Plan de respuesta a incidentes para Powerpuff

Autor: Grupo 4, powerpuff@proton.me

Revisión 1, Publicado 23 Mar 2023

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 23 Mar 2023. Fue probado por última vez en 28 Mar 2023.

Contents

Plan de respuesta a incidentes para Powerpuff

Autor: Grupo 4, powerpuff@proton.me

Revisión 1, Publicado 23 Mar 2023

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 23 Mar 2023. Fue probado por última vez en 28 Mar 2023.

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. Llame al Incident Commander de turno/de guardia.
2. **No** discuta el incidente fuera del equipo de respuesta a menos que el Incident Commander lo autorice
3. Inicie y/o únase al chat de respuesta en discord.gg/IkdosuTSm.
4. Iniciar y/o unirse a la llamada de respuesta en 609128234 y/o meet.google.org/syn-fcts-xzh.
5. Preferible usar la llamada de voz, el chat y el intercambio seguro de archivos sobre cualquier otro método.
6. **No** utilizar el correo electrónico principal si es posible. Si el correo electrónico es necesario, utilícelo con moderación o use correo alternativo en pm.power.puff@proton.me. Encripte los correos electrónicos cuando cualquier participante esté fuera del dominio powerpuff.org.
7. **No** usar SMS/texto para comunicar el incidente, a menos que sea para decirle a alguien que se mueva a un canal más seguro.
8. Invite al personal de turno/guardia a la llamada y al chat de respuesta.
    - Invite al equipo de seguridad.

    - Invitar al SME de los equipos y sistemas afectados.
    - Invitar a las partes interesadas ejecutivas y a los asesores jurídicos lo antes posible, pero dar prioridad a los responsables operativos.

9. OPCIONAL:_ Establecer una sala de colaboración en persona (“sala de guerra”) para 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	powerpuff.org/incident_commander
Lista del Incident Commander	powerpuff.org/incident_commander_roster
Lista del equipo de seguridad	Ismael García Vela
Lista del equipo SME	María Dolores Galán Tejero
Lista de ejecutivos	Daniel Sánchez Gómez

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 10 minutos** 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 7 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.
- **Utilizar una terminología clara y evitar acrónimos o abreviaturas. La

claridad y la precisión son más importantes que la brevedad.

Realizar la actualización de la respuesta

- Llevar a cabo actualizaciones programadas utilizando la estructura de llamada de actualización cada 7 horas en el puente activo.
- 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** pregunte 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.

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 powerpuff.org/files/823982 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	powerpuff.org/cil
Lista de activos críticos	powerpuff.org/cal
Base de datos de gestión de activos	powerpuff.org/assets
Mapa de red	powerpuff.org/netmap
Consola SIEM	siem.powerpuff.org
Agregador de registros	elk.powerpuff.org

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?
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 sophos.
- 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 DumpIT.
- Recoger la imagen del disco, si es necesario, utilizando FTK Imager.

- 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 powerpuff.org/files/823982 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 ir.powerpuff.org/report/template. **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: ir.powerpuff.org/report/recipients.

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 equipo de cumplimiento, legal@powerpuff.org.

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 equipo de marketing, marketing@powerpuff.org.
- 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 la oficina principal, bosses@powerpuff.org y equipo de lo legal, legal@powerpuff.org antes de interactuar con las fuerzas del orden.
- Póngase en contacto con las fuerzas del orden locales en Cuerpo Nacional de Policía, policia@gov.es.
- Póngase en contacto con el FBI en 1-800-CALL-FBI (225-5324), 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 Infosec Institute 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 {https://www.support.net para que le ayude con las relaciones públicas y la comunicación externa.
- Póngase en contacto con Ifar, https://ifar.es 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://info.net/industry/contact, 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

Identificar, informar, configurar y comunicar!

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

Identificar el ataque

El primer paso es determinar si realmente se está produciendo un ataque DDoS. A menudo, los sistemas afectados pueden parecer lentos o inaccesibles, pero esto también puede ser causado por problemas de red o por el tráfico legítimo excesivo. Para determinar si realmente se trata de un ataque DDoS, debemos realizar las siguientes acciones:

- Monitorear los registros del servidor para ver si hay un aumento inusual en la cantidad de tráfico de entrada.
- Verificar si hay múltiples solicitudes de un solo origen o varias solicitudes de múltiples orígenes.
- Utilizar herramientas de análisis de red, como Wireshark, para capturar y analizar el tráfico de red.

Si se confirma que estamos siendo objeto de un ataque DDoS, debemos pasar al siguiente paso.

Informar al proveedor de servicios de internet (ISP)

Es importante informar al proveedor de servicios de internet (ISP) para que puedan ayudarnos a mitigar el ataque. Muchos ISP tienen medidas de seguridad en su lugar para detectar y mitigar los ataques DDoS.

Al informarles, podemos obtener su asistencia para proteger nuestra red y reducir el impacto del ataque. Es importante tener disponible el número de teléfono o dirección de correo electrónico de contacto del proveedor de servicios de internet.

Configurar el cortafuegos para bloquear el tráfico no deseado

Para reducir el impacto del ataque, podemos configurar el cortafuegos para bloquear el tráfico no deseado. Podemos hacer esto configurando las reglas del

firewall para bloquear todo el tráfico excepto el tráfico de los puertos necesarios para el funcionamiento normal del sistema.

También podemos bloquear direcciones IP sospechosas o todo el tráfico entrante de un país en particular si detectamos que la mayor parte del tráfico malintencionado proviene de ese país.

Redirigir el tráfico legítimo a servidores alternativos

Otra estrategia para reducir el impacto del ataque es redirigir el tráfico legítimo a servidores alternativos. Podemos hacer esto mediante la configuración de DNS o mediante la redirección de tráfico a través de un balanceador de carga.

Si bien esto puede no detener completamente el ataque DDoS, puede reducir su impacto al asegurarnos de que el tráfico legítimo pueda llegar a nuestros servidores.

Monitorear el tráfico y ajustar las medidas de seguridad

Es importante monitorear continuamente el tráfico de red para asegurarnos de que las medidas de seguridad que hemos implementado estén funcionando correctamente.

Si detectamos nuevas fuentes de tráfico malicioso, debemos ajustar nuestras medidas de seguridad para bloquearlos.

Mantener informados a los usuarios

Durante un ataque DDoS, es importante mantener informados a los usuarios sobre el estado de nuestros sistemas y las medidas que estamos tomando para mitigar el ataque.

Podemos hacer esto mediante la publicación de actualizaciones en nuestro sitio web o a través de las redes sociales.

Lista de verificación

Para finalizar, se tendrían que verificar que la siguiente lista de acciones se han realizado:

- Monitorear registros del servidor
- Verificar origen del tráfico
- Utilizar herramientas de análisis de red
- Tener disponible información de contacto del proveedor de servicios de internet
- Informar al proveedor de servicios de internet
- Configurar reglas del firewall
- Bloquear direcciones IP sospechosas
- Bloquear tráfico entrante de países sospechosos

- Redirigir tráfico legítimo a servidores alternativos
- Monitorear tráfico de red
- Ajustar medidas de seguridad
- Publicar actualizaciones en nuestro sitio web o a través de las redes sociales

Playbook: Desaparición de sitios web

Investigar, remediar (contener, erradicar) y comunicar en paralelo! Asigne los pasos a individuos o equipos para que trabajen simultáneamente, cuando sea posible; este playbook no es puramente secuencial. Utilice su mejor criterio.

Investigar

1. Desconecte inmediatamente el servidor desconfigurado para investigarlo.
    - Esto es especialmente importante si la desfiguración es insultante o provocadora de algún modo. Elimine esto de la vista del público tan pronto como sea posible para evitar daños, así como para mitigar el impacto del negocio.
    - El mensaje de desfiguración también puede contener información falsa que podría confundir a los usuarios o ponerlos en peligro.
    - Desconectar el servidor permitirá una investigación más profunda de la desfiguración. Esto puede ser necesario, ya que el ciberdelincuente puede haberse adentrado en la organización accediendo a servidores de aplicaciones, bases de datos, etc.
2. Determine el origen de la vulnerabilidad del sistema que ha utilizado el atacante. Los exploits más comunes son:
    - Ataques de inyección SQL
        - Este tipo de ataque se produce cuando un atacante interfiere en las consultas de una aplicación a la base de datos. Por lo tanto, esto puede conducir a un acceso no autorizado a datos privados o sensibles. Lea más sobre los ataques de inyección SQL aquí
    - Ataques de inclusión remota de archivos (RFI)
        - Este tipo de ataque explota la función de referencia de una aplicación para cargar malware desde una URL remota. Más información sobre los ataques RFI aquí
    - webshells
        - Más información sobre web shells y defacement de sitios web aquí
    - mal diseño de aplicaciones web
        - hacks de javascript
        - hacks de PHP/ASP
        - Aquí hay más sobre hacking con javascript
    - otros métodos de detección incluyen:
        - Comprobar los registros del servidor
            * buscar en el registro de acceso y en el registro de errores de la página web cualquier actividad sospechosa o desconocida

        * por supuesto, también es una buena idea comprobar los registros del firewall IDS o IPS, si están disponibles
    - Comprobar los archivos con contenido estático
    - Escanear las bases de datos en busca de contenido malicioso
    - Comprobación de los enlaces presentes en la página
3. Recoge cualquier pista sobre quién es el ciberdelincuente o para qué organización trabaja. Considera las siguientes preguntas:
    - ¿Qué representa la desfiguración? ¿Incluía un mensaje obvio?
    - ¿Parece que la desfiguración es inofensiva o intencionada? ¿Podría ser el ciberdelincuente un niño jugando o un grupo profesional que trabaja con un motivo?
    - ¿Parece que su organización haya sido el objetivo? ¿Quién podría querer atacar a su organización?
    - ¿Qué esperaba conseguir el ciberdelincuente?
    - Consulta aquí para saber más sobre los tipos de ciberdelincuentes que pueden haber atacado tu página web.
4. Recoge otra información importante de la página que ha sido desfigurada, como por ejemplo
    - una captura de pantalla de la desfiguración
    - el dominio y la dirección IP de la página
    - detalles del servidor web
    - el código fuente de la página
        - analizarlo cuidadosamente para identificar el problema y asegurarse de que se encuentra en un servidor de la empresa
    - nombre o cualquier información sobre el atacante
5. También existen herramientas que ayudan a la detección y al análisis de los registros. A continuación se enumeran algunas de ellas:
    - Weblog Expert
    - Sawmill
    - Deep Log Analyzer

Remediar

Planificar eventos de reparación en los que estos pasos se pongan en marcha juntos (o de forma coordinada), con los equipos adecuados listos para responder a cualquier interrupción. * **Considere el momento y las compensaciones** de las acciones de remediación: su respuesta tiene consecuencias.

Contención

1. Haga una copia de seguridad de todos los datos almacenados en el servidor web con fines forenses.
2. Como se ha mencionado anteriormente, asegúrese de que el servidor de la página desfigurada está temporalmente fuera de servicio mientras se lleva a cabo la investigación.
    - Debe tener una página de error preparada para esta situación que

informe al usuario y/o a los empleados de que el mantenimiento está en marcha y que la página que buscaban volverá en breve. Incluso podría tener preparada una página web de respaldo en la que pueda publicar contenido mientras se lleva a cabo la investigación y la reparación, y hacer que su página de error temporal redirija a los usuarios a este sitio de respaldo.
    - Compruebe su mapa de arquitectura de red. Si la brecha es otro sistema de la red, descárguelo e investíguelo.
3. Una vez que se haya determinado el origen del ataque, aplique los pasos necesarios para garantizar que esto no vuelva a suceder. Esto puede incluir la modificación del código o la edición de los derechos de acceso.
    - Consulte la sección "Investigar" para conocer las fuentes comunes de vulnerabilidad.
    - Si esto está fuera de su dominio, simplemente asegúrese de que ha dado al personal apropiado toda la información sobre el ataque que tiene y permita que los expertos hagan su trabajo.

Recover

1. Elimine el mensaje del ciberdelincuente y reemplácelo por el contenido original y legítimo. Si se han perdido datos en el ataque, consulte las copias de seguridad y restaure la página original en la medida de lo posible.
    - Compruebe las copias de seguridad en busca de indicadores de compromiso
    - Considere la recuperación parcial y la prueba de integridad de las copias de seguridad
2. Considere pedir a los usuarios que cambien sus credenciales de acceso si el servidor web tiene autenticación de usuario.
3. Después de aplicar las medidas para evitar riesgos (como se recomienda a continuación), restaure su servidor mostrando el contenido original de la página.
4. Si es necesario y/o aplicable, prepare una disculpa/explicación del ataque ocurrido para los usuarios o cualquier persona que haya presenciado la desfiguración. Asegúrese de que queda claro que el contenido desfigurado no refleja a su organización de ninguna manera.

Evitar riesgos

1. Utilice el menor número de plug-ins posible. Los piratas informáticos tienen como objetivo los sitios web que son vulnerables y tienen muchas fuentes de entrada. Puedes limitar estas fuentes de entrada utilizando sólo lo que necesites y eliminando los plug-ins y el software que no utilices o sean antiguos. También es importante actualizarlos lo antes posible.
2. Controle de cerca y ordene el acceso a los contenidos administrativos. Permita que las personas accedan sólo a lo que necesitan. Esto reducirá la posibilidad de que un error humano provoque un ciberataque. Hay más

métodos de prevención DIY mencionados en este artículo (pasos 6-12) y en el recurso #4 al final de este playbook.
3. Comprueba regularmente si hay malware en tu sitio web escaneando el código fuente. Busca scripts, iframes o URLs que te parezcan desconocidos y asegúrate de escanear también las URLs que sí te resulten familiares.
4. Hay muchos escáneres automáticos de sitios web de gran reputación que no le costarán nada de su tiempo y escanearán a fondo su sitio en busca de vulnerabilidades con regularidad. Aquí hay un enlace a escáneres populares.
5. Defiéndase contra los puntos comunes de explotación, como las inyecciones SQL y los ataques XSS. Este artículo incluye las mejores prácticas para defender estos ataques.
6. Instala programas de detección de desfiguración para que, si volviera a producirse un ataque, estés preparado y respondas rápidamente. Aquí hay un artículo que resume algunos de los mejores servicios de monitoreo de 2020.
7. Habla con tus empleados de la importancia de mantener el acceso administrativo limitado y confidencial e infórmales de estos pasos para evitar incidentes, incluyendo la formación periódica de concienciación sobre ciberseguridad.

Comunicar

1. 1. Elevar el incidente y comunicarlo a la dirección según el procedimiento
2. 2. Documentar el incidente según el procedimiento (e informar si procede)
3. Comunicarse con los asesores jurídicos internos y externos según el procedimiento, incluyendo discusiones sobre el cumplimiento, la exposición al riesgo, la responsabilidad, el contacto con las fuerzas del orden, *etc.*.
4. Comunicarse con los usuarios (internos)
    1. Comunicar las actualizaciones de la respuesta a incidentes según el procedimiento
    2. Comunicar el impacto del incidente **y** las acciones de respuesta al incidente (por ejemplo, contención: "¿por qué está caído el archivo compartido?")
    3. Comunicar los requisitos: "¿qué deben hacer y no hacer los usuarios?"
5. Comunicar a los clientes
    1. Centrarse especialmente en aquellos cuyos datos se vieron afectados
    2. Generar las notificaciones requeridas en base a las regulaciones aplicables (particularmente aquellas que puedan considerar la desfiguración como una violación de datos o que requieran notificaciones de otro tipo).

6. Contactar con los proveedores de seguros
    1. Discutir qué recursos pueden poner a disposición, qué herramientas y proveedores apoyan y pagarán, *etc.*.
    2. Cumplir con los requisitos de presentación de informes y reclamaciones para proteger la elegibilidad
7. Considerar la posibilidad de notificar e implicar a las fuerzas del orden. TODO: Vincule las siguientes viñetas con los recursos reales de su organización
    1. Aplicación de la ley local
    2. 1. Aplicación de la ley a nivel estatal o regional
    3. 1. Fuerzas de seguridad federales o nacionales
8. Comuníquese con los proveedores de seguridad y de TI
    1. Notifique y colabore con proveedores gestionados según el procedimiento
    2. 2. Notificar y colaborar con consultores de respuesta a incidentes por procedimiento

Recursos

Referencia: Acciones del usuario ante un ataque de sospecha de defacement

1. Mantenga la calma y respire profundamente.
2. 2. Desconecte su sistema de la red.
3. Haz fotos de la página que veas con tu smartphone mostrando las cosas que has notado: el mensaje de desfiguración y cualquier otro cambio en el sitio habitual.
4. 2. 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:
    3. ¿Qué has notado?
    4. ¿Cuándo ocurrió por primera vez, y con qué frecuencia desde entonces?
    5. ¿A qué datos suele acceder?
    6. ¿Con quién más se ha puesto en contacto en relación con este incidente y qué le ha dicho?
5. Ponte en contacto con el servicio de asistencia y sé lo más servicial posible.
6. Ten paciencia: deja que el personal informático lo controle, ¡puedes estar protegiendo a otros de un daño! **Gracias.**

Referencia: Acciones del Help Desk ante un presunto ataque de defacement

1. Mantenga la calma y respire profundamente.
2. Abra un ticket para documentar el incidente, según el procedimiento.
3. Utiliza tu mejor criterio para decidir qué pasos priorizar (por ejemplo, si la desfiguración dejó contenido dañino o desencadenante, prioriza la retirada del servidor inmediatamente).
4. Pídele al usuario que tome fotos de su pantalla con su teléfono inteligente mostrando las cosas que notó.
5. 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, haga preguntas detalladas, incluyendo 1. ¿Qué has notado?
    1. ¿Cuándo ocurrió por primera vez, y con qué frecuencia desde entonces?
    2. ¿A qué datos suele acceder?
    3. ¿Con quién más se ha puesto en contacto en relación con este incidente y qué le ha dicho?
6. Haga las preguntas de seguimiento que sean necesarias. **Usted es una persona que responde al incidente, contamos con usted.**
7. Obtenga información de contacto detallada del usuario (domicilio, oficina, móvil), si procede.
8. Registre toda la información en el ticket, incluyendo notas manuscritas y de voz.
9. Ponga en cuarentena a los usuarios y sistemas afectados.
10. Póngase en contacto con el [equipo de seguridad] (#TODO-link-to-actual-resource) y prepárese para participar en la respuesta según las indicaciones: investigación, reparación, comunicación y recuperación.

Información adicional

1. Un útil y detallado paper sobre la detección de la desfiguraciónw
2. 10 herramientas parabetter website monitoring and security
3. 2019 Website Threat Research Report con estadísticas útiles
4. Article incluyendo bricolaje y mejores prácticas para evitar la desfiguración de sitios web

Playbook: Compromiso de identidad y acceso

El compromiso de identidad y acceso es una de las amenazas más comunes en el mundo de la seguridad informática. Es fundamental contar con un plan de acción para minimizar el impacto y recuperarse rápidamente.

Investigar

- Identificar la fuente del compromiso de identidad y acceso. ¿Fue a través de un ataque externo o interno?

- Analizar los registros de actividad del sistema y la red para detectar cualquier actividad sospechosa.
- Identificar el alcance del compromiso. ¿Qué datos, sistemas o recursos se han visto comprometidos?
- Recopilar información sobre los usuarios afectados. ¿Qué usuarios se vieron afectados por el compromiso de identidad y acceso?
- Realizar un análisis forense para determinar cómo se produjo el compromiso de identidad y acceso.
- Identificar cualquier otra amenaza potencial y tomar medidas preventivas adicionales.

Remediar

- Planificar eventos de remediación en los que estos pasos se lancen juntos (o de forma coordinada), con los equipos apropiados listos para responder a cualquier interrupción.
- Considere el tiempo y las compensaciones de las acciones de remediación: su respuesta tiene consecuencias.

Contención

- Pasos en la conteción:
  - Identificar y aislar el sistema comprometido:
    - Identificar el sistema afectado, aislarlo y establecer controles de acceso.
  - Detener la propagación del compromiso:
    - Identificar y detener el compromiso.
  - Recopilar evidencia y datos de actividad:
    - Activar la monitorización recopilando logs y registros de actividad relevantes.
    - Identificar y recuperar cualquier dato o archivo comprometido.
  - Actualizar y parchear sistemas afectados:
    - Identificar vulnerabilidades explotadas, aplicarles actualizaciones y parches de seguridad en los sistemas afectados y verificarción de ello.
  - Realizar análisis forense:
    - Realizar análisis forense para identificar la causa raíz del compromiso.
    - Identificar y analizar cualquier malware encontrado en los sistemas afectados.
    - Identificar cualquier acceso no autorizado o actividad maliciosa.
  - Comunicación y colaboración:
    - Mantener una comunicación abierta y constante con el equipo.

        * Trabajar en colaboración para compartir información y recursos.

- Herramientas y procedimientos:

  Estas son algunas herramientas que se pueden utilizar tras un compromiso de identidad y acceso:

  - Identificación y aislamiento: Herramientas de monitorización de red y firewall para bloquear tráfico no autorizado. (Wireshark)
  - Detención de la propagación: Herramientas de detección de malware, análisis de procesos y bloqueo de direcciones IP y dominios. (Malwarebytes o Norton)
  - Recopilación de evidencia: Herramientas de monitorización de actividad, recuperación de datos y análisis de logs. (OSSEC, Recuva y Splunk)
  - Actualización y parcheo: Herramientas de análisis de vulnerabilidades. (Nessus y WSUS)
  - Análisis forense: Herramientas de análisis de malware, análisis de memoria y análisis de registro. (Volatility, FTKImager o RegRipper)

Erradicar

- Pasos en la erradicación:
  - Eliminar el malware o software malicioso que se haya identificado como responsable del compromiso.
  - Realizar una revisión exhaustiva de los sistemas y dispositivos comprometidos para asegurarse de que se han eliminado todas las amenazas.
  - Restablecer los sistemas y dispositivos afectados a un estado seguro conocido.
  - Realizar una revisión de seguridad adicional para confirmar que se han eliminado todas las amenazas y que los sistemas y dispositivos son seguros para su uso.
- Herramientas y procedimientos:

  Estas son algunas herramientas que se pueden utilizar tras un compromiso de identidad y acceso:

  - Herramientas de eliminación de malware: Malwarebytes.
  - Herramientas de recuperación de sistemas: System Restore en Windows o Acronis.
  - Herramientas de verificación de integridad del sistema: Como Microsoft Baseline Security Analyzer o Nessus.

Referencia: Recursos de remediación

- Identificar los recursos financieros necesarios para llevar a cabo la remediación.
- Identificar los recursos de personal necesarios para llevar a cabo la remediación.
- Identificar los recursos logísticos necesarios para llevar a cabo la remediación.

Comunicar

- Comunicar a los usuarios afectados sobre el compromiso y las medidas que se están tomando para remediarlo.
- Comunicar a los equipos de TI y de seguridad sobre el compromiso y las medidas que se están tomando para remediarlo.
- Comunicar a la alta dirección sobre el compromiso y las medidas que se están tomando para remediarlo.
- Comunicar a los accionistas sobre el compromiso y las medidas que se están tomando para remediarlo.

Recuperación

- Restaurar los sistemas y recursos afectados a su estado anterior al compromiso.
- Realizar una revisión de seguridad adicional para confirmar que los sistemas y recursos restaurados son seguros para su uso.

Recursos

Información adicional

`1. Compromiso de identidad y acceso, Sánchez (28/03/2023)`

playbook-ingenieria-social

Es fundamental que los empleados de la organización puedan identificar y saber actuar ante una alerta de una posible amenaza de ingeniería social.

¡Este documento puede variar dependiendo del tipo de ataque que se realice!

Identificación.

Para empezar deberemos responder a las siguientes preguntas para tener una idea clara de a lo que nos enfrentamos:

- ¿Nos han pedido demasiada información o información muy específica?
- ¿El correo electrónico, mensaje o llamada contiene errores de ortografía, gramática, formato o contenido inusual?
- ¿El remitente o la persona que llama ejerce presión para que se tome una acción rápida sin pensar?
- ¿Se solicita que se haga alguna acción sin consentimiento previo a algún superior?

Si la respuesta a algunas de estas preguntas ha sido "Sí", nos enfrentamos a un ataque de ingeniería social.

Investigación.

Si se ha identificado un posible intento de ingeniería social, es importante investigar y recopilar información para determinar si se trata de una amenaza real y su gravedad.

Para ello podemos seguir estas acciones:

- Verificar al remitente: obtener información sobre el remitente y rastrear su origen para determinar si es legítimo o no.
- Consultar con el personal de seguridad o TI: verifique si se han reportado incidentes similares recientemente. Pregunte al personal de seguridad o de TI si han visto alguna actividad sospechosa o si hay alguna amenaza conocida que pueda estar relacionada con el mensaje o llamada.
- Buscar patrones o tendencias: revise otros mensajes de correo electrónico, llamadas o solicitudes similares que se hayan recibido recientemente para identificar patrones o tendencias. Si hay varios incidentes similares, esto puede indicar una campaña de ingeniería social más amplia.

Una vez que se ha recopilado la información, determine el nivel de gravedad del incidente. La gravedad se puede determinar por el tipo de información solicitada o acción requerida, la credibilidad del remitente o la persona que llama, y la probabilidad de que la amenaza se materialice.

Es importante recordar que durante esta fase se deben tomar precauciones para evitar que la amenaza se propague. La información recopilada debe manejarse de manera segura y sólo debe ser compartida con las personas involucradas en la respuesta al incidente.

Respuesta y mitigación.

La respuesta a un incidente de ingeniería social debe ser rápida y eficiente para minimizar el daño potencial. Además, se deben tomar medidas para prevenir futuros incidentes.

Estas medidas podrían ser:

- Informar a las partes afectadas: si se ha comprometido información confidencial, informe a las partes afectadas de inmediato. Proporcione detalles sobre lo que ha sucedido y las medidas que se están tomando para remediar la situación.
- Restablecer contraseñas: en caso de que se haya comprometido una contraseña o credencial de inicio de sesión, es importante restablecerla de inmediato. Se deben restablecer todas las contraseñas relacionadas y se deben establecer políticas más estrictas para la creación y el almacenamiento de contraseñas.
- Eliminar archivos infectados: elimine los archivos infectados y actualice el software de seguridad para prevenir futuras infecciones.
- Concienciar al personal: avisar al personal para que este atento a cualquier mensaje o llamada extraños.
- Informar a las autoridades: si hay sospecha de delito o pérdida de información, es importante informar a las autoridades relevantes, como la policía o el departamento de seguridad nacional.
- Usar herramientas: utilice herramientas de análisis de correo electrónico y otros sistemas para identificar cualquier amenaza potencial. Estas herramientas pueden identificar virus, malware o intentos de phishing.
- Actualizar políticas y procedimientos: utilice el incidente como una oportunidad para actualizar las políticas y procedimientos de seguridad de la información de su organización, como por ejemplo, incluir políticas más estrictas para la creación y el almacenamiento de contraseñas y actualización del software de seguridad.

Documentación.

La documentación es la parte más importante ya que nos servirá para tener claro cada paso que se ha realizado y las consecuencias que ha tenido, esta deberá de ser detallada y precisa para ayudarnos a prevenir futuros incidentes, además de servir como guía para un futuro.

Para realizar dicho informe de manera adecuada podremos seguir los siguientes consejos:

- Registrar todos los detalles del incidente: incluyendo la fecha y hora, las personas involucradas, la descripción del incidente, las medidas tomadas y los resultados.
- Documentar las lecciones aprendidas: esto te puede ayudar a mejorar las políticas y procedimientos de seguridad de la información de su organización.## Playbook: Phishing

Investigar, remediar (contener, erradicar), y comunicar en paralelo!

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

Investigar

1. **Ámbito del ataque** Normalmente se le notificará que se está produciendo un posible ataque de phishing, ya sea por parte de un usuario, cliente o socio.

    - Determinar el **número total de usuarios afectados**.
    - Comprender **las acciones de los usuarios** en la respuesta al phishing de un correo electrónico (*e.j.*, ¿Descargarón el archivo adjunto?, ¿Visitarón el sitio suplantado?, ¿O, dieron alguna información personal o comercial como credenciales?)
    - Encontrar la actividad potencialmente relacionada. Comprueba:
        - Redes Sociales
        - Cualquier correo electrónico sospechoso posible.
        - Correos electrónicos con enlaces a URL's externas y desconocidas.
        - Correos electrónicos de no-retorno o no-entregables.
        - Cualquier tipo de notificación de actividad sospechosa.

2. **Analizar el mensaje** utilizando un dispositivo seguro (es decir, **no** abrir los mensajes en un dispositivo con acceso a datos sensibles o credenciales ya que el mensaje puede contener malware), determinar:

    - Quién ha recibido el mensaje
    - Quién era el objetivo del mensaje (puede ser diferente de los destinatarios a los que iba realmente dirigido el mensaje)
    - Dirección de correo electrónico del remitente
    - línea de asunto
    - Cuerpo del mensaje
    - Adjuntos (**no abra los archivos adjuntos** salvo según los procedimientos establecidos)
    - Enlaces, dominios, y nombres de host (**no siga los enlaces**, excepto según los procedimientos establecidos)
    - Metadatos del correo electrónico inluidas las cabeceras de los mensajes (véase más adelante)
        - Información del remitente en el campo "de" y en la cabecera del usuario autenticado-X
        - Todas las direcciones IP del cliente y del servidor de correo
    - Anotar las "peculiaridades" o características sospechosas

3. **Analizar los enlaces y los archivos adjuntos**

    - Utilizar la recopilación pasiva como nslookup y whois para encontrar direcciones IP e información de registro
    - Encontrar dominios relacionados utilizando OSINT (*e.j.*, reverse whois) en direcciones de correo electrónico y otros datos de registro.
    - Enviar enlaces, archivos adjuntos y/o hashes a VirusTotal
    - Enviar enlaces, adjuntos y/o hashes a un sandbox de malware como Cuckoo, Hybrid Analysis, Joe Sandbox, o VMray.

4. Categorice el tipo de ataque.
5. **Determine la gravedad.** Considerar:
    - Si la seguridad pública o personal está en riesgo
    - Si los datos personales (u otros datos sensibles) están en riesgo
    - Si hay pruebas de quién está detrás del ataque
    - Número de activos afectados
    - El impacto preliminar en el negocio
    - Si los servicios se ven afectados
    - Si se pueden controlar/registrar los sistemas críticos

Remediar

- **Planificar eventos de remediación** en los que estos pasos se pongan en marcha juntos (o de forma coordinada), con los equipos adecuados listos para responder a cualquier interrupción.
- **Considere el momento y las compensaciones** de las acciones de remediación: su respuesta tiene consecuencias.

Contener

- Contener las cuentas afectadas
    - Cambiar las credenciales de acceso
    - Reducir el acceso a los servicios, sistemas o datos críticos hasta que se complete la investigación
    - Reforzar la autenticación multifactor (MFA)
- Bloquear la actividad en función de los indicadores de compromiso descubiertos, *e.j.*:
    - Bloquear dominios maliciosos mediante DNS, cortafuegos o proxies
    - Bloquear los mensajes con remitentes, cuerpos de mensajes, asuntos, enlaces, archivos adjuntos similares, etc., utilizando la puerta de enlace predeterminada o el servicio de correo electrónico.
- Implementar la retención forense o conservar copias forenses de los mensajes
- Purgar los mensajes relacionados de las bandejas de entrada de otros usuarios, o hacerlos inaccesibles de otro modo.
- Contener el compromiso más amplio de acuerdo con el plan general de IR
- Considerar medidas de contención de los dispositivos móviles, como el borrado a través de la gestión de dispositivos móviles (MDM). Equilibrio con el impacto de la investigación/forense.
- Aumentar el "nivel de alerta" de la detección, con una mayor supervisión, en particular de las cuentas, dominios o direcciones IP relacionadas.
- Considerar la posibilidad de contar con asistencia externa en materia de seguridad para apoyar la investigación y la correción.
- Confirmar las actualizaciones de software y antimalware pertinenestes en los activos.

Comunicar

1. Elevar el incidente y comunicarlo a la dirección según el procedimiento
2. Documente el incidente según el procedimiento (y informe)
3. Comunicarse con los asesores jurídicos internos y externos según el procedimiento, incluyendo discusiones sobre el cumplimiento, la exposición al riesgo, la responsabilidad, el contacto con las fuerzas del orden, *etc.*
4. Comnunicación con los usuarios (interna)
    1. Comunicar las actualizaciones de la respuesta a incidentes según el procedimiento
    2. Comunicar el impacto del incidente **y** las acciones de respuesta al mismo (e.j., contención: "¿Por qué está caído el archivo compartido?")
    3. Comunicar los requisitos: "¿Qué deben hacer y no hacer los usuarios?"
5. Comunicar a los clientes
    1. Centrarse especialmente en aquellos cuyos datos se vieron afectados
    2. Genere las notificaciones requeridas en base a las regulaciones aplicables (particularmente aquellas que puedan considerar el phishing como una violación de datos o que requieren notificaciones de otro tipo)
6. Contactar con el/los proveedor/es de seguros
    1. Discutir qué recursos pueden poner a disposición, qué herramientas y proveedores apoyan y pagarán, *etc.*
    2. Cumplir con los requisitos de presentación de informes y reclamaciones para proteger la elegibilidad.
7. Considere la posibilidad de notificar e implicar a las fuerzas del orden
    1. Aplicación de la ley local
    2. Aplicación de la ley a nivel estatal o regional
    3. Fuerzas de seguridad nacionales o europeas
8. Comuníquese con los proveedores de seguridad y de TI
    1. Notifique y colabore con proveedores gestionados para el procedimiento
    2. Notifique y colabore con consultores de respuesta ante incidentes para el procedimiento

Recuperación

1. Poner en marcha un plan de continuidad de negocio/recuperación de desastres si el compromiso implica interrupciones de negocio: *e.j.*, considerar la migración a ubicaciones operativas alternativas, clústers de conmutación por error, sistemas de copias de seguridad.
2. Reforzar los programas de formación sobre los ataques de phishing sospechosos. Los principales indicadores de sospecha pueden ser:
    - Errores ortográficos en el mensaje o en el asunto
    - Nombres de remitentes que parezcan de telélefono, incluida la falta de coincidencia entre el nombre y la dirección de correo electrónico.
    - Direcciones de correo electrónico personales para asuntos oficiales

(e.j., correos electrónicos de gmail o yahoo de colegas de trabajo)
- Líneas de asunto marcadas con "[EXTERNO]" en correos electrónicos que parecen internos.
- enlaces maliciosos o sospechosos
- Recibir un correo electrónico o un archivo adjunto que no se esperaba, pero que proviene de alguien conocido (contactar con el remitente antes de abrirlo).
- Informar de actividades sospechosas al departamento de TI o de seguridad.

3. Asegúrate de que el personal de TI y de seguridad está al día de las técnicas de phishing más recientes.
4. Determine si ha fallado algún control al ser victima de un ataque y rectifíquelo. He aquí una buena fuente a tener en cuenta tras un ataque de phishing.

Recursos

Referencia: Acciones del usuario ante la sospecha de un ataque de phishing

1. Mantenga la calma y respire profundamente.
2. Haz fotos de tu pantalla con tu smartphone mostrando las cosas que has notado: el mensaje de phishing, el enlace si lo has abierto, la información del remitente.
3. Toma notas sobre el problema o los problemas utilizando la aplicación de notas de voz de tu smartphone o con papel y boli. Todo por poco que sea, 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.*)
    7. ¿Qué cuenta utilizas?
    8. ¿A qué datos suele acceder?
    9. ¿Con quién más te has puesto en contacto sobre este incidente y qué les has dicho?
4. Ponte en contacto con el servicio de ayuda utlizando la línea directa de phishing o la barra de herramientas de informe de phishing y sé lo más servicial posible.
5. Ten paciencia: La respuesta puede ser perturbardora, pero estas protegiendo a tu equipo y a la organización! **Gracias.**

Referencia: Acciones del servicio de ayuda ante un presunto ataque phishing

1. Mantenga la calma y respire profundamente.
2. Abra un ticket para documentar el incidente, según el procedimiento.
3. Pídale al usuario que tome fotos de su pantalla usando su smartphone mostrando las cosas que notó: el mensaje de phishing, el enlace si lo abrió, la información del remitente, *etc.* Si es algo que notó 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 boli. Si se trata de un informe de usurio, haz preguntas detalladas, incluyendo:
    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. ¿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 te has puesto en contacto sobre este incidente y qué les has dicho?
5. Haz las preguntas de seguimiento que sean necesarias. **Usted es de respuesta ante Incidentes, Contamos contigo.**
6. Obtenga información de contacto detallada del usuario (domicilio, oficina, móvil), si procede.
7. Registra 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 prepárase para participar en la respuesta según las indicaciones: investigación, remediación comunicación y recuperación.

Información adicional

1. Recurso Ataque Anti-Phishing
2. Métodos de Identificación de Ataques Phishing
3. Ejemplos Correos electrónicos de Phishing
4. Mejores prácticas Anti-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.

Investigación

1. **Determinar el tipo** de ransomware (*es decir,* ¿cuál es la familia, la variante o el tipo?)[1]
    1. Encuentre cualquier mensaje relacionado. Compruebe:
        - las interfaces gráficas de usuario (GUI) del propio malware
        - archivos de texto o html, que a veces se abren automáticamente tras el cifrado
        - archivos de imange, a menudo, como fondos de pantalla del sistema infectado
        - correos electrónicos de contacto en extensiones de archivo encriptadas
        - ventanas emergentes después de intentar abrir un archivo encriptado
        - mensajes de voz
    2. Analice los mensajes en busca de pistas sobre el tipo de ransomware:
        - nombre del ransomware
        - lenguaje, estructura, frases, material gráfico
        - correo electrónico de contacto
        - formato de la identificación del usuario
        - especificaciones de la demanda de rescate (*p.ej.*, moneda digital, tarjetas de regalo)
        - dirección de pago en caso de moneda digital
        - chat de soporte o página de soporte
    3. Analice los archivos afectados y/o nuevos. Compruebe:
        - el esquema de cambio de nombre de los archivos encriptados, incluyendo la extensión (*p.ej.*, `.cry`, `.cry`, `.locked`) y el nombre base
        - corrupción de archivos frente a encriptación
        - Tipos de archivos y ubicaciones objetivo
        - usuario/grupo propietario de los archivos afectados
        - Icono de los archivos encriptados
        - marcadores de archivos
        - existencia de listados de archivos, archivos clave u otros archivos de datos
    4. Analice los tipos de software o sistemas afectados. Algunas variantes de ransomware sólo afectan a determinadas herramientas (*p.ej.*,

databases) or platforms (*e.g.*, NAS products)
5. Subir los indicadores a servicios de categorización automatizados como Crypto Sheriff, ID Ransomware, o similar.

2. **Determinar el alcance:**
   1. ¿Qué sistemas están afectados?
      - Busque indicadores de compromiso (IOC), como archivos/hashes, procesos, conexiones de red, etc. Utilice endpoint protection/EDR, endpoint telemetry, system logs, etc.
      - Comprobar la infección de sistemas similares (_por ejemplo, usuarios, grupos, datos, herramientas, departamento, configuración, estado de los parches): comprobar IAM tools, permissions management tools, directory services, *etc.*
      - Find external command and control (C2), if present, and find other systems connecting to it: check firewall or IDS logs, system logs/EDR, DNS logs, netflow or router logs, *etc.*
   2. ¿Qué datos están afectados? (*e.g.*, tipos de archivo, departamento o grupo, software afectado).
      - Buscar cambios anómalos en los metadatos de los archivos, como cambios masivos en las horas de creación o modificación. Comprobar herramientas de búsqueda de metadatos de archivos
      - Buscar cambios en archivos de datos normalmente estables o críticos. Comprobar las herramientas de supervisión de la integridad de los archivos
3. **Evaluar el impacto** para priorizar y motivar los recursos
   1. Evaluar el impacto funcional: impacto en la empresa o en la misión.
      - ¿Cuánto dinero se pierde o está en riesgo?
      - ¿Cuántas (y cuáles) misiones se degradan o están en riesgo?
   2. Evaluar el impacto en la información: impacto en la confidencialidad, integridad y disponibilidad de los datos.
      - ¿Qué importancia tienen los datos para la empresa/misión?
      - ¿Cuán sensibles son los datos? (*p.ej.*, secretos comerciales)
      - ¿Cuál es la situación reglamentaria de los datos (*p.ej.*, PII, PHI)?
4. **Encuentra el vector de infección.** Comprueba las tácticas capturadas en la Initial Access tactic of MITRE ATT&CK[4]. Los datos más comunes y las fuentes de datos son:
   - archivo adjunto de correo electrónico: comprobar email logs, email security appliances and services, e-discovery tools, *etc.*
   - insecure remote desktop protocol (RDP): check vulnerability scanning results, firewall configurations, *etc.*
   - auto-propagación (worm or virus) (check host telemetry/EDR, system logs, forensic analysis, *etc.*)

Remediar

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

cualquier interrupción. **Considere el momento y las compensaciones** de las acciones de reparación: su respuesta tiene consecuencias.

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

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

Erradicar

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

Comunicar

> **No recomendamos pagar el rescate:** no garantiza la solución del problema. Puede salir mal (*e.*, los errores podrían hacer que los datos sean irrecuperables incluso con la clave). Además, pagar demuestra que el ransomware funciona y podría aumentar los ataques contra ti o contra otros grupos.[2, paraphrased]

1. Poner en marcha un plan de continuidad de la actividad/recuperación de desastres: Por ejemplo, considerar la migración a ubicaciones operativas alternativas, sitios de conmutación por error, sistemas de respaldo.
2. Recuperar los datos de las copias de seguridad ya limpias en sistemas ya limpios, parcheados y monitorizados (post-erradicación), de acuerdo con nuestra well-tested backup strategy. *Comprobar las copias de seguridad en busca de indicadores de peligro
    - Considerar la recuperación parcial y las pruebas de integridad de las copias de seguridad
3. ¡Encuentre y pruebe desencriptadores conocidos para la(s) variante(s) descubierta(s) utilizando recursos como el proyecto No More Ransom! Project's Decryption Tools page.
4. Considerar el pago del rescate por los activos/datos críticos irrecuperables, de acuerdo con la política.
    - Considerar las ramificaciones con las partes interesadas apropiadas
    - Comprender las implicaciones financieras y el presupuesto
    - Comprender las implicaciones legales, reglamentarias y de seguros
    - Comprender los mecanismos (por ejemplo, tecnologías, plataformas, proveedores intermedios/intermediarios)

Recursos

Referencia: Acciones de los usuarios ante la sospecha de ransomware

1. Mantenga la calma y respire profundamente.
2. Desconecte su sistema de la red.
3. 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.*.
4. 2. 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:
   3. ¿Qué has notado?
   4. ¿Por qué pensaste que era un problema?
   5. ¿Qué estabas haciendo en el momento en que lo detectaste?
   6. ¿Cuándo se produjo por primera vez, y con qué frecuencia desde entonces?

7. ¿Dónde estaba cuando ocurrió y en qué red? (oficina/casa/tienda, con cable/inalámbrica, con/sin VPN, *etc.*)
8. ¿Qué sistemas está utilizando? (sistema operativo, nombre de host, *etc.*)
9. ¿Qué cuenta utilizas?
10. ¿A qué datos suele acceder?
11. ¿Con quién más se ha puesto en contacto en relación con este incidente y qué le ha dicho?

5. Contacta al help desk y ser lo más útil posible

6. Tenga paciencia: la respuesta puede ser perturbadora, pero está protegiendo a su equipo y a la organización. **Gracias.**

Referencia: Acciones del servicio de asistencia técnica ante la sospecha de ransomware

1. Mantenga la calma y respire profundamente.

2. Abra un ticket para documentar el incidente, según el procedimiento.

3. 2. 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. 2. ¿De qué sistemas se trata? (sistema operativo, nombre de host, *etc.*)

    7. 2. ¿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

Información adicional

1. "Ransomware Identification for the Judicious Analyst", Hahn (12 Jun 2019)
2. No More Ransom! Project, including their Crypto Sheriff service and their Q&A
3. ID Ransomware service
4. MITRE ATT&CK Matrix, including the Initial Access and Impact tactics

Playbook: Compromiso de la cadena de suministro

Investigar, remediar (contener, erradicar) y comunicar en paralelo!.

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.

Investigar

`TODO: Ampliar los pasos de la investigación, incluyendo las preguntas y estrategias clave, para el compromiso de la cadena de suministro.`

1. TODO

Remediar

- **Planificar eventos de remediación** en los que estos pasos se pongan en marcha juntos (o de forma coordinada), con los equipos adecuados listos para responder a cualquier interrupción.
- **Considere el momento y las compensaciones** de las acciones de remediación: su respuesta tiene consecuencias.

Contención `TODO: Personalizar los pasos de contención, tácticos y estratégicos, para el compromiso de la cadena de suministro.`

`TODO: Especifique las herramientas y los procedimientos para cada paso, a continuación.`

*TODO

`TODO: Considerar la posibilidad de automatizar las medidas de contención mediante herramientas de orquestación.`

Erradicar `TODO: Personalizar los pasos de erradicación, tácticos y estratégicos, para el compromiso de la cadena de suministro.`

`TODO: Especificar las herramientas y los procedimientos para cada paso, a continuación.`

- TODO

Referencia: Recursos de remediación `TODO: Especificar los recursos financieros, de personal y logísticos para llevar a cabo la remediación.`

Comunicar

`TODO: Personalizar los pasos de la comunicación para el compromiso de la cadena de suministro`

`TODO: Especifique las herramientas y los procedimientos (incluyendo quién debe participar) para cada paso, a continuación, o consulte el plan general.`

Además de los pasos y orientaciones generales del plan de respuesta a incidentes:

1. TODO

Recuperación

`TODO: Personalizar los pasos de recuperación para el compromiso de la cadena de suministro.`

`TODO: Especifique las herramientas y procedimientos para cada paso, a continuación.`

Además de los pasos y orientaciones generales del plan de respuesta a incidentes:

1. TODO

Recursos

Información adicional

1. “Title”, Author Last Name (Date)

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.

`TODO: Personalizar los roles, las descripciones, las funciones y la formación, si es necesario.`

Estructura de los roles

- Equipo de Mando
  - Incident Commander
  - Incident Commander-Adjunto
  - 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. Para más información, lea cómo gestionamos los Incidentes Complejos.

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 Comandante del incidente 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.
- Los primeros intervinientes (las personas que actúan como primeros intervinientes de un equipo/servicio) son las personas de mayor rango de ese servicio.
- Las decisiones serán tomadas por el IC tras considerar la información presentada. Una vez tomada la decisión, es definitiva.

- El IC puede tomar decisiones más arriesgadas que las que normalmente se considerarían en tiempos de paz.
- El IC 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 IC puede elegir la opción del desacuerdo a pesar del voto de la mayoría. Aunque no esté de acuerdo, la decisión del IC es definitiva. Durante la convocatoria no es el momento de discutir con ellos.
- El IC 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 IC te pida que abandones la llamada, o incluso que te eche a la fuerza de una llamada. Esto queda a discreción del IC 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 Incident Commander.

Deberes

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 Incident Commander (IC) en la llamada.
- Respetar las limitaciones de tiempo dadas por el Incident Commander.
- 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 Incident Commander El Incident Commander (IC) es el líder del proceso de respuesta al incidente.

- Siga las instrucciones del Incident Commander.
- No realice ninguna acción a menos que el Incident Commander 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: Incident Commander

Descripcion

El Incident Commander(IC) actua como la única fuente de lo que realmente está ocurriendo y va a ocurrir durante un incidente grave. El IC 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 Incident commander las decisivas.

Tu trabajo como Incident commander 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 Incident Commanders.
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 Incident Commander 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 Incident Commander utiliza métodos y lenguajes adicionales:

- Siempre anuncie cuando se una a la llamada si es el IC 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 Incident Commander 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 Incident Commander actual sin participar activamente, manteniendo sus preguntas hasta el final.
- Tomar la iniciativa de un Incident Commander. Responda a incidentes con el IC actual allí para hacerse cargo si es necesario.
- *OPCIONAL:* facilitar las prácticas
- *OPCIONAL:* recurre a Incident Responders as Facilitators (and Therapists) y al PagerDuty Incident Commander training para mas ideas y discussiones.

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

- 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 Incident Commander no requieren un conocimiento técnico profundo de nuestros sistemas. Su trabajo como Incident Commander es coordinar la respuesta, no realizar cambios técnicos. No crea que no puede ser un Incident Commander solo porque no está en el departamento de ingeniería.

Graduación Al finalizar el entrenamiento, agréguese a la lista de Incident Commander.

Rol: adjunto del Incident Commander (adjunto)

Descripción

Un adjunto del Incident Commander (adjunto) es un papel de apoyo directo al Incident Commander (IC). El adjunto permite que el IC 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 IC y lo mantiene centrado en el incidente. Como adjunto, se espera que asuma el mando del IC si éste lo solicita.

Funciones

1. 1. Plantear al Incident Commander cuestiones que, de otro modo, no se abordarían (vigilar los temporizadores que se han puesto en marcha, retomar los elementos que se han perdido de una lista, etc.).
2. 1. Ser un Incident Commander "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 IC.
3. 1. Gestionar la llamada del incidente y estar preparado para retirar a las personas de la llamada si así lo indica el Incident Commander.
4. Supervisar el estado del incidente y notificar al IC si el nivel de gravedad del incidente aumenta.
5. Supervise los temporizadores:
   - controlar el tiempo que ha durado el incidente
   - Notificar al IC cada X minutos para que pueda tomar medidas (por ejemplo, "IC, el incidente está ahora en la marca de 10 minutos").
6. Supervisar los plazos de las tareas (*p.ej.*, "IC, 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.

Requisitos previos

- Estar entrenado como Incident Commander.

Traducción realizada con la versión gratuita del traductor www.DeepL.com/Translator

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 IC los proporcione
   - Cualquier llamada clave durante la llamada o en la revisión final
3. Actualice el chat indicando quién es el IC, quién es el adjunto y que usted es el escribiente (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 escribiente.

- El resultado de cualquier decisión de la votación. ### Cualquier elemento de seguimiento que se llame "Deberíamos hacer esto..", "¿Por qué no se hizo esto?", etc.

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 escribiente durante un incidente, y son elegidos por el Incident Commander al inicio de la llamada.
- Normalmente, el ayudante actuará como escribiente.

Proceso de formación

- Lea el plan de respuesta a incidentes, incluyendo todos los roles y libros de jugadas.
- *OPCIONAL:* Paralizar las acciones de un escriba durante un incidente o ejercicio, y buscar la opinión del escriba real y del Incident Commander.

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 Incident Commander 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 Incident Commander, asegúrese de no estar de guardia con su equipo al mismo tiempo que está de guardia como Incident Commander.

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 Incident Commander 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 IC 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 Incident Commander y otras partes interesadas.

6. Según proceda, mantener a los clientes informados durante un incidente.
7. Actuar como voz de nuestros clientes ante el Incident Commander, ya que esto es útil para la toma de decisiones del IC.
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 IC antes de continuar.

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.

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.
- *OPCIONAL:* Formación en atención al cliente.

- *OPCIONAL:* Comunicación corporativa o formación en marketing.

Realizar una revisión posterior a la acción (Conduct an After Action Review, AAR)

1. Programe una reunión de revisión posterior a la acción (AAR) dentro de 5 días laborales e invite a los asistentes que figuran en ir.powerpuff.org/aar/asistentes. Incluya siempre a los siguientes:
   - El Incident Commander.
   - Los propietarios de los servicios implicados en el incidente.
   - Ingeniero(s)/responsable(s) clave(s) implicado(s) en el incidente.
2. Designe a un propietario del AAR que investigue el incidente antes de la reunión para prepararlo, estudiando el proceso del incidente en sí, incluyendo la revisión de notas e informes.

Realización de la reunión AAR

Documente las respuestas a las siguientes preguntas clave:

1. **¿Qué ocurrió?** Cree una línea de tiempo, apoyada con datos u otros artefactos. **Evitar las culpas. Busca los hechos.**
2. **¿Qué se suponía que iba a ocurrir?**
   - Detallar las desviaciones del proceso, el procedimiento o las mejores prácticas, incluidas las evaluaciones de los SME.
   - Identifique las formas en que el incidente podría haberse detectado antes o haberse respondido con mayor eficacia.
3. **¿Cuáles fueron las causas fundamentales?** Encuentre la raíz de lo que ocurrió y de lo que debería haber ocurrido.
4. **¿Cómo podemos mejorar?** Capture los elementos de acción con asignados y fechas de vencimiento. Considerar:
   - Detener: ¿Qué debemos dejar de hacer?
   - Empezar: ¿Qué deberíamos empezar a hacer?
   - Continuar: ¿Qué debemos seguir haciendo?

Comunicar el estado y los resultados del AAR

El propietario del informe, en coordinación con el enlace interno, comunicará el estado del informe (véase más abajo).

Descripciones de estado

Estado	Descripción
Borrador	La investigación de la AAR sigue en curso

Estado	Descripción
En revisión	La investigación AAR se ha completado, y está lista para ser revisada durante la reunión AAR.
Revisado	La reunión de AAR ha terminado y el contenido ha sido revisado y acordado. Si hay "Mensajes externos" adicionales, el equipo de comunicación tomará medidas para prepararlos.
Cerrado	No es necesario realizar más acciones en el AAR (los problemas pendientes se rastrean en los tickets).Si no hay "Mensajes Externos", pase directamente a esto una vez que la reunión haya terminado.Si hay "Mensajes Externos" adicionales, el equipo de comunicaciones actualizará el AAR Cerrado una vez enviado.

Comunicar internamente los resultados del AAR y finalizar la documentación del AAR.

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

Esta plantilla esta proporcionado bajo la licencia de apache, version 2.0. puedes ver el codigo fuente en https://github.com/counteractive.

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.