivos.
- Realizar análisis extensos para identificar mecanismos de persistencia de afuera hacia adentro y viceversa.

Fase de Recuperación

No se recomienda pagar el rescate, nada garantiza que los ciberdelincuentes vayan a acceder y proporcionarnos la llave para desencriptar los archivos/sistemas infectados. Además, pagar demuestra que el ransomware funciona y podría aumentar el número de ataques que sufriríamos nosotros y otras organizaciones.

- Volver a conectar los sistemas y restaurar los datos de copias de seguridad cifradas sin conexión en función de una priorización de los servicios críticos.
- Tener cuidado de no volver a infectar los sistemas limpios durante la recuperación. Por ejemplo, si se ha creado una nueva red VLAN con fines de recuperación, asegurarse de que solo se agreguen sistemas limpios.
- Documentar las lecciones aprendidas del incidente y las actividades de respuesta asociadas para informar las actualizaciones y refinar las políticas, planes y procedimientos de la organización y guiar los ejercicios futuros de los mismos.

Fase Post-Incidente

- Reunión informativa: Analizar lo que ha salido bien, los desafíos enfrentados y las mejoras potenciales.
- Documentación: Realizar un informe detallado del incidente, incluidos los cronogramas, sistemas afectados, acciones de respuesta y hallazgos para la referencia futura.
- Actualización del plan: Según lo aprendido, actualiza el plan de respuesta incidentes, protocolos y herramientas.

Recursos

Acciones de los usuarios ante un incidente de ransomware:

- Mantenga la calma y respire profundamente.

1. Desconecte su sistema de la red.
2. 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.*.
3. Toma notas sobre el problema o los problemas utilizando la aplicación de notas de voz de tu smartphone o con papel y lápiz. Todo ayuda. Documenta lo siguiente:
    1. ¿Qué has notado?
    2. ¿Por qué pensaste que era un problema?
    3. ¿Qué estabas haciendo en el momento en que lo detectaste?
    4. ¿Cuándo se produjo por primera vez, y con qué frecuencia desde entonces?
    5. ¿Dónde estaba cuando ocurrió y en qué red? (oficina/casa/tienda, con cable/inalámbrica, con/sin VPN, *etc.*)
    6. ¿Qué sistemas está utilizando? (sistema operativo, nombre de host, *etc.*)¿Qué cuenta utilizas?
    7. ¿A qué datos suele acceder?
    8. ¿Con quién más se ha puesto en contacto en relación con este incidente y qué le ha dicho?
4. Contacta al servicio de asistencia técnica y ser lo más útil posible
5. Tenga paciencia: la respuesta puede ser perturbadora, pero está protegiendo a su equipo y a la organización. **Gracias.**

Acciones del servicio de asistencia técnica ante un incidente de ransomware:

1. Mantenga la calma y respire profundamente.
2. Abra un ticket para documentar el incidente, según el procedimiento.
3. Pida al usuario que tome fotos de su pantalla usando su smartphone mostrando las cosas que ha notado: mensajes de rescate, archivos encriptados, mensajes de error del sistema, *etc.* Si es algo que ha notado directamente, haga lo mismo usted.

4. Toma notas sobre el problema o los problemas utilizando la aplicación de notas de voz de tu smartphone o con papel y lápiz. 2. Si se trata de un informe de usuario, haz preguntas detalladas, incluyendo:
    1. ¿Qué ha notado?
    2. ¿Por qué pensaste que era un problema?
    3. ¿Qué estabas haciendo en el momento en que lo detectaste?
    4. ¿Cuándo se produjo por primera vez, y con qué frecuencia desde entonces?
    5. ¿De qué redes se trata? (oficina/casa/tienda, cableada/inalámbrica, con/sin VPN, *etc.*)
    6. ¿De qué sistemas se trata? (sistema operativo, nombre de host, *etc.*)
    7. ¿De qué datos se trata? (rutas, tipos de archivos, archivos compartidos, bases de datos, software, *etc.*)
    8. ¿Qué usuarios y cuentas están implicados? (directorio activo, SaaS, SSO, cuentas de servicio, *etc.*)
    9. ¿A qué datos suelen acceder los usuarios implicados?
    10. ¿Con quién más has contactado acerca de este incidente y qué les has dicho?
5. Haz las preguntas de seguimiento que sean necesarias. **Usted es el encargado de responder al incidente, contamos con usted.**
6. Obtenga información de contacto detallada del usuario (domicilio, oficina, móvil), si procede.
7. Registre toda la información en el ticket, incluyendo notas manuscritas y de voz.
8. Poner en cuarentena a los usuarios y sistemas afectados.
9. Póngase en contacto con el equipo de seguridad y estar preparados para participar en la respuesta según las indicaciones: investigación, reparación, comunicación y recuperación. # Roles

A continuación se presentan las descripciones, los deberes y la formación para cada uno de los roles definidos en la respuesta a un incidente.

Estructura de los roles

- Equipo de Mando
    - Jefe de Departamento
    - Subjefe de Departamento
    - Escriba
- Equipo de enlace
    - Enlace Interno Enlace
    - Enlace externo
- Equipo de Operaciones
    - Expertos en la materia (SMEs) para Sistemas
    - SMEs para equipos/unidades de negocio
    - SMEs para las funciones ejecutivas (*p.ej.*, Legal, RRHH, Finanzas) En el caso de incidentes complejos de mayor envergadura, la estructura

de funciones puede ajustarse para tener en cuenta la creación de subequipos.

Esta es una **estructura flexible**: cada rol no será ocupado por una persona diferente para cada incidente. Por ejemplo, en un incidente pequeño, el adjunto podría actuar como escribiente y enlace interno. La estructura es flexible y se adapta al incidente.

Tiempos de Guerra vs. Tiempos de Paz

En las llamadas de respuesta a Incidentes ("tiempos de guerra"), una estructura organizativa diferente anula las operaciones normales ("tiempos de paz"):

- El Jefe de Departamento está al mando. Independientemente de su rango en tiempos de paz, ahora es la persona de mayor rango en la llamada, superior al director general o CEO.
- Las decisiones serán tomadas por el Jefe de Departamento tras considerar la información presentada. Una vez tomada la decisión, es definitiva.
- El Jefe de Departamento puede tomar decisiones más arriesgadas que las que normalmente se considerarían en tiempos de paz.
- El Jefe de Departamento puede ir en contra de una decisión consensuada. Si se hace una encuesta, y 9/10 personas están de acuerdo pero 1 está en desacuerdo, el Jefe de Departamento puede elegir la opción del desacuerdo a pesar del voto de la mayoría. Aunque no esté de acuerdo, la decisión del Jefe de Departamento es definitiva. Durante la convocatoria no es el momento de discutir con ellos.
- El Jefe de Departamento puede utilizar un lenguaje o comportarse de una manera que usted considere grosera. Esto es tiempo de guerra, y necesitan hacer lo que sea necesario para resolver la situación, por lo que a veces se producen groserías. Esto no es personal, y es algo que debes estar preparado para experimentar si nunca has estado en una situación de guerra.
- Es posible que el Jefe de Departamento te pida que abandones la llamada, o incluso que te eche a la fuerza de una llamada. Esto queda a discreción del Jefe de Departamento si considera que no estás aportando nada útil. De nuevo, esto no es personal y debes recordar que los tiempo de guerra son diferentes a los tiempo de paz.

Roles: Todos los participantes

Descripción

Todos los participantes en la respuesta a un incidente tienen la responsabilidad de ayudar a resolver el incidente de acuerdo con el plan de respuesta a incidentes, bajo la autoridad del Jefe de Departamento.

Deberes

Herramienta de llamada La herramienta para la coordinación de los equipos para enfrentarse a las incidencias será el Google Meet, debido a sus funcionalidades de organización dentro de la llamada y su gestión.

Exhibir la etiqueta de la llamada

- Participar tanto en la llamada como en el chat.
- Mantener el ruido de fondo al mínimo.
- Mantener el micrófono silenciado hasta que tenga algo que decir.
- Identifícarse cuando entre en la llamada; diga su nombre y su función (por ejemplo, "Soy el SME del equipo x").
- Hablar con claridad.
- Ser directo y objetivo.
- Mantener las conversaciones/debates breves y al grano.
- Comunicar cualquier preocupación al Jefe de Departamento en la llamada.
- Respetar las limitaciones de tiempo dadas por el Jefe de Departamento.
- Si te unes a un solo canal (llamada o chat), no participar activamente, ya que provoca una comunicación inconexa.
- **Utilizar una terminología clara y evitar usar acrónimos o abreviaturas. La claridad y la precisión son más importantes que la brevedad.**

Referencia: Procedimiento común de voz El [procedimiento de voz] estándar de la radio (https://en.wikipedia.org/wiki/Voice_procedure#Words_in_voice_procedure) **no es obligatorio**, sin embargo, es posible que escuche ciertos términos (o que tenga que utilizarlos usted mismo). Las frases comunes incluyen:

- **Ack/Rog:** "He recibido y entendido"
- **Say Again:** "Repita su último mensaje"
- **Standby:** "Por favor, espere un momento para la siguiente respuesta"
- **Wilco:** "Cumpliré"

No invente nuevas abreviaturas; favorezca ser explícito sobre lo implícito.

Seguir al Jefe de Departamento El Jefe de Departamento es el líder del proceso de respuesta al incidente.

- Siga las instrucciones del Jefe de Departamento.
- No realice ninguna acción a menos que el Jefe de Departamento se lo indique.
- El jefe normalmente sondeará si hay objeciones fuertes antes de asignar una acción importante. Plantee sus objeciones si las tiene.
- Una vez que el jefe haya tomado una decisión, sígala (incluso si no está de acuerdo).
- Responde a cualquier pregunta que te haga el jefe de forma clara y concisa. Responder "no sé" es aceptable. No adivine.

- El jefe puede pedirte que investigues algo y que le contestes en X minutos. Esté preparado con una respuesta dentro de ese tiempo. Pedir más tiempo es aceptable, pero proporcione al jefe una estimación.

Capacitación

Lee y entiende el plan de respuesta a incidentes, incluyendo los roles y los libros de jugadas.

Rol: Jefe de Departamento

Descripcion

El Jefe de Departamento actua como la única fuente de lo que realmente está ocurriendo y va a ocurrir durante un incidente grave. El Jefe de Departamento es el individuo con mayor rango en cualquier llamada de incidente, sin importar el rango en el dia a dia. Ellos son los que toman decisiones durante un incidente; delegan tareas y prestan atencion a expertos en la materia que están tratando para resolver el incidente. Las decisiones tomadas por el Jefe de Departamento son las decisivas.

Tu trabajo como Jefe de Departamento es evaluar la situación, proveer un guiado claro y coordinado, contratar otros trabajadores para recolectar contexto/detalles.**No realizar investigaciones o remedios**, delega estos trabajos.

Deberes

Resuelve el incidente lo más rápido y seguro posible usando el plan de respuesta de incidentes como plantilla de trabajo: guia al equipo de investigacion, remedio, comunicación. Utiliza al adjunto para que te ayude, y delegue a relevantes enlaces y expertos a tu discreción.

1. Ayuda a prepararos para los incidentes,
    - Establecer canales de comunicación para incidentes.
    - Redirige a las personas hacia estos canales de comunicación cuando acurra algún incidente grave.
    - Entrena a miembros del equipo sobre como comunicarte durante incidentes y entrena a otros Jefe de Departamento.
2. Dirige los incidentes hacia una solución,
    - Lleva a todos al mismo canal de comunicación.
    - Recolecta información de los miembros del equipo por sus servicios de estatus.
    - Recolecta propuestas de reparación de acciones, después recomienda acciones de reparación para que se lleven a cabo.
    - Delega todas la acciones de reparación, el Jefe de Departamento no es un resolvedor.
    - Es la única fuente de autoridad en el estado del sistema.
3. Facilita las llamadas y reuniones,

- Gana consenso (Realiza encuestas durante las llamadas)
- Proporciona actualizaciones de estatus
- Reduce el alcance (despedir a los asistentes cuando sea posible)
- Spin off sub-equipos
- Transfiere el control cuando sea necesario
- Firmar las llamadas
- Mantener el orden
- Obtén respuestas directas
- Manejar las caídas de ejecutivos como
  - Anular al Incident Commander
  - Desmotivación
  - Petición de información
  - Cuestionar la severidad
- Manejar respuestas perturbadoras o beligerantes

4. Post Mortem,
   - Crear la plantilla inicial justo después del incidente para que las personas puedan escribir sus opiniones mientras están frescas.
   - Asignar el post-mortem después de que el evento termine, esto puede darse después de terminar la llamada.
   - Trabaja con los gerentes o jefes de equipo para organizar acciones preventivas.

El Jefe de Departamento utiliza métodos y lenguajes adicionales:

- Siempre anuncie cuando se una a la llamada si es el Jefe de Departamento de guardia.
- **No** permita que las discusiones se salgan de control. Mantenga las conversaciones cortas.
- Tenga en cuenta las objeciones de los demás, pero tu decision es la definitiva.
- Si alguien está interrumpiendo activamente tu decision, expúlsalo.
- Anuncia el final de la llamada.
- Después de un incidente, comuníquese con otros Jefe de Departamento sobre cualquier acción que considere necesaria.

Utilice una terminología clara y evite las siglas o abreviaturas. La claridad y la precisión son más importantes que la brevedad.

Prácticas

- Lea el plan de respuesta a incidentes, incluidos todos los roles y manuales.
- Participar en un ejercicio de respuesta a incidentes.
- Seguir a un Jefe de Departamento actual sin participar activamente, manteniendo sus preguntas hasta el final.
- Tomar la iniciativa de un Jefe de Departamento. Responda a incidentes con el Jefe de Departamento actual allí para hacerse cargo si es necesario.

pre-requisitos No hay requisitos previos de antigüedad o unidad de negocios para convertirse en Jefe de Departamento, es un rol abierto a cualquier persona con la capacitación y la capacidad. Antes de que pueda ser un Jefe de Departamento, se espera que cumpla con los siguientes criterios:

- Conocimientos básicos de ciberseguridad.
- Excelentes **habilidades de comunicación** verbal y escrita.
- **Conocimiento de alto nivel** de la infraestructura y las funciones comerciales.
- Excelente pensamiento crítico, juicio y toma de decisiones.
- Flexibilidad y capacidad para **escuchar comentarios de expertos**, modificando los planes según sea necesario.
- **Participó en al menos dos respuestas a incidentes**.
- Capacidad para **tomar el mando** y **disposición para expulsar a las personas de una llamada** para eliminar las distracciones, incluso si se trata del director ejecutivo.

¡No se requieren conocimientos técnicos profundos! Los Jefe de Departamento no requieren un conocimiento técnico profundo de nuestros sistemas. Su trabajo como Jefe de Departamento es coordinar la respuesta, no realizar cambios técnicos. No crea que no puede ser un Jefe de Departamento solo porque no está en el departamento de ingeniería.

Graduación Al finalizar el entrenamiento, agréguese a la lista de Jefe de Departamento.

Rol: adjunto del Jefe del Departamento (adjunto)

Descripción

Un adjunto del Jefe del Departamento (adjunto) es un papel de apoyo directo al Jefe de Departamento. El adjunto permite que el Jefe de Departamento se centre en el problema que tiene entre manos, en lugar de preocuparse por documentar los pasos o controlar los tiempos. El adjunto apoya al Jefe de Departamento y lo mantiene centrado en el incidente. Como adjunto, se espera que asuma el mando del Jefe de Departamento si éste lo solicita.

Funciones

1. Plantear al Jefe de Departamento cuestiones que, de otro modo, no se abordarían.
2. Ser un Jefe de Departamento “de reserva”, en caso de que el jefe principal tenga que hacer la transición a un SME, o tenga que alejarse de la función de Jefe de Departamento.
3. Gestionar la llamada del incidente y estar preparado para retirar a las personas de la llamada si así lo indica el Jefe de Departamento.

4. Supervisar el estado del incidente y notificar al Jefe de Departamento si el nivel de gravedad del incidente aumenta.
5. Supervise los temporizadores:
    - controlar el tiempo que ha durado el incidente
    - Notificar al Jefe de Departamento cada X minutos para que pueda tomar medidas (por ejemplo, "Jefe, el incidente está ahora en la marca de 10 minutos").
6. Supervisar los plazos de las tareas (*p.ej.*, "Jefe, avisa de que el temporizador de la investigación de [TEAM] se ha agotado").

Formación

- Leer y comprender el plan de respuesta a incidentes, incluyendo los roles y los libros de jugadas.
- La formación para este rol se usará la misma formacion que se ha hecho con el Jefe de Departamento.

Requisitos previos

- Estar entrenado como Jefe de Departamento.

Rol: Escriba

Descripción

Un escriba documenta la línea de tiempo de un incidente a medida que avanza, y se asegura de que todas las decisiones y datos importantes se capturen para su posterior revisión. El escriba debe centrarse en el archivo del incidente, así como en los elementos de seguimiento para una acción posterior.

Funciones

1. Asegurarse de que la llamada del incidente se está grabando.
2. 2. Anotar en el chat y en la línea de tiempo del expediente: los datos, eventos y acciones importantes, a medida que se producen. Específicamente:
    - Acciones clave a medida que se llevan a cabo
    - Informes de estado cuando el Jefe de Departamento los proporcione
    - Cualquier llamada clave durante la llamada o en la revisión final
3. Actualice el chat indicando quién es el Jefe de Departamento, quién es el adjunto y que usted es el escriba (si no lo ha hecho ya).

Escribir es más un arte que una ciencia. El objetivo es mantener un registro preciso de los eventos importantes que ocurrieron, Usa tu juicio y experiencia. Pero aquí hay algunas cosas generales que definitivamente querrás capturar como escriba.

- El resultado de cualquier decisión de la votación.
- Motivos por el cual no llegó a realizarse ciertas acciones, o preguntas que surgieron durante la decisión.

Formación

Lea y comprenda el plan de respuesta a incidentes, incluyendo los roles y los libros de jugadas.

Requisitos previos

- Excelentes habilidades de **comunicación verbal y escrita**.
- Cualquiera puede actuar como escriba durante un incidente, y son elegidos por el Jefe de Departamento al inicio de la llamada.
- Normalmente, el ayudante actuará como escriba.

Proceso de formación

- Lea el plan de respuesta a incidentes, incluyendo todos los roles y libros de jugadas.

Rol: Experto en la materia {Subject Matter Expert (SME)}

Descripción

Un experto en la materia (SME) es un experto en el dominio o responsable designado de un equipo, componente o servicio (un "área"). Está ahí para apoyar al Jefe de Departamento en la identificación de la causa del incidente, sugiriendo y evaluando las acciones de investigación, remediación y comunicación, y realizando el seguimiento de las mismas según se le encomiende.

Funciones

1. Diagnosticar problemas comunes dentro de su área de experiencia.
2. Solucionar rápidamente los problemas detectados durante un incidente.
3. Comunicación concisa:
    - Estado: ¿Cuál es el estado actual de su área? ¿Está buen estado o no?
    - Acciones: ¿Qué medidas hay que tomar si su zona no se encuentra en un buen estado?
    - Necesidades: ¿Qué apoyo necesita para realizar una acción?
4. Participar en las fases de investigación, remediación y/o comunicación de la respuesta.
5. Anunciar todas las sugerencias al comandante del incidente, es su decisión cómo proceder, no siga ninguna acción a menos que se le indique.

Si está de guardia para cualquier equipo, puede ser llamado para un incidente y se espera que responda como experto en la materia (SME) para su equipo,

componente o servicio. Cualquiera que se considere un "experto en la materia" puede actuar como SME para un incidente. Por lo general, el principal de guardia del equipo actuará como SME para ese equipo.

Prepárese para el periodo de guardia

1. Esté preparado, habiéndose familiarizado ya con nuestras políticas y procedimientos de respuesta a incidentes.
2. Asegúrese de que ha configurado sus métodos de alerta de acuerdo con nuestro procedimiento de guardia.
3. Compruebe que puede unirse a la llamada de incidentes. Es posible que tenga que instalar un plugin para el navegador.
4. Tenga en cuenta su próxima vez de guardia y organice los cambios en función de los viajes, las vacaciones, las citas, etc.
5. Si usted es el Jefe de Departamento, asegúrese de no estar de guardia con su equipo al mismo tiempo que está de guardia como Jefe de Departamento.

Durante el periodo de guardia

1. Tenga su ordenador portátil e Internet con usted en todo momento durante su período de guardia (oficina, casa, un MiFi, un teléfono con un plan de conexión, etc).
2. Si tiene citas importantes, debe conseguir que otra persona de su equipo cubra esa franja horaria con antelación.
3. Cuando recibas una alerta de incidente, se espera que te unas a la llamada de incidente y chatees lo antes posible (en cuestión de minutos).
4. El Jefe de Departamento le hará preguntas o le dará acciones. Responde a las preguntas de forma concisa y sigue todas las acciones que se te den (incluso si no estás de acuerdo con ellas).
5. Si no estás seguro de algo, haz venir a otros miembros de tu equipo que puedan ayudarte. **Nunca dudes en escalar**, si es necesario.

6. No culpes. Este proceso de respuesta a incidentes no tiene ninguna culpa: culpar es contraproducente y distrae del problema en cuestión. La revisión posterior a la acción identificará los puntos en los que todos podemos mejorar.

Formación

- Lea y comprenda el plan de respuesta a incidentes, incluidas las funciones y las guías de actuación.

Rol: Enlace

Descripción

Los enlaces interactuan con otros equipos o partes interesadas fuera del equipo de respuesta a incidentes. A menudo incluyen:

- Enlace externo: responsable de interactuar con clientes, ya sea directamente o por vía pública.
- Enlace interno: responsable de interactuar con las partes interesadas internas. Tanto si se trata de notificar un incidente al equipo interno como al movilizar respuestas adicionales dentro de la organización.

Deberes

Enlace con el exterior o con el cliente

1. Subir cualquier mensaje de cara al público con respecto al incidente (Twitter, etc).
2. Notificar al Jefe de Departamento de cualquier cliente o medios de comunicación que informen de los efectos del incidente.
3. Proporcionar a los clientes el mensaje externo del post-mortem una vez que se haya completado.
4. Contactar o interactuar con las partes interesadas externas, como proveedores, socios, fuerzas de seguridad, *etc.*
5. **No** sentirse responsable de la creación de cada mensaje: trabajar con el Jefe de Departamento y otras partes interesadas.
6. Según proceda, mantener a los clientes informados durante un incidente.
7. Actuar como voz de nuestros clientes ante el Jefe de Departamento, ya que esto es útil para la toma de decisiones del Jefe de Departamento.
8. Obtener la aprobación del mensaje después de haber elaborado el mensaje público: copiar el mensaje en el chat y esperar la confirmación verbal/escrita del Jefe de Departamento antes de continuar.
9. No sentirse responsable por las decisiones que se toman. Solo, sigues ordenes de el Jefe de Departamento, aunque te sientas culpable de una acción, no es culpa tuya.

Pistas para mensajes públicos

- Preparar de antemano un mensaje por defecto que pueda utilizarse para la actualización inicial si se desconoce el alcance del problema.
- Sé honesto. No mientas o supongas.
- Describa nuestros progresos en la resolución del incidente.
  - *"Somos conscientes de un incidente..."*
  - *"Estamos investigando los retrasos en las notificaciones..."*
  - *"Se ha aplicado una corrección y se está desplegando actualmente..."*
  - *"El problema ha sido resuelto..."*

- Explique claramente cómo afecta el incidente a los clientes. Esta es la principal información que les interesa a los clientes.
- Proporcionar soluciones que los clientes puedan utilizar hasta que se resuelva la incidencia.
- No calcule los tiempos de resolución.
- Proporcionar el nivel de detalle adecuado.
- Resolver cualquier duda que se le genera al cliente, si tiene alguna duda.

Enlace interno

1. Página de SMEs u otro personal de guardia según las instrucciones del Incident Commander.
2. Notificar o movilizar a otros equipos de la organización (por ejemplo, Finanzas, Legal, Marketing), según las instrucciones del Incident Commander.
3. Seguir y anticiparse a los SMEs en la convocatoria.
4. Interactuar con las partes interesadas y proporcionar actualizaciones de estado cuando sea necesario.
5. Interactuar con las partes interesadas internas para responder a sus preguntas, para mantener la llamada principal libre de distracciones.
6. Proporcionar actualizaciones periódicas de la situación al equipo ejecutivo, ofreciendo un resumen ejecutivo de la situación actual.

Formación

Leer y comprender el plan de respuesta a incidentes, incluyendo los roles y las guías.

Prerequisitos

- Excelentes **habilidades de comunicación** verbal y escrita.

Informe de Revisión Posterior a la Acción (AAR)

Preparación del AAR

1. Miembros implicados Identificamos a los participantes clave que estuvieron involucrados en la respuesta al incidente. Esto incluye al equipo de seguridad de TI, al equipo de respuesta a incidentes, a los administradores de los sistemas y a cualquier parte interesada relevante al evento.
2. Agenda Estableceremos una agenda para la AAR, esto incluye una revisión de los hechos, una discusión de lo que salió bien y lo que se puede mejorar, y la identificación de lecciones aprendidas.
3. Documentación Recopilaremos toda la documentación relevante. Esto incluye registros de incidentes, playbooks utilizados, comunicaciones internas y externas, y cualquier otra información relevante.

Realización del AAR

1. Reuniones Se organizarán reuniones para llevar a cabo el AAR. Nos aseguraremos de que todos los participantes clave estuvieran presentes y de que se dispusiera de suficiente tiempo para una discusión detallada.
2. Comunicación del Estado Se comenzará con una descripción general del incidente y de las acciones tomadas en respuesta. Esto incluye cuando ocurrió, como se descubrió, sistemas afectados, datos afectados y que acciones se llevaron a cabo en respuesta al incidente.
3. Discusión Se realizará una discusión abierta y honesta. Se pedirá a cada participante que comparta su perspectiva sobre el incidente y su respuesta. Incluyendo lo que salió bien, lo que se podría haber hecho mejor y cualquier lección aprendida en el proceso.

Identificación de lecciones aprendidas

1. Lecciones aprendidas Basándonos en la discusión, identificaremos las lecciones clave aprendidas. Esto incluye las áreas de mejor fortaleza, así como las áreas que debemos mejorar.
2. Plan de acción Para cada lección aprendida, desarrollaremos un plan de acción correspondiente. Esto incluye cambios en los playbooks, formación del personal, actualizaciones de las políticas, etc.

Comunicación de los Resultados

1. Informe AAR Se redactará un informe de la AAR que documentará los hallazgos y las lecciones aprendidas. Este informe será compartido con todas las partes interesadas relevantes.
2. Seguimiento Se realizará un seguimiento regular de los planes de acción para asegurarnos de que se estaban implementando. Consideramos la posibilidad de realizar una AAR de seguimiento después de un periodo de tiempo para revisar los progresos y las lecciones aprendidas adicionales.

Acerca de

Esta plantilla ha sido creada por el equipo de Counteractive Security, para ayudar a todas las organizaciones a comenzar de forma concisa, directa, especifica, flexible y gratuita un plan de respuesta de incidentes. crea un plan que utilizaras para responder de manera eficiente, minimizando los costes e impactos, para volver a trabajar lo mas rapido posible.

Licencia

Instrucciones

Personaliza esta plantilla para tu organizacion. Las instrucciones estan disponibles en el README del projecto. Para asistencia profesional con respuestas de incidentes, o con customizacion, implementacion, o testeo de tu plan, porfavor contacta con nosotros por email o telefono.

Referencias y material adicional

- NIST Computer Security Incident Handling Guide (NIST)
- CERT Societe Generale Incident Response Methodologies
- NIST Cybersecurity Framework
- Incident Handler's Handbook (SANS)
- Responding to IT Security Incidents (Microsoft)
- Defining Incident Management Processes for CSIRTs: A Work in Progress (CMU)
- Creating and Managing Computer Security Incident Handling Teams (CSIRTS) (CERT)
- Incident Management for Operations (Rob Schnepp, Ron Vidal, Chris Hawley)
- *Incident Response & Computer Forensics, Third Edition* (Jason Luttgens. Matthew Pepe. Kevin Mandia)
- *Incident Response* (Kenneth R. van Wyk, Richard Forno)
- The Checklist Manifesto (Atul Gawande)
- The Field Guide to Understanding Human Error (Sidney Dekker)
- Normal Accidents: Living with High-Risk Technologies (Charles Perrow)
- Site Reliability Engineering (Google)
- Debriefing Facilitation Guide (Etsy)
- Every Minute Counts: Leading Heroku's Incident Response (Blake Gentry)
- Three Analytical Traps in Accident Investigation (Dr. Johan Bergström)
- US National Incident Management System (NIMS) (FEMA)
- Informed's NIMS Incident Command System Field Guide (Michael J. Ward)
- Advanced PostMortem Fu and Human Error 101 (Velocity 2011)
- Blame. Language. Sharing.