Incident Response Plan for Anpipada SL

Author: Grupo 2, carlospablodavid@anpipada.es

Revision 1, Released 27/03/2024

Abstract

This incident response plan is based on the concise, directive, specific, flexible, and free plan available on Counteractive Security's Github and discussed at www.counteractive.net

It was last reviewed on 27/03/2024. It was last tested on 27/03/2024.

Contents

Plan de respuesta a incidentes para ANPIPADA S.L.

Autor: Grupo 2, carlospablodavid@anpipada.es

Revisión 1, Publicado 27/03/2024

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

Fue revisado por última vez el 27/03/2024. Fue probado por última vez en 27/03/2024.

Contexto de este plan

Posterior a la creación de este plan de respuesta se han realizado varios pasos que quedan detallados a continuación:

Identificación de activos

Tras obtener una breve descripción de la empresa se realizón un inventariado de activos con los que trabajaremos más adelante, quedando una hoja de cálculo como la siguiente:

INVENTARIO DE ACTIVOS						
Identificador	**Nombre**	**Descripción**	**Responsable**	**Tipo**	**Ubicación**	**Crítico**
ID_0001	Servidor 01 (Contabilidad)	Servidor de contabilidad.	Director Financiero.	Servidor (físico)	Sala de CPD1 Sede 1	Sí
ID_0002	*Servidor de correo electrónico 01*	Servidor de correo interno	Administradores de sistemas	Servidor (físico)	Sala de CPD1 Sede 1	No
ID_0003	*Servidor de correo electrónico 02*	Servidor de correo interno	Administradores de sistemas	Servidor (físico)	Sala de CPD1 Sede 2	No
ID_0003	Servidor 02 (Web)	Servidor para la página web corporativa.	Dpto. Informática.	Servidor (Externalizado)	CPD Externo	Sí
ID_0004-0105	PC	Sistemas dedicados a los trabajadores	Administradores de sistemas	Dispositivo(Físico)	Sede 1 y 2	No
ID_0106-0124	Dispositivos impresoras	Sistemas de impresión	Administradores de sistemas	Dispositivo(Físico)	Sede 1	No
ID_0125-0145	Teléfonos	Dispositivos móviles de uso empresarial	Departamento de TI	Dispositivo(Físico)	Trabajadores	No
ID_0146-0150	Ordenadores portátiles	Laptops personales	Departamento de TI	Dispositivo(Físico)	Trabajadores	No
ID_0150-0160	Tabletas	*Tabletas iPad.*	Departamento de TI	Dispositivo(Físico)	Trabajadores	No
ID_0161-0180	*Sistemas de almacenamiento*	*USB, discos duros y SSD*	Departamento de seguridad	Dispositivo de almacenamiento(Físico)	Dpto. de seguridad	Sí
ID_0181	*Router Wifi (Corporativo) 01*	*Router que permite acceso a internet en las sedes.*	Administradores de sistemas	Dispositivo de red	Sede 1	Sí
ID_0182	*Router Wifi (Corporativo) 02*	*Router que permite acceso a internet en las sedes.*	Administradores de sistemas	Dispositivo de red	Sede 1	Sí
ID_0183	*Router Wifi (Corporativo) 03*	*Router que permite acceso a internet en las sedes.*	Administradores de sistemas	Dispositivo de red	Sede 2	Sí

Figure 1: Resultados 1

Nivel de madurez y proyectos

También hemos realizado una evaluación de madurez de la empresa y obtuvimos los siguientes resultados:

Medida	% de madurez	% de madurez esperado	Descripción
Copias de seguridad	60 %	80 %	Gestionadas por los empleados TIC, que se almacenan en la sede principal.Documentado con un procedimiento básico que permite repetir el procedimiento.
Antivirus	60 %	80 %	Gestionado por una subcontrata que se encarga que este actualizado, con un procedimiento documentado pero que no ha sido aprobado por la dirección.
Cumplimiento de la RGPD	80 %	80 %	A través de la contratación de una consultoría. Bien documentado tras el trabajo de la consultoría, aprobado por la dirección y formal.
Firewall	40 %	80 %	Establece una zona segura y otra publica en la red de la empresa. Subred segmentada por departamentos. La información solo la conoce el administrador de red.
Políticas de seguridad	0 %	80 %	No existen políticas de seguridad por escrito
Pagina web	0 %	80 %	Externalizada y no tiene control sobre su estado en cuanto a securización.

Figure 2: Resultados 1

Entre las tareas propuestas para aumentar el nivel de madurez tenemos:

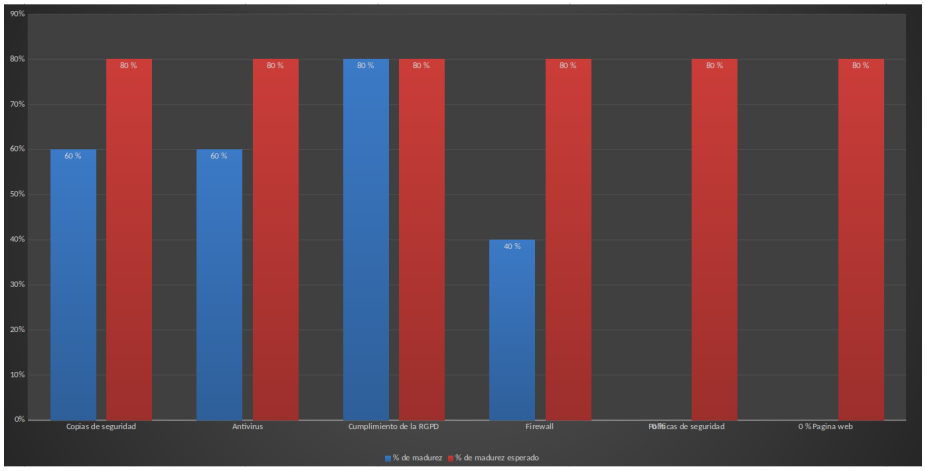

Figure 3: Resultados 2

1. Análisis de riesgo y amenazas:

- Responsable: Departamento de seguridad
- Tarea: Identificar y evaluar los riesgos y amenazas que puedan afectar a la organización.

2. Definicion de politicas de seguridad:

- Responsable: Director de seguridad
- Tarea: Establecer políticas y directrices de seguridad que la organización debe seguir.

3. Elaboración de procedimientos y normativas:

- Responsable: Departamento de seguridad
- Tarea: Desarrollar procedimientos y normativas específicas para implementar las políticas de seguridad.

4. Gestión de accesos y autorizaciones:

- Responsable: Departamento de seguridad
- Tarea: Administrar los permisos de acceso a sistemas, instalaciones y datos de la organización.

5. Formación y concienciación de en seguridad:

- Responsable: Departamento de recursos humanos
- Tarea: Hacer saber a los empleados sobre la concienciación en seguridad

6. Seguridad física:

- Responsable: Departamento de seguridad

- Tarea:Garantizar la protección de las instalaciones, activos y personal de forma activa y pasiva.

7. Seguridad de la información:

- Responsable: Equipo de TI
- Tarea: Proteger la integridad, confidencialidad y disponibilidad de los datos y sistemas de la organización.

8. Gestión de incidentes de seguridad:

- Responsable: Equipo de respuesta a incidentes de seguridad
- Tarea:Investigar, gestionar y mitigar incidentes de seguridad como brechas de información.

9. Evaluación y auditoría de seguridad:

- Responsable: Auditores internos o externos
- Tarea: Evaluar y auditar de forma regular las medidas de seguridad implementadas en la empresa.

10. Actualización y mejora continua:

- Responsable: Departamento de seguridad
- Tarea: Revisar y actualizar regularmente el plan de seguridad para adaptarse a cambios en amenazas.

11. Monitoreo de la seguridad y de la página web:

- Responsable: Equipo de operaciones de seguridad
- Tarea: Establecer sistemas de monitoreo continuo para detectar y responder a las amenazas de la página web.Es necesario tanto la realización de una documentación como la aprobación de dicho trámite.

12. Configuración y mantenimiento del firewall:

- Responsable: Administradores de sistemas
- Tarea:Configurar y mantener el firewall para controlar el tráfico de red y prevenir o detectar intrusiones no autorizadas. Es necesario tanto la realización de una documentación como la aprobación de dicho trámite.

13. Implementación y actualización del software antivirus:

- Responsable: Departamento de TI o personal de seguridad
- Tarea:Garantizar la instalación y actualización regular de software antivirus en los sistemas para detectar y eliminar malware. Es necesaria la aprobación del sistema.

14. Ejecucion y supervision de copias de seguridad:

- Responsable: Administradores de sistemas o personal de seguridad.
- Tarea:Garantizar que se realicen copias de seguridad periódicas y que se supervisen para asegurarse de que sean efectivas. Es necesaria la aprobación del sistema.

Posibles amenazas

En el apartado de análisis ed amenzas que usaremos para posteriormente calcular riesgos hemos tenido en cuenta las usadas por INCIBE.

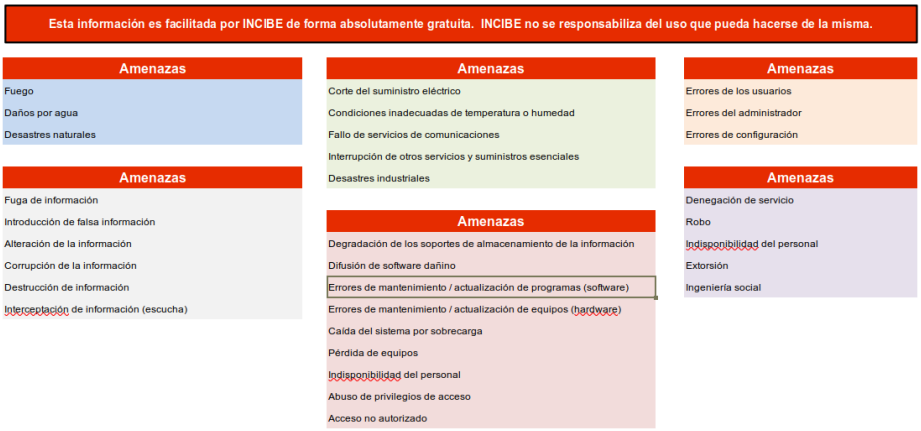

Figure 4: Calculo risgo

Cálculo del riesgo

Teniendo un inventario de activos y las posibles amenazas a las que nos enfrentamos tenemos una hoja en la que existe el calculo del risgo(impacto*probabilidad) de todas las posibilidades consideradas.

Taxonomía de incidentes

Se realizó una taxonomía de varios incidentes posibles que podrían afectar a nuestra empresa objetivo, siendo estos:

1. **Escaneo de Redes (Scanning)**
   - **Descripción:** Identificación de dispositivos en una red, utilizado tanto para mantenimiento como para ataques.
   - **Funcionamiento:** Atacantes utilizan herramientas y protocolos comunes de escaneo de red.
   - **Identificación:** Detección mediante monitoreo de umbrales y modelos probabilísticos.
   - **Protección:** Uso de sistemas de detección de intrusiones y firewalls.
   - **Caso Real:** Violación de la confidencialidad de usuarios del software MOVEit por el grupo “Cl0p”.
2. **Ingeniería Social**
   - **Descripción:** Manipulación de personas para obtener información confidencial.

ANÁLISIS DE RIESGOS				
Activo	Amenaza	Probabilidad	Impacto	Riesgo
ordenador(es)	Fuga de información	Medio (2)	Medio (2)	4
ordenador(es)	Introducción de falsa información	Alto (3)	Medio (2)	6
ordenador(es)	Alteración de la información	Bajo (1)	Medio (2)	2
ordenador(es)	Corrupción de la información	Medio (2)	Medio (2)	4
ordenador(es)	Destrucción de información	Bajo (1)	Medio (2)	2
ordenador(es)	Interceptación de información (escucha)	Bajo (1)	Medio (2)	2
ordenador(es)	Corte del suministro eléctrico	Bajo (1)	Alto (3)	3
ordenador(es)	Condiciones inadecuadas de temperatura o humedad	Bajo (1)	Bajo (1)	1
ordenador(es)	Fallo de servicios de comunicaciones	Bajo (1)	Medio (2)	2
ordenador(es)	Interrupción de otros servicios y suministros esenciales	Bajo (1)	Medio (2)	2
ordenador(es)	Desastres industriales	Bajo (1)	Alto (3)	3
ordenador(es)	Degradación de los soportes de almacenamiento de la información	Bajo (1)	Alto (3)	3
ordenador(es)	Difusión de software dañino	Bajo (1)	Alto (3)	3
ordenador(es)	Errores de mantenimiento / actualización de programas (software)	Bajo (1)	Medio (2)	2
ordenador(es)	Errores de mantenimiento / actualización de equipos (hardware)	Bajo (1)	Medio (2)	2
ordenador(es)	Caída del sistema por sobrecarga	Bajo (1)	Medio (2)	2
ordenador(es)	Pérdida de equipos	Bajo (1)	Alto (3)	3
ordenador(es)	Abuso de privilegios de acceso	Medio (2)	Alto (3)	6
ordenador(es)	Acceso no autorizado	Bajo (1)	Alto (3)	3
ordenador(es)	Errores de los usuarios	Medio (2)	Medio (2)	4
ordenador(es)	Errores del administrador	Bajo (1)	Alto (3)	3
ordenador(es)	Errores de configuración	Bajo (1)	Medio (2)	2
ordenador(es)	Denegación de servicio	Bajo (1)	Medio (2)	2
ordenador(es)	Robo	Bajo (1)	Alto (3)	3
móvil(es) principalmente para telefonía	Fuga de información	Bajo (1)	Medio (2)	2
móvil(es) principalmente para telefonía	Introducción de falsa información	Bajo (1)	Medio (2)	2
móvil(es) principalmente para telefonía	Alteración de la información	Bajo (1)	Alto (3)	3
móvil(es) principalmente para telefonía	Corrupción de la información	Bajo (1)	Medio (2)	2
móvil(es) principalmente para telefonía	Destrucción de información	Bajo (1)	Alto (3)	3
móvil(es) principalmente para telefonía	Interceptación de información (escucha)	Medio (2)	Medio (2)	4
móvil(es) principalmente para telefonía	Corte del suministro eléctrico	Bajo (1)	Medio (2)	2

Figure 5: Calculo risgo

- **Funcionamiento:** Engañar a las víctimas para realizar acciones comprometedoras.
- **Identificación:** Señales como solicitudes inusuales y análisis crítico de comunicaciones.
- **Protección:** Educación, verificación de fuentes y políticas de seguridad.
- **Caso Real:** Campaña de phishing afectando a usuarios de Office 365.

3. **Explotación de Vulnerabilidades Conocidas**
   - **Descripción:** Aprovechamiento de debilidades en sistemas informáticos.
   - **Funcionamiento:** Atacantes desarrollan herramientas para explotar vulnerabilidades.
   - **Identificación:** Uso de herramientas de diagnóstico y monitoreo de seguridad.
   - **Protección:** Mantenimiento actualizado del software.
   - **Caso Real:** Compromiso del videojuego CS2 mediante vulnerabilidades.
4. **Ataque Desconocido**
   - **Descripción:** Ataque con métodos no totalmente comprendidos por las soluciones de seguridad.
   - **Funcionamiento:** Diseñado para evitar la detección y robar datos.
   - **Identificación:** Monitoreo constante y análisis de comportamientos inusuales.
   - **Protección:** Mantenimiento actualizado, educación en ciberseguridad.
   - **Caso Real:** Inserción de virus en instalaciones de una planta nuclear.
5. **Intento de Acceso con Vulneración de Credenciales**
   - **Descripción:** Acceso a sistemas utilizando credenciales comprometidas.
   - **Funcionamiento:** Prueba de múltiples combinaciones de credenciales.
   - **Identificación:** Señales como fallos de inicio de sesión y alertas de seguridad.
   - **Protección:** Uso de contraseñas fuertes y autenticación de múltiples factores.
   - **Caso Real:** Acceso ilegal en la computadora de un antiguo trabajador de Ticketmaster.
6. **Compromiso de Cuenta con Privilegios**
   - **Descripción:** Acceso no autorizado a cuentas con derechos elevados.
   - **Funcionamiento:** Obtención de acceso a través de phishing o explotación de vulnerabilidades.
   - **Identificación:** Actividades inusuales en cuentas de alto nivel y alertas de seguridad.
   - **Protección:** Uso de contraseñas fuertes y monitoreo constante.
   - **Caso Real:** Compromiso de cuenta privilegiada de un empleado de

Cisco.

7. **Compromiso de Cuentas sin Privilegios**
   - **Descripción:** Acceso no autorizado a cuentas con permisos limitados.
   - **Funcionamiento:** Uso de fuerza bruta o explotación de vulnerabilidades.
   - **Identificación:** Monitoreo del comportamiento de cuentas de usuario.
   - **Protección:** Autenticación de múltiples factores y concienciación de usuarios.
   - **Caso Real:** Intrusión en sistemas Docker para minar criptomonedas.

Respuestas a las preguntas

1.a ¿Qué relacción existe entre el trabajo que has hecho con las matrices MITRE ATT&CK y RE&CT y el plan de respuesta que estás planteando? ¿De qué manera te ha ayudado el trabajo previo sobre las matrices a la hora de generar el plan? Deja evidencias del trabajo que has realizado sobre el navegador de las matrices, para obtener la información.

La relación entre estas y el plan de respuesta se basa en utilizar el conocimiento obtenido de estas matrices para diseñar estrategias de detección, respuesta y recuperación, etc. ante posibles amenazas. El trabajo previo con estas matrices ha sido fundamental para comprender los diferentes tipos de ataques, sus técnicas y procedimientos, lo que nos ha permitido identificar posibles puntos de vulnerabilidad en nuestro entorno y desarrollar respuestas adecuadas.

Para evidenciar el trabajo realizado, podemos proporcionar capturas de pantalla o registros de actividad del navegador mientras investigabamos y explorabamos las matrices MITRE ATT&CK y RE&CT para identificar tácticas, técnicas y procedimientos de ataque relevantes para nuestra organización.

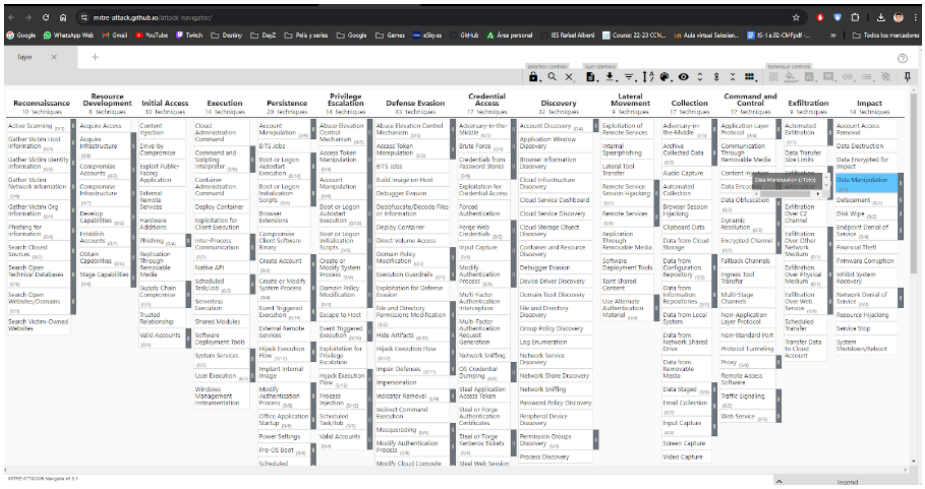

Figure 6: 2024-03-30_17-58.png

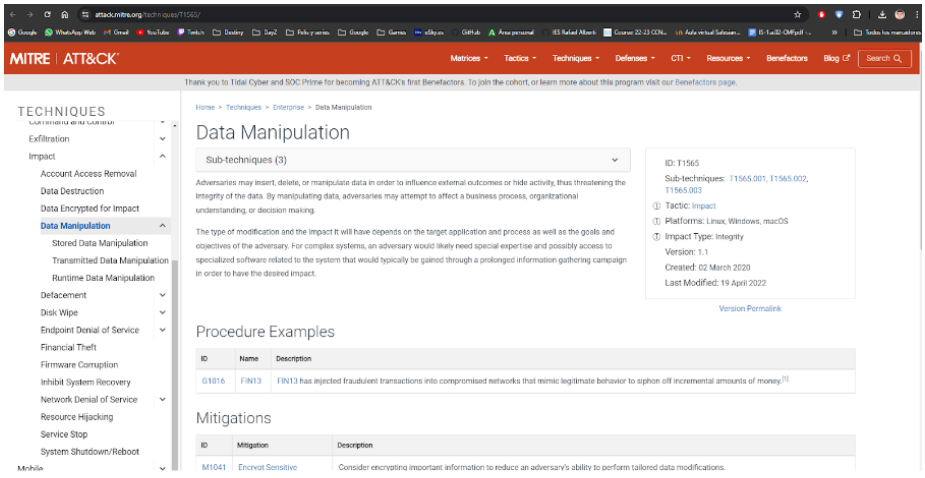

Figure 7: 2024-03-30_17-59.png

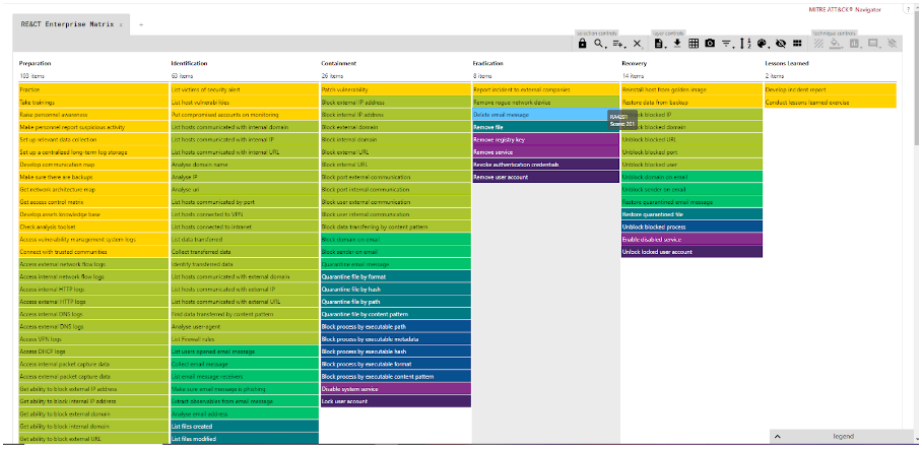

Figure 8: 2024-03-30_17-59_1.png

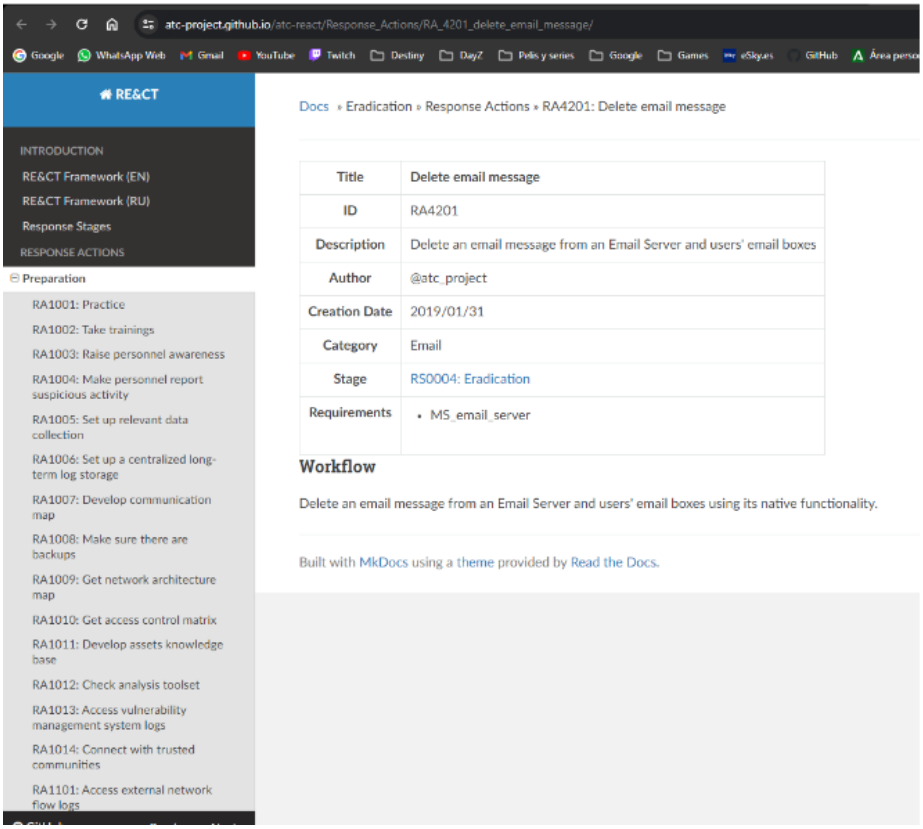

Figure 9: 2024-03-30_17-59_2.png

1.b ¿Qué playbooks has identificado como necesarios en este plan de respuesta y en que te has basado para identificar esos playbooks y saber que son los necesarios? Deja algún diagrama que describa el flujo de un playbook. En este plan de respuesta, se han identificado varios playbooks necesarios para abordar diferentes escenarios de amenazas (Los más típicos en una empresa como la nuestra). Para determinar los playbooks necesarios, nos basamos en la evaluación de riesgos específicos de nuestra organización, así como en las tácticas y técnicas de ataque identificadas a través de las matrices MITRE ATT&CK y RE&CT. Por ejemplo, para un compromiso en la cadena de proveedores, se ha identificado un playbook específico que incluye pasos detallados para su adecuada respuesta:

1.c¿Cómo te has asegurado que has cubierto todas las fases del plan de respuesta? ¿Qué fase consideras que está más floja en un plan? ¿Cuál de ellas consideras que está mejor trabajada en tu plan? Asegúrate de hablar de todas las fases y como las cubres.

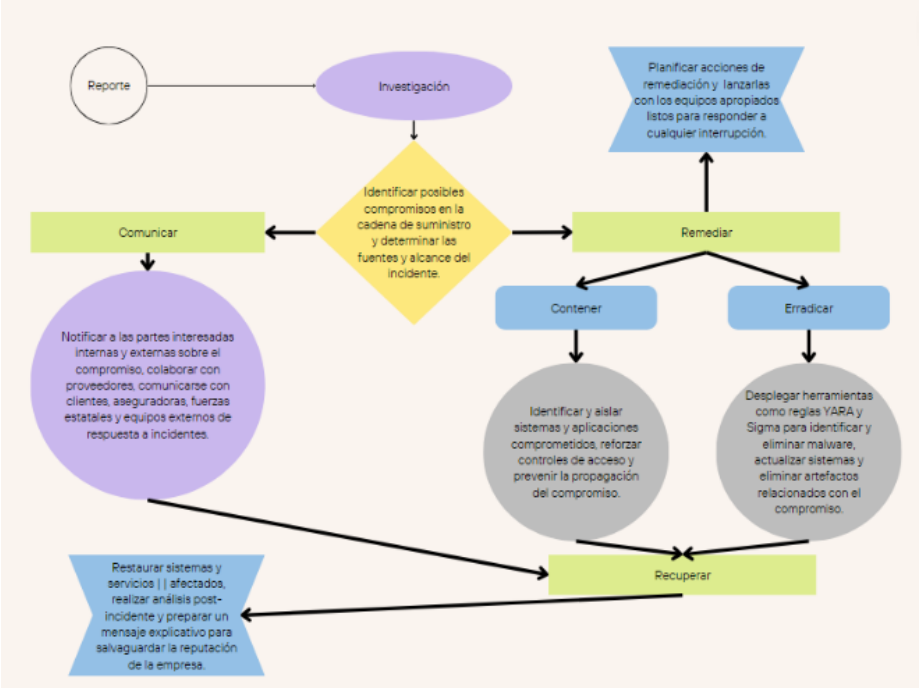

Figure 10: 2024-03-30_17-59_3.png

En un plan de respuesta a incidentes, es fundamental asegurarse de que todas las fases estén cubiertas para garantizar una gestión efectiva y completa de cualquier incidente que ocurra. Aquí está cómo se abordan cada una de las fases en un plan típico y cómo nos aseguramos de que estén completamente cubiertas:

- Investigar: Esta fase implica recopilar información sobre el incidente, determinar su alcance y comprender cómo ocurrió. Para cubrir esta fase, se establecen procedimientos para la recolección de datos relevantes, como registros de actividad, registros de seguridad y análisis forense digital. Además, se designan responsables para llevar a cabo estas investigaciones de manera efectiva.
- Remediar: Una vez que se comprende el incidente, es necesario tomar medidas inmediatas para mitigar el daño y detener cualquier actividad maliciosa. Esto puede incluir la aplicación de parches, la eliminación de malware o la reconfiguración de sistemas comprometidos. En eli plan, se especifican claramente los pasos a seguir para abordar cada tipo de incidente de manera rápida y eficiente.
- Contener: La fase de contención implica aislar el incidente para evitar que se propague y cause más daño. Esto puede implicar la desconexión de sistemas comprometidos de la red o la implementación de medidas de seguridad adicionales para limitar el acceso no autorizado. En el plan, se detallan los procedimientos para establecer perímetros de seguridad y garantizar que el incidente no afecte a otros sistemas o datos.
- Erradicar: Una vez que el incidente está contenido, es importante eliminar completamente cualquier rastro del sistema comprometido y abordar cualquier vulnerabilidad que haya sido explotada. Esto puede requerir una limpieza profunda de sistemas, cambios en la configuración de seguridad y la implementación de medidas de protección adicionales. En el plan, se establecen procedimientos para garantizar que se eliminen todas las amenazas y se fortalecen las defensas para evitar futuros incidentes similares.
- Comunicar: La comunicación efectiva es esencial durante un incidente para informar a las partes interesadas pertinentes, incluidos el equipo de gestión de incidentes, el personal afectado y las autoridades reguladoras si es necesario. En el plan, se detallan los canales de comunicación, las responsabilidades de cada parte interesada y los mensajes clave que deben transmitirse durante cada etapa del incidente.
- Recuperar: Finalmente, la fase de recuperación implica restaurar los sistemas afectados a un estado operativo normal y revisar los procedimientos y controles de seguridad para prevenir futuros incidentes. En el plan, se establecen procedimientos para restaurar sistemas y datos desde copias de seguridad, evaluar el impacto del incidente y realizar mejoras en las políticas y procedimientos de seguridad según sea necesario.

En cuanto a qué fase consideramos que puede ser más floja en un plan de respuesta a incidentes, depende de la organización y de sus recursos disponibles. Sin embargo, la fase de comunicación a menudo se subestima y puede ser descuidada,

lo que puede llevar a confusiones y retrasos en la gestión del incidente. Es crucial asegurarse de tener un plan de comunicación claro y efectivo en su lugar.

En el plan, consideramos que la fase mejor trabajada es la fase de investigar. Esto se debe a que una comprensión completa del incidente es fundamental para tomar decisiones informadas sobre cómo remediar y contener la situación. Además, una investigación exhaustiva puede proporcionar información valiosa para prevenir incidentes similares en el futuro. Por lo tanto, se dedica una atención especial a la recopilación y análisis de datos durante esta fase.

2.a ¿En qué consiste el Flujo de Toma de Decisiones y Escalado de tu plan de respuesta? ¿Existe un plan de comunicación, protocolos, etc? Si la respuesta es correcta, haz un resumen del plan y protocolos. Deja evidencias del flujo, mediante un diagrama.

Plan de Comunicación y Protocolos:

Flujo de Toma de Decisiones y Escalado

- 1. Jerarquía de Toma de Decisiones:

Coordinador Principal: Líder del equipo de respuesta a incidentes con la autoridad final en la toma de decisiones.

Equipo de Respuesta a Incidentes: Compuesto por miembros designados para áreas específicas, como investigación, remediación y comunicación.

- 2. Protocolos de Comunicación:

Canales Claros y Definidos: Establecimiento de canales de comunicación para informar sobre incidentes y compartir actualizaciones.

Comunicación Interna y Externa: Procedimientos definidos para la comunicación dentro del equipo de respuesta a incidentes y con partes interesadas externas.

- 3. Etapas de Escalado:

Niveles de Escalado: Definición de niveles de escalado para incidentes según su gravedad y alcance.

Escalado Progresivo: Los incidentes se escalan desde el equipo de respuesta a incidentes local hasta niveles superiores de gestión según sea necesario.

Diagrama del Flujo de Toma de Decisiones y Escalado:

Este diagrama visualiza el flujo de toma de decisiones y escalado en el equipo de respuesta a incidentes, desde la identificación inicial hasta la recuperación posterior al incidente. Cada etapa está claramente definida con sus responsabilidades y protocolos correspondientes.

3.a ¿Cómo te has asegurado de que tu plan tiene respuestas resilientes? ¿Por qué son resilientes y en qué fases se centran?

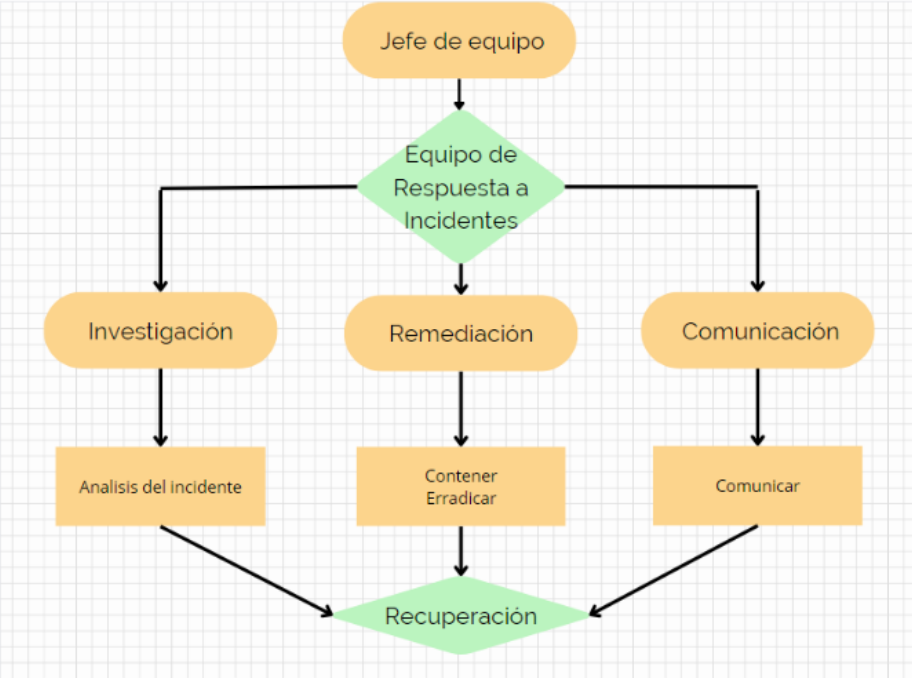

Figure 11: 2024-03-30_18-00.png

Para asegurarnos de que el plan de respuesta a incidentes tiene respuestas resilientes, hemos implementado varias estrategias y prácticas que se centran en diferentes fases del proceso de gestión de incidentes:

- Flexibilidad en el Proceso:

Mi plan está diseñado para ser flexible y adaptable a diferentes tipos de incidentes y situaciones imprevistas. Esto significa que puedo ajustar y modificar los procedimientos según sea necesario para abordar nuevas amenazas o desafíos que puedan surgir.

- Capacidades de Recuperación Rápida:

Se han implementado medidas para una recuperación rápida de los sistemas y datos afectados. Esto incluye la disponibilidad de copias de seguridad actualizadas, procedimientos de restauración eficientes y la capacidad de restaurar sistemas críticos en un tiempo mínimo.

- Enfoque en el Aprendizaje y Mejora Continua:

Después de cada incidente, se realiza una revisión exhaustiva para identificar áreas de mejora y lecciones aprendidas. Esta retroalimentación se incorpora al plan para fortalecer aún más la capacidad de respuesta ante incidentes en el futuro.

- Planificación para Escenarios de Crisis:

El plan incluye la planificación para escenarios de crisis potenciales, como interrupciones graves en la infraestructura, ataques cibernéticos masivos o desastres naturales. Se han establecido protocolos específicos para abordar estas situaciones de manera efectiva.

- Colaboración y Coordinación:

Se fomenta la colaboración y coordinación entre diferentes equipos y partes interesadas tanto internas como externas durante la gestión de incidentes. Esto asegura una respuesta rápida y eficiente, incluso en situaciones de crisis.

Las fases en las que se centran estas prácticas resilientes son principalmente la fase de contención, la fase de recuperación y la fase de aprendizaje posterior al incidente.

Durante la fase de contención, la flexibilidad en el proceso y la capacidad de recuperación rápida son críticas para limitar el impacto del incidente y evitar su propagación. La fase de recuperación se centra en restaurar los sistemas y datos afectados de manera rápida y efectiva para minimizar el tiempo de inactividad. Y la fase de aprendizaje posterior al incidente permite identificar áreas de mejora y fortalecer la capacidad de respuesta para futuros eventos. Estas prácticas resilientes aseguran que el plan esté preparado para enfrentar desafíos y mantener la continuidad del negocio incluso en las circunstancias más adversas.

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 chat.anpipada.com.

4. Iniciar y/o unirse a la llamada de respuesta en 123-456-7890 y/o webex.com/124154sxffsdsa.
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 carlospanlodavid2@anpipada.es. Encripte los correos electrónicos cuando cualquier participante esté fuera del dominio anpipada.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	412343124
Url del Incident Commander	ir.anpipada.com/ic
Lista del Incident Commander	ir.anpipada.com/roster
Lista del equipo de seguridad	ir.anpipada.com/sec-roster
Lista del equipo SME	ir.anpipada.com/sme-roster
Lista de ejecutivos	ir.anpipada.com/exec-roster

Establecer el ritmo de batalla

Realizar la primera llamada de respuesta

1. Realice la llamada inicial utilizando la estructura de llamada de respuesta inicial
2. Siga las instrucciones del Incident Commander. Si el Incident Commander de turno/de guardia no se une a la llamada **dentro de 15 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 6 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 6 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 ir.anpipada.com/files/412343124 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	ir.anpipada.com/files/cil
Lista de activos críticos	ir.anpipada.com/files/critasli
Base de datos de gestión de activos	ir.anpipada.com/assets
Mapa de red	ir.anpipada.com/MAP
Consola SIEM	ir.anpipada.com/siem
Agregador de registros	ir.anpipada.com/log

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?

Táctica del atacante	La forma en que los atacantes ...	Posibles preguntas clave
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 teamviewer.
- 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 volatility.

- Recoger la imagen del disco, si es necesario, utilizando nero.
- 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 ir.anpipada.com/files/412343124 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.anpipada.com/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.anpipada.com/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 legal@anpipada.es.

Notificar a los clientes

- **No** notifique o actualice al personal que no responde hasta que el Incident Commander lo autorice.
- Coordine las notificaciones a los clientes con marketing@anpipada.es.
- 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 exec@anpipada.es y legal@anpipada.es antes de interactuar con las fuerzas del orden.
- Póngase en contacto con las fuerzas del orden locales en Policia San Fernando.
- Póngase en contacto con el FBI en 855-835-5324 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 AT&T USM Anywhere 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 pr.anpipada.com para que le ayude con las relaciones públicas y la comunicación externa.

- Póngase en contacto con The Hartford 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 ee-isac, 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. # Playbooks

Los siguientes playbooks determiann las fases de investigación, remediación y comunicación para incidentes particuales que podrían afectar a la empresa objetivo, dando instrucciones clara que seguir en cda incidente.

Playbook: Ataques de Fuerza Bruta

Investigar

- **Análisis de Logs de Autenticación:**

Revisar los logs de autenticación en busca de intentos de inicio de sesión fallidos o patrones de actividad sospechosa que puedan indicar un ataque de fuerza bruta.

- **Monitorización de Registros de Eventos:**

Analizar los registros de eventos del sistema en busca de actividad anormal, como múltiples intentos de acceso a recursos protegidos. Además, examinar los patrones de tráfico de red en busca de comportamientos anómalos que puedan indicar intentos de fuerza bruta.

- **Escaneo de Vulnerabilidades:**

Realizar un escaneo de vulnerabilidades en los sistemas afectados para identificar posibles puntos de entrada para ataques de fuerza bruta, como servicios mal configurados o contraseñas débiles. También, considerar un análisis geográfico de las direcciones IP para identificar posibles ubicaciones de los atacantes.

Remediar

- **Bloqueo de IP:**

Configurar reglas de firewall para bloquear direcciones IP que realicen múltiples intentos de inicio de sesión fallidos en un período corto de tiempo.

- **Implementación de Mecanismos de Bloqueo Automático:**

Configurar sistemas de prevención de intrusos (IPS) o sistemas de detección de intrusiones (IDS) para bloquear automáticamente direcciones IP que realicen intentos de inicio de sesión repetidos. Además, asegurarse de que todos los sistemas estén actualizados con los últimos parches de seguridad para evitar explotaciones de vulnerabilidades conocidas.

- **Política de contraseñas:**

Reforzar la política de contraseñas de la organización, exigiendo contraseñas complejas y que se cambien periódicamente para evitar la adivinación de contraseñas. También, implementar la autenticación multifactor (MFA) para agregar una capa adicional de seguridad.

Contener

- **Aislamiento de Cuentas Comprometidas:**

Aislar las cuentas comprometidas y limitar su acceso a recursos sensibles hasta que se resuelva el incidente y se tomen medidas correctivas adicionales.

- **Monitorización Continua:**

Implementar sistemas de monitorización continua para detectar y responder rápidamente a cualquier intento adicional de fuerza bruta o actividad maliciosa. Además, configurar sistemas de respuesta automatizada que puedan tomar medidas inmediatas para mitigar los ataques.

Erradicar

- **Identificación de Origen del Ataque:**

Identificar la fuente del ataque de fuerza bruta y tomar medidas para mitigar cualquier riesgo asociado, como la identificación y eliminación de botnets o sistemas comprometidos utilizados en el ataque. Realizar un análisis forense exhaustivo para determinar cómo se llevó a cabo el ataque y qué medidas adicionales de seguridad pueden ser necesarias.

- **Revisión de Políticas de Seguridad:**

Revisar y actualizar las políticas de seguridad para incluir medidas específicas para prevenir la fuerza bruta y promover prácticas seguras de autenticación. Además, colaborar con la comunidad de seguridad para compartir información

sobre el incidente y ayudar a otras organizaciones a protegerse contra ataques similares.

Recuperar

- **Restablecimiento de contraseñas:**

Restablecer las contraseñas de las cuentas comprometidas y de cualquier otra cuenta que pueda haber sido comprometida durante el ataque de fuerza bruta.

- **Monitorización Continua de Actividad:**

Implementar una monitorización continua de la actividad de inicio de sesión para detectar y responder rápidamente a cualquier intento futuro de fuerza bruta. También, actualizar el plan de continuidad del negocio (BCP) para incluir procedimientos específicos para manejar ataques de fuerza bruta y otros incidentes de seguridad cibernética.

Comunicar

- **Notificar a las Partes Interesadas:**

Informar a las partes interesadas sobre la detección y respuesta al ataque de fuerza bruta, los pasos tomados para mitigar la situación y cualquier acción adicional que pueda ser necesaria.

- **Alertar a la Dirección:**

Comunicar a la dirección sobre el incidente de fuerza bruta, resaltando los riesgos para la organización y las medidas tomadas para mitigar el impacto. Además, colaborar con los proveedores de servicios de Internet (ISP) para bloquear o filtrar el tráfico malicioso en la red antes de que alcance la infraestructura de la organización.

Recursos

- Guía de Buenas Prácticas de Seguridad en Gestión de Contraseñas.
- Soluciones de Prevención de Intrusos (IPS).
- "Seguridad de la Información: Prácticas Recomendadas para la Detección y Respuesta ante Ataques de Fuerza Bruta"

Playbook: Compromiso en la cadena de proveedores

Investigar

El producto que ofrecemos o los mecanismos involucrados en el suministro de los mismos podría verse comprometido de cara al consumidor final o el sistema final. Las fases en las que puede ocurrir esto son:

- Manipulación de herramientas de desarrollo.
- Manipulación de un entorno de desarrollo.

- Manipulación de repositorios de código fuente (públicos o privados)
- Manipulación del código fuente en dependencias de código abierto.
- Manipulación de mecanismos de actualización/distribución de software.
- Imágenes del sistema comprometidas/infectadas
- Reemplazo de software legítimo con versiones modificadas
- Ventas de productos modificados/falsificados a distribuidores legítimos
- Interdicción de envíos

El mayor desafío es que los ataques a la cadena de suministro son utilizados por adversarios avanzados, a menudo utilizando nuevas técnicas y herramientas que son difíciles de detectar. Además, la detección de anomalías es un arte impreciso y puede generar demasiadas alertas que los equipos de seguridad deben abordar. Ampliar el equipo de operaciones de seguridad para responder a las alertas y así reducir el tiempo de detección sigue siendo un desafío.

Los ataques a la cadena de suministro amplían aún más el alcance. Además de lo que está bajo el control directo de las organizaciones, los equipos de seguridad deben:

- Hacer un inventario y supervise las herramientas de terceros que utiliza la organización y conozca las vulnerabilidades y las infracciones reveladas.
- Monitorear el acceso remoto otorgado a proveedores, restrinjalo y fortalézcalo con capas adicionales como la autenticación multifactor.
- Supervisar a los proveedores externos que tengan acceso a los recursos corporativos.

Remediar

- **Planificar eventos de remediación** donde estos pasos se lancen juntos (o de manera coordinada), con equipos apropiados listos para responder a cualquier interrupción.
- **Considerar el tiempo y los compromisos** de las acciones de remediación: tu respuesta tiene consecuencias.

Contener

- **Identificar y aislar sistemas comprometidos y aplicaciones:** Identificar los sistemas afectados en la cadena de proveedores y aislarlos de la red, siempre teniendo en cuenta el impacto hacia el negocio.
- **Implementar controles de acceso:** Reforzar los controles de acceso para prevenir la propagación del compromiso a través de la cadena de suministro.
- **Garantizar que no vuelva a suceder:** Si se logra identificar cual fué el origen del ataque, proceder inmediatamente al arrego y puesta en marcha de vuelta del elemento comprometido.

Erradicar

- **Despliegue de reglas YARA:** Es una herramienta de código abierto que fue desarrollada por la plataforma VirusTotal para identificar los elementos de un malware por medio de un análisis estático automatizado.
- **Despliegue de reglas Sigma:** Es un metalenguaje genérico y abierto, creado por Florian Roth, que permite describir en formato YAML reglas para detectar registros relevantes de una manera directa. El formato de la regla es muy flexible, fácil de escribir y aplicable a cualquier tipo de registro.
- **Eliminar malware y artefactos:** Realizar un escaneo exhaustivo de todos los sistemas afectados para identificar y eliminar malware y otros artefactos relacionados con el compromiso.
- **Actualizar sistemas y software:** Aplicar parches de seguridad y actualizaciones de software para cerrar posibles brechas de seguridad en la cadena de proveedores.

Referencia: Recursos de Remediación Reglas YARA

Reglas Sigma

Comunicar

1. **Notificar a las partes interesadas:** Comunicar de manera proactiva el compromiso a las partes interesadas internas y externas, proporcionando información relevante sobre el impacto y las acciones tomadas.
2. **Coordinar con proveedores:** Establecer una comunicación transparente con los proveedores afectados para colaborar en la respuesta al compromiso y mitigar su impacto.
3. **Comunicar a llos clientes:** Comunicar a todos los clientes que pueden ser víctimas de recibir el producto malformado.
4. **Contactar con aseguradoras:** Rápidamente consultar a la aseguradora e informar detalladamente del incidente para saber que recursos nos prestarán.
5. **Contactar con fuerzas estatales:** Establecer una comunicación transparente con las fuerzas del estado si fuera necesario.
6. **Contactar con empresas externas:** Informar incidentes a empresas de seguridad externas, es decir, Equipos Nacionales de Respuesta a Incidentes de Seguridad Informática (CSIRT). Proporcionar todos los indicadores de compromiso e indicadores de ataque que se hayan observado.

Recuperar

1. **Restaurar la funcionalidad:** Implementar medidas para restaurar los sistemas y servicios afectados a un estado operativo normal.
2. **Realizar análisis post-incidente:** Evaluar el impacto del compromiso en la cadena de proveedores y mejorar los procesos y controles de seguridad

para prevenir futuros incidentes.

3. **Preparar un mensaje explicativo:** Tras este tipo de incidente y para salvaguardar la reputación de la empresa lo mejor es tener un mensaje explciativo de cara al público de que ha pasado y de como lo hemos solucinado.
4. **Creación de un reporte:** Desarrollr el Informe de Incidencia utilizando tu plantilla corporativa. Debe incluir:

- Resumen ejecutivo con una breve descripción de los daños, las acciones tomadas, la causa raíz y las métricas clave (tiempo para detectar, tiempo para responder, tiempo para recuperarse, etc.)
- Cronograma detallado de las acciones del adversario asignadas a las tácticas de ATT&CK (puedes usar Kill Chain, pero lo más probable es que la mayoría de las acciones estén en la etapa Acciones según el objetivo, que no es muy representativa ni útil) Cronograma detallado de las acciones tomadas por el equipo de respuesta a incidentes
- Análisis de causa raíz y recomendaciones de mejora en función de su conclusión.
- Lista de especialistas involucrados en Respuesta a Incidentes con sus roles

Información adicional

1. "Playbook of the Week: Automated Rapid Response to 3CXDesktopApp Supply Chain Attack", Jane Goh (Apr 06, 2023)
2. "How to Respond to a Supply Chain Attack", Kasey Panetta (Jan 11, 2021)
3. "Supply Chain Attack Framework and Attack Patterns", John F. Miller (Dec 2013)

Playbook: Denegación de Servicio de Dispositivos Finales

Investigar

La investigación en respuesta a un ataque de denegación de servicio es un procedimiento multifacético que comienza con la supervisión del rendimiento de los dispositivos finales, como los servidores. Este monitoreo es una tarea crucial que se debe realizar con regularidad para identificar cualquier anomalía que pueda surgir. Las anomalías podrían incluir una disminución repentina en el rendimiento del dispositivo o un aumento inusual en el uso de recursos. Estos podrían ser signos tempranos de un ataque en curso y el reconocimiento temprano de estos signos puede ser esencial para mitigar el impacto del ataque.

Además del monitoreo del rendimiento del dispositivo, también es importante revisar y analizar los logs del sistema. Los logs del sistema son registros que mantienen un seguimiento de toda la actividad que ocurre en el servidor, y son una fuente valiosa de información para identificar posibles amenazas a la seguridad. Durante el análisis de estos logs, es importante buscar eventos

inusuales que puedan indicar un ataque de denegación de servicio. Estos eventos podrían ser intentos de acceso repetidos, solicitudes anómalas o errores de sistema inesperados. Una vez más, la detección temprana de estos signos puede ser crucial para prevenir o mitigar un ataque.

Finalmente, la etapa de investigación también implica el seguimiento de las alertas de seguridad. Estas alertas son generadas por sistemas de detección de intrusos (IDS) o sistemas de prevención de intrusos (IPS). Estos sistemas son una parte integral de la seguridad de la red, ya que pueden identificar y alertar sobre posibles ataques de denegación de servicio. Es crucial estar atento a estas alertas y tomar las medidas necesarias para mitigar cualquier ataque que pueda estar en curso.

En resumen, la investigación en respuesta a un ataque de denegación de servicio es un proceso que requiere vigilancia constante, análisis detallado y una reacción rápida. Al combinar estos pasos, se puede garantizar la seguridad y la continuidad del servicio.

Remediar

- **Optimización de Configuraciones:**

Ajustar las configuraciones de los dispositivos finales, como servidores, para optimizar el rendimiento y reducir la vulnerabilidad a los ataques de denegación de servicio.

- **Implementación de Cortafuegos:**

Configurar y activar cortafuegos en los dispositivos finales para filtrar el tráfico malicioso y mitigar los ataques de denegación de servicio.

- **Actualización de Software:**

Mantener actualizado el software y los sistemas operativos de los dispositivos finales para corregir vulnerabilidades conocidas y mejorar la resistencia a los ataques de denegación de servicio.

Contener

- **Bloqueo de IPs Maliciosas:**

Bloquear las direcciones IP identificadas como origen del ataque de denegación de servicio en los dispositivos finales para evitar futuros intentos de ataque desde esas direcciones.

- **Segmentación de Red:**

Segmentar la red para limitar el impacto de los ataques de denegación de servicio y aislar los dispositivos finales críticos del resto de la infraestructura.

Erradicar

- **Identificar Origen del Ataque:**

Investigar y identificar el origen del ataque de denegación de servicio en los dispositivos finales, ya sea mediante el análisis de registros de red o la colaboración con proveedores de servicios de Internet (ISP).

- **Mejora de Políticas de Seguridad:**

Actualizar las políticas de seguridad para incluir medidas específicas para prevenir y mitigar ataques de denegación de servicio en dispositivos finales.s

Recuperar

- **Restauración de Servicios:**

Restaurar los servicios afectados por el ataque de denegación de servicio tan pronto como sea posible para minimizar el impacto en la operación del negocio.

- **Análisis Post-Mortem:**

Realizar un análisis detallado después del ataque para identificar las causas subyacentes y tomar medidas para fortalecer la seguridad y prevenir futuros ataques similares.

Comunicar

- **Notificar a las Partes Interesadas:**

Informar a las partes interesadas sobre el ataque de denegación de servicio en los dispositivos finales, las medidas tomadas para mitigar el impacto y las acciones adicionales que se están tomando para fortalecer la seguridad.

- **Alertar a la Dirección:**

Comunicar a la dirección sobre el incidente de denegación de servicio, resaltando los riesgos para la operación del negocio y las medidas implementadas para proteger los dispositivos finales.

- **Coordinar con Proveedores de Servicios:**

Colaborar con proveedores de servicios de Internet y otros proveedores externos para compartir información sobre el ataque y coordinar esfuerzos para defenderse contra futuros ataques de denegación de servicio.

Recursos

- Referencia: Guía de Buenas Prácticas de Seguridad del Centro Nacional de Ciberseguridad (NCSC) sobre Protección de Dispositivos Finales
- Referencia: Herramientas de Monitoreo de Rendimiento del Sistema
- “Mitigación de Ataques de Denegación de Servicio en Dispositivos Finales: Estrategias y Prácticas Recomendadas”

Playbook: Denegación de Servicio en Internet (DDoS)

Investigar

El procedimiento de respuesta a un ataque de denegación de servicio (DDoS) comienza con el monitoreo constante del tráfico de red. Este monitoreo tiene como objetivo identificar cualquier anomalía que pueda surgir. Algunos ejemplos de estas anomalías podrían ser picos inusuales en la cantidad de tráfico, la presencia de paquetes maliciosos o patrones de actividad que resulten sospechosos. Todos estos pueden ser indicativos de un intento de ataque a la red.

El siguiente paso es la revisión y análisis de los logs del servidor. Los logs son registros que mantienen un seguimiento de toda la actividad que ocurre en el servidor, y son una fuente valiosa de información para identificar posibles amenazas a la seguridad. Durante el análisis, es importante buscar signos de intentos de acceso maliciosos, solicitudes repetidas desde una misma dirección IP o cualquier otro comportamiento que pueda considerarse anómalo. Estos pueden ser signos de un ataque en proceso o de un intento de invasión.

La última etapa involucra el seguimiento de las alertas de seguridad. Estas alertas son generadas por sistemas de detección de intrusiones (IDS) o sistemas de prevención de intrusiones (IPS). Estos sistemas son vitales para la seguridad de la red ya que pueden identificar y alertar sobre posibles ataques de denegación de servicio. Es crucial estar atento a estas alertas y tomar las medidas necesarias para mitigar cualquier ataque que pueda estar en curso.

En resumen, la respuesta a un ataque de denegación de servicio es un proceso que requiere vigilancia constante, análisis detallado y reacción rápida para garantizar la seguridad y la continuidad del servicio.

Remediar

- **Implementación de Filtros de Tráfico:**

Configurar y activar filtros de tráfico para bloquear paquetes maliciosos y mitigar el impacto de los ataques de denegación de servicio.

- **Actualización de Firmas de IDS/IPS:**

Mantener actualizadas las firmas de IDS/IPS para detectar y bloquear nuevos tipos de ataques de denegación de servicio.

- **Redirección de Tráfico:**

Utilizar técnicas de redirección de tráfico para desviar el tráfico malicioso lejos de los sistemas críticos y mantener la disponibilidad de los servicios.

Contener

- **Bloqueo de IPs Maliciosas:**

Bloquear las direcciones IP identificadas como origen del ataque de denegación de servicio para evitar futuros intentos de ataque desde esas direcciones.

- **Segmentación de Red:**

Segmentar la red para limitar el impacto de los ataques de denegación de servicio y aislar los sistemas críticos del resto de la infraestructura.

Erradicar

- **Identificar Origen del Ataque:**

Investigar y identificar el origen del ataque de denegación de servicio, ya sea mediante el análisis de registros de red o la colaboración con proveedores de servicios de Internet (ISP).

- **Mejora de Políticas de Seguridad:**

Actualizar las políticas de seguridad para incluir medidas específicas para prevenir y mitigar ataques de denegación de servicio en el futuro.

Recuperar

- **Restauración de Servicios:**

Restaurar los servicios afectados por el ataque de denegación de servicio tan pronto como sea posible para minimizar el impacto en la operación del negocio.

- **Análisis Post-Mortem:**

Realizar un análisis exhaustivo después del ataque para identificar las vulnerabilidades explotadas y tomar medidas para fortalecer la infraestructura de seguridad y prevenir futuros ataques similares.

Comunicar

- **Notificar a las Partes Interesadas:**

Informar a las partes interesadas sobre el ataque de denegación de servicio, las medidas tomadas para mitigar el impacto y las acciones adicionales que se están tomando para fortalecer la seguridad.

- **Alertar a la Dirección:**

Comunicar a la dirección sobre el incidente de denegación de servicio, resaltando los riesgos para la operación del negocio y las medidas implementadas para proteger los sistemas y datos.

- **Coordinar con Proveedores de Servicios:**

Colaborar con proveedores de servicios de Internet y otros proveedores externos para compartir información sobre el ataque y coordinar esfuerzos para defenderse contra futuros ataques de denegación de servicio.

Recursos

- Referencia: Guía de Buenas Prácticas de Seguridad de DDoS del National Institute of Standards and Technology (NIST)
- Referencia: Herramientas de Monitoreo de Red y Seguridad
- "Mitigación de Ataques de Denegación de Servicio: Estrategias y Prácticas Recomendadas"

Playbook: Escaneo activo

Investigar

Los adversarios pueden ejecutar exploraciones de reconocimiento activas para recopilar información que pueda utilizarse durante la selección de objetivos. Los escaneos activos son aquellos en los que el adversario investiga la infraestructura de la víctima a través del tráfico de red, a diferencia de otras formas de reconocimiento que no implican interacción directa.

Para realizar estos tipos de reconocimientos se hacen uso de ciertos protocolos como puede ser el ICMP. La información que consiguen se puede traducir en objetivos potencialesy oportunidades para los atacantes.

Para la detección de este tipo de ataque se ha de monitorear y analizar patrones de tráfico e inspección de paquetes asociados a protocolos que no siguen los estándares de protocolo y flujos de tráfico esperados (por ejemplo, paquetes extraños que no pertenecen a flujos establecidos, patrones de tráfico anómalos o gratuitos, sintaxis o estructura anómala). Considere la correlación con el monitoreo de procesos y la línea de comando para detectar la ejecución de procesos anómalos y los argumentos de la línea de comando asociados a los patrones de tráfico (por ejemplo, monitorear anomalías en el uso de archivos que normalmente no inician conexiones para los protocolos respectivos).

También se ha de supervisar los datos de la red para detectar flujos de datos poco comunes. Los procesos que utilizan la red y que normalmente no tienen comunicación de red o que nunca antes se han visto son sospechosos.

Podemos encontrar tres sub-técnicas que son:

- **Escaneo de bloques de IP:** Los atacantes pueden escanear los bloques de IP de las víctimas para recopilar información que pueda utilizarse durante la focalización. Las direcciones IP públicas se pueden asignar a organizaciones por bloque o por un rango de direcciones secuenciales.
- **Escaneo de vulnerabildiades:** Un atacante puede escanear a las víctimas en busca de vulnerabilidades que puedan utilizarse durante la orientación. Los análisis de vulnerabilidades suelen comprobar si la configuración de un host/aplicación de destino (por ejemplo, software y versión) se alinea potencialmente con el objetivo de un exploit específico que el adversario pueda intentar utilizar.

- **Escaneo con diccionarios:** Un atancate podría sondear iterativamente la infraestructura utilizando técnicas de rastreo y fuerza bruta. Si bien esta técnica emplea métodos similares a la Fuerza Bruta, su objetivo es la identificación de contenido e infraestructura en lugar del descubrimiento de credenciales válidas. Las listas de palabras utilizadas en estos escaneos pueden contener nombres genéricos de uso común y extensiones de archivo o términos específicos de un software en particular.

Remediar

Preparación Entre algunas técinas para protejernos para estos ataques tenemos:

- Realizar inspecciones rutinarias.
- Asegurar que sistemas como el IDS/IPS, SIEM o firewall se encuentran actualizados.
- Revisar las reglas del firewall y del IDS/IPS rutinalmente basadas en las necesidades del entorno.
- Restringir acceso via protocolos RDP o SSH y similares donde no sean necesarios.
- Quitar banners de protocolos de conexión.
- Quitar los encabezados por defecto de apliciones web.
- Confirmar que los logs de los diferentes servidores y puestos de trabajo se envian a un lugar centralizado.

Contener Entro los diferentes pasos para contener este tipo de ataque tenemos:

- Realizar un inventariado enumerando los diferentes activos sujetos al escaner.
- Archivar artefactos relacionados con es escaneo como puden ser direcciones IP, las peticiones o el propio user agent.
- Realizar un análisis exhaustivo para identificar los puntos de entrada utilizados por el atacante durante el escaneo activo.
- Creación de un refuerzo perimetral para diferentes actores de este tipo de amenaza conocidos.
- Realizar capturas de tráfico en los puntos clave para posterior análisis.

Erradicar

- Inmediatamente realizar escaneres antivirus en los endpints objetivo.
- Cambiar las posibles contraseñas comprometidas.

- Inscpeccionar tanto la actividad de usuario como los dispositivos en busca de actividad IOC coincidente con el perfil del ataque.
- Proceder al bloqueo del origen del ataque como puden ser los diferentes protocolos usados, user agents o una IP.

Comunicar

Después de un incidente de escaneo activo, la comunicación efectiva es esencial para informar a las partes pertinentes y manejar la situación de manera adecuada. A continuación, se detallan los pasos para comunicar el incidente:

- Equipo de Respuesta a Incidentes (IR Team):

Notificar de inmediato al Equipo de Respuesta a Incidentes (IR Team) interno sobre el incidente de escaneo activo. Establecer un canal de comunicación directo y seguro para el IR Team para facilitar la coordinación y la toma de decisiones.

- Responsables Internos:

Informar a los responsables internos relevantes, como el equipo de seguridad de la información, el equipo de TI y la alta dirección, sobre el incidente. Proporcionar detalles precisos sobre la naturaleza del escaneo activo y su impacto potencial en el entorno organizacional.

- Autoridades Regulatorias y de Cumplimiento:

Según las regulaciones y políticas aplicables, notificar a las autoridades regulatorias pertinentes sobre el incidente de escaneo activo. Cooperar plenamente con las autoridades regulatorias y proporcionar la información requerida de manera oportuna y precisa.

- Proveedores de Servicios y Socios Comerciales:

Comunicar el incidente a los proveedores de servicios y socios comerciales que puedan verse afectados por el escaneo activo. Coordinar con los proveedores de servicios y socios comerciales para mitigar cualquier impacto potencial en sus sistemas y datos.

- Clientes y Usuarios Finales:

Si es necesario, informar a los clientes y usuarios finales sobre el incidente de escaneo activo y cualquier acción recomendada que deban tomar. Proporcionar orientación clara y precisa para ayudar a los clientes y usuarios finales a proteger sus datos y sistemas.

- Comunicación Externa:

Preparar un comunicado de prensa o declaración pública para proporcionar transparencia sobre el incidente de escaneo activo, especialmente si puede afectar la confianza del público en la organización. Designar un portavoz oficial para manejar las consultas de los medios y garantizar un mensaje consistente y preciso.

Recuperar

- Validar si los IOC contactados en los puntos finales detectados no se ven en otros dispositivos, ya que esto puede indicar que se pueden realizar más escaneos de red.
- Considerar implementar y desplegar tecnologías de engaño (como un honeypot) para alejar a los ciberdelincuentes de los verdaderos activos de su organización. Estos señuelos imitan servidores, aplicaciones y datos legítimos para engañar al delincuente haciéndole creer que se ha infiltrado y obtenido acceso a los activos más importantes de su organización cuando en realidad no es así.
- Verificar que los dispositivos víctmas del escaner no han sufrido ningún ataque.

Información adicional

1. "Network Scan Incident Response Playbook", Lomu (Apr 08, 2023)
2. "GSPBC-1030: Reconnaissance – Active Scanning", Rylan Wallace (Oct 21, 2021)

Playbook: Exfiltración de Datos

Investigar

- **Análisis de Logs de Seguridad:**

Revisar los logs de seguridad en busca de actividades sospechosas, como transferencias de archivos inusuales, accesos no autorizados o intentos de autenticación fallidos.

- **Monitorización del Tráfico de Red:**

Analizar el tráfico de red en busca de patrones anómalos, como transferencias de datos no autorizadas o comunicaciones con direcciones IP desconocidas.

- **Revisión de Acceso a Recursos Sensibles:**

Investigar los accesos a recursos sensibles o bases de datos que podrían indicar intentos de exfiltración de datos.

- **Escaneo de Malware:**

Realizar un escaneo completo de malware en sistemas comprometidos para identificar y eliminar posibles amenazas que podrían facilitar la exfiltración de datos.

Remediar

- **Restricción de Acceso:**

Implementar políticas de control de acceso más estrictas para restringir el acceso a datos sensibles solo a usuarios autorizados y limitar los permisos de escritura en sistemas críticos.

- **Actualización de Políticas de Seguridad:**

Revisar y actualizar las políticas de seguridad para incluir medidas específicas para prevenir la exfiltración de datos y promover prácticas seguras de gestión de información.

- **Implementación de DLP:**

Desplegar soluciones de prevención de pérdida de datos (DLP) para monitorear y prevenir la transferencia no autorizada de información sensible fuera de la red corporativa.

Contener

- **Aislamiento de Sistemas Comprometidos:**

Aislar los sistemas comprometidos de la red principal para prevenir la propagación de la exfiltración de datos y limitar el daño potencial.

- **Monitorización Continua:**

Implementar sistemas de monitorización continua para detectar y responder rápidamente a cualquier intento adicional de exfiltración de datos.

Erradicar

- **Método de Exfiltración:**

Identificar el método utilizado para la exfiltración de datos, como correo electrónico, transferencia FTP, o carga a servicios en la nube, y tomar medidas para mitigar cualquier riesgo asociado.

- **Revisión de Políticas de Seguridad:**

Revisar y actualizar las políticas de seguridad para incluir medidas específicas para prevenir la exfiltración de datos y promover prácticas seguras de gestión de información.

Recuperar

- **Restauración de Datos:**

Restaurar los datos exfiltrados desde copias de seguridad limpias y verificadas para asegurar la integridad y la disponibilidad de la información.

- **Auditoría Post-Incidente:**

Realizar una auditoría exhaustiva post-incidente para identificar las causas subyacentes del incidente de exfiltración de datos y recomendar medidas preventivas adicionales.

Comunicar

- **Notificar a las Partes Interesadas:**

Informar a las partes interesadas sobre la detección y respuesta a la exfiltración de datos, los pasos tomados para remediar la situación y cualquier acción adicional que pueda ser necesaria.

- **Alertar a la Dirección:**

Comunicar a la dirección sobre el incidente de exfiltración de datos, resaltando los riesgos para la organización y las medidas tomadas para mitigar el impacto.

- **Coordinar con Equipos de Seguridad:**

Colaborar con equipos de seguridad internos y externos para compartir información sobre el incidente y desarrollar estrategias de defensa contra la exfiltración de datos en el futuro.

- **Evaluación de Impacto:**

Realizar una evaluación de impacto del incidente de exfiltración de datos para comprender completamente las repercusiones en la organización y en los interesados, y así poder proporcionar una comunicación clara y precisa.

- **Asesoramiento Legal:**

Consultar con el equipo legal para evaluar cualquier implicación legal relacionada con la exfiltración de datos, incluyendo posibles responsabilidades, cumplimiento normativo y acciones legales que puedan ser necesarias.

- **Gestión de Crisis de Imagen:**

Coordinar con el equipo de relaciones públicas o gestión de crisis para desarrollar mensajes consistentes y precisos destinados a proteger la reputación de la organización y mantener la confianza del público y de los clientes.

- **Canal de Comunicación Segura:**

Establecer un canal de comunicación seguro y confidencial para discutir el incidente con los interesados internos y externos, garantizando la confidencialidad de la información sensible relacionada con el incidente.

Recursos

- Guía de Buenas Prácticas de Seguridad en Gestión de Datos Sensibles
- Soluciones de Prevención de Pérdida de Datos (DLP)
- "Seguridad de la Información: Prácticas Recomendadas para la Detección y Respuesta ante Exfiltración de Datos"

Playbook: Explotación de Aplicaciones Públicas

Investigar

Las aplicaciones públicas pueden ser objeto de explotación por parte de adversarios que buscan comprometer la integridad, confidencialidad o disponibilidad de los datos. Las fases en las que podría ocurrir esto incluyen:

- Identificación de vulnerabilidades en la aplicación.
- Explotación de vulnerabilidades para obtener acceso no autorizado.
- Manipulación de datos sensibles o críticos.
- Inyección de código malicioso.
- Robo de credenciales de usuarios.
- Intercepción de comunicaciones sensibles.
- Exfiltración de datos.

El desafío principal radica en la detección y mitigación oportuna.

Identificación/detección

- Detectar cambios inusuales en la aplciación, ya sea en su manera de funcionar, su consumo de recursos o su apariencia.
- Los cambios en la base de datos como un aumentom repentino del numero de consultas o la provenencia de las mismas pueden ser un indicador, además de la modificación de datos inusual.
- Busquar correos electrónicos de phishing. Los correos electrónicos de phishing son el método más común de robo de credenciales.
- Busquar correos electrónicos con enlaces a sitios de recolección de credenciales.
- Busquar en el historial web del usuario para determinar si se visitó algún sitio potencialmente malicioso.
- Busquar malware potencial en la estación de trabajo del usuario.
  - Recolectores de credenciales como Mimikatz.
  - Software de grabación de pulsaciones de teclas.
  - Malware de raspado del portapapeles.

Remediar

- **Planificar eventos de remediación:** Coordinar acciones de remediación con equipos relevantes para minimizar el impacto y restaurar la integridad de las aplicaciones comprometidas.
- **Evaluar el riesgo:** Priorizar acciones de remediación según el nivel de riesgo y el impacto en la seguridad de las aplicaciones.
- **Si la aplicación web está alojada en otro servicio:** (GoDaddy, HostGator, Ionos, empresa de alojamiento local, etc.), comuníquese con el servicio de alojamiento para informar el problema.
  - Pregunte sobre cualquier problema de seguridad reciente en su entorno.
  - Pregunte sobre los posibles registros que puedan poseer.

  - Obtenga estos registros y consérvelos lo antes posible.
- **Determinar el método inicial de compromiso:** Esto se limitará a aquellos con acceso administrativo o de gestión de aplicaciones web. Realizar entrevistas a los usuarios impactados y realizar una serie de preguntas que podrían ser:
  - ¿Recibiste un correo electrónico sospechoso?
  - ¿Ingresó sus credenciales de correo electrónico después de hacer clic en un enlace o en un sitio web que parecía no aceptarlas?
  - ¿Has descargado algún software nuevo?
  - ¿Ha recibido algún documento por correo electrónico que no esperaba?
  - ¿No ha notado acciones anormales en su estación de trabajo?

Mitigar Entre algunas opciones para mitigar el daño que puede provocar este acceso inicial a nuestros sistemas tenemos:

- El aislamiento de la aplicación limitará a qué otros procesos y características del sistema puede acceder el objetivo explotado.
- Los firewalls de aplicaciones web se pueden utilizar para limitar la exposición de las aplicaciones y evitar que el tráfico de explotación llegue a la aplicación.
- Segmentar los servidores y servicios externos del resto de la red con una DMZ o en una infraestructura de alojamiento independiente.
- Usar el privilegio mínimo para las cuentas de servicio limitará los permisos que obtiene el proceso explotado en el resto del sistema.
- Escanear periódicamente los sistemas externos en busca de vulnerabilidades y establezca procedimientos para parchear rápidamente los sistemas cuando se descubran vulnerabilidades críticas mediante el escaneo y la divulgación pública.

Contener

- **Identificar y aislar sistemas comprometidos:** Identificar las aplicaciones afectadas y aislarlas de la red para evitar la propagación del compromiso.
- **Implementar controles de acceso:** Reforzar los controles de acceso para prevenir futuros accesos no autorizados a las aplicaciones.
- **En caso de compromiso de cuentas administrativas:** Cambiar todas las contraseás del resto de cuentas de administración de la aplicación web, empezando obviamente por la cuenta comprometida. Además es conveniente habilitar autenticación multifactor, deshabilitar metodos de autenticación alternativos como podrían ser certficados. Deshabiltiar los tekens de autentciaciónd e todas las cuentas. Si se identifica una

organización externa durante la investigación, notifique a la organización sobre cualquier compromiso o inquietud.

- **En caso de encontrar malware:** Conserve una muestra del malware. Analizar el malware con cualquier herramienta disponible. Recopilar el hash del archivo utilizando el cmdlet "Get-Filehash" de PowerShell. Enviar hash a fuentes de la comunidad VirusTotal, Hybrid-Analysis, etc. Si las fuentes de la comunidad han visto el hash, tenga en cuenta las características del malware.

Erradicar

- **Desplegar actualizaciones de seguridad:** Aplicar parches y actualizaciones de seguridad para corregir las vulnerabilidades explotadas en las aplicaciones comprometidas.
- **Realizar análisis de código:** Revisar el código de las aplicaciones en busca de posibles puertas traseras o vulnerabilidades adicionales.
- **Eliminar malware y artefactos:** Realizar escaneos exhaustivos para identificar y eliminar cualquier malware o código malicioso presente en las aplicaciones comprometidas.
- **Buscar cambios en la aplciación:** Es conveniente realziar una comprarción del código fuente de la aplicación para saber si el atacante ha conseguido inyectar su propio código malicioso.

Referencia: Recursos de Remediación OWASP Top 10 CERT Guide to Malware Incident Prevention and Handling

Comunicar

1. **Notificar a las partes interesadas:** Comunicar de manera proactiva el compromiso a las partes interesadas internas y externas, proporcionando información relevante sobre el impacto y las acciones tomadas.
2. **Coordinar con proveedores:** Establecer una comunicación transparente con los proveedores de servicios afectados para colaborar en la respuesta al compromiso y mitigar su impacto.
3. **Comunicar a los clientes:** Informar a los usuarios afectados sobre el incidente de seguridad y proporcionar orientación sobre las medidas que deben tomar para proteger sus datos.
4. **Contactar con aseguradoras:** Consultar con la aseguradora para informar sobre el incidente y evaluar el alcance de la cobertura de seguro disponible.
5. **Contactar con fuerzas estatales:** Establecer comunicación con las autoridades competentes según sea necesario, siguiendo los protocolos legales y regulatorios aplicables.
6. **Contactar con empresas externas:** Informar a organizaciones externas relevantes, como agencias de seguridad cibernética y organismos de re-

spuesta a incidentes, para compartir información y colaborar en la respuesta al incidente.

Recuperar

1. **Restaurar la funcionalidad:** Implementar medidas para restaurar las aplicaciones afectadas a un estado operativo normal, asegurando la integridad y disponibilidad de los datos.
2. **Reemplazar la aplicación:** Restaurar la aplicación con una copia segura del estado del código anterior al incidente. 3.**Restaurar lso sitemas:** Restaurar los sistemas afectados a partir de una copia de seguridad limpia, realizada antes de la infección, si estas copias de seguridad están disponibles.
3. **Realizar análisis post-incidente:** Evaluar el impacto del compromiso en las aplicaciones y mejorar los controles de seguridad para prevenir futuras explotaciones.
4. **Preparar un mensaje explicativo:** Elaborar un comunicado público detallando el incidente, las acciones tomadas y las medidas de seguridad adicionales implementadas para mitigar futuros riesgos.
5. **Crear un informe detallado:** Documentar el incidente, incluyendo el cronograma de eventos, las acciones de respuesta tomadas y las lecciones aprendidas, para mejorar la preparación y respuesta ante futuros incidentes.

Información adicional

1. "OWASP Application Security Verification Standard"
2. "Web Application Attack Response Playbook"
3. "Exploit Public-Facing Application ID: T1190" (Apr 14, 2023)

Playbook: Phishing

Investigar

- **Determinar el Alcance del Ataque:**

Identificar el alcance del ataque, incluyendo el número total de usuarios afectados y las acciones tomadas en respuesta al correo electrónico de phishing (por ejemplo, descarga de archivos adjuntos, visita al sitio web falsificado, divulgación de información personal o comercial).

- **Análisis de Mensajes:**

Analizar el mensaje de phishing utilizando un dispositivo seguro para determinar la información clave, como remitente, destinatarios, asunto, cuerpo del mensaje, adjuntos y enlaces.

- **Análisis de Enlaces y Adjuntos:**

Utilizar herramientas como nslookup, whois, VirusTotal y sandboxes de malware para analizar los enlaces y adjuntos sospechosos en busca de indicadores de compromiso (IOC).

- **Categorización y Evaluación de la Gravedad:**

Clasificar el tipo de ataque de phishing y evaluar la gravedad considerando el riesgo para la seguridad pública o personal, la exposición de datos sensibles, el impacto en el negocio y la capacidad para controlar o registrar sistemas críticos.

Remediar

- **Bloqueo de URLs Maliciosas:**

Bloquear el acceso a las URLs maliciosas identificadas para prevenir que los usuarios accedan a sitios web fraudulentos.

- **Educación del Usuario:**

Capacitar a los usuarios sobre cómo identificar correos electrónicos de phishing y qué hacer en caso de recibir uno, incluyendo no hacer clic en enlaces sospechosos ni proporcionar información confidencial.

- **Implementación de Filtros Anti-Phishing:**

Reforzar los filtros de correo electrónico para detectar y bloquear correos electrónicos de phishing antes de que lleguen a la bandeja de entrada del usuario.

- **Reporte de Phishing:**

Establecer un proceso para que los usuarios reporten correos electrónicos de phishing sospechosos al equipo de seguridad para una acción adicional.

- **Cambiar Credenciales:**

Cambiar las credenciales de acceso para cuentas comprometidas y reforzar la autenticación multifactor (MFA) cuando sea posible.

Contener

- **Bloqueo de Cuentas Comprometidas:**

Bloquear las cuentas de usuario comprometidas que hayan sido utilizadas para acceder a enlaces de phishing o proporcionar información confidencial.

- **Despliegue de Parches de Seguridad:**

Aplicar parches de seguridad a los sistemas y aplicaciones afectados por cualquier exploit utilizado en los correos electrónicos de phishing para mitigar posibles riesgos de seguridad.

- **Bloquear Acceso a Dominios Maliciosos:**

Bloquear el acceso a dominios maliciosos identificados utilizando DNS, firewalls o proxies.

- **Implementar Retención Forense:**

Implementar retención forense de mensajes y purgar mensajes relacionados de otras bandejas de entrada de usuario.

Erradicar

- **Identificar Origen del Phishing:**

Identificar el origen del correo electrónico de phishing y tomar medidas para mitigar cualquier riesgo asociado, como el compromiso de cuentas de usuario o la exposición de información confidencial.

- **Revisión de Políticas de Seguridad:**

Revisar y actualizar las políticas de seguridad para incluir medidas específicas para prevenir el phishing y promover prácticas seguras de uso del correo electrónico.

Recuperar

- **Restauración de Datos:**

En caso de que se hayan comprometido cuentas o información confidencial, restaurar los datos desde copias de seguridad limpias y verificadas para asegurar la integridad y la disponibilidad de la información.

- **Revisión de Políticas de Seguridad:**

Revisar y actualizar las políticas de seguridad para incluir medidas específicas para prevenir el phishing y promover prácticas seguras de uso del correo electrónico.

Comunicar

- **Notificar a las Partes Interesadas:**

Informar a las partes interesadas sobre la detección y respuesta al phishing, los pasos tomados para remediar la situación y cualquier acción adicional que pueda ser necesaria.

- **Alertar a la Dirección:**

Comunicar a la dirección sobre el incidente de phishing, resaltando los riesgos para la organización y las medidas tomadas para mitigar el impacto.

- **Coordinar con Equipos de Seguridad:**

Colaborar con equipos de seguridad internos y externos para compartir información sobre el incidente y desarrollar estrategias de defensa contra el phishing en el futuro.

Recursos

- Guía de Buenas Prácticas de Seguridad de Phishing de la FTC
- Herramientas de Análisis de Correo Electrónico
- "Seguridad en el Correo Electrónico: Prácticas Recomendadas para la Detección y Respuesta ante Phishing"

Playbook: Robo Financiero

Investigar

- **Monitoreo de Transacciones:**

Supervisar las transacciones financieras en busca de actividades inusuales o no autorizadas, como transferencias de fondos no reconocidas, cambios repentinos en los patrones de gasto o retiros sospechosos.

- **Análisis de Logs de Acceso:**

Revisar los logs de acceso a sistemas financieros para detectar intentos de acceso no autorizados o actividades anómalas por parte de usuarios internos o externos.

- **Seguimiento de Alertas de Fraude:**

Estar atento a las alertas generadas por sistemas de detección de fraude que puedan indicar actividades fraudulentas en curso, como intentos de acceso desde ubicaciones inusuales o cambios en la información de la cuenta.

Remediar

- **Bloqueo de Transacciones Fraudulentas:**

Detener y revertir las transacciones fraudulentas tan pronto como sean detectadas para limitar el impacto financiero en la organización.

- **Restablecimiento de Credenciales:**

Restablecer las credenciales de acceso comprometidas o sospechosas para evitar futuros intentos de robo financiero.

- **Mejora de Controles de Acceso:**

Fortalecer los controles de acceso a sistemas financieros mediante la implementación de autenticación multifactorial y la revisión periódica de los privilegios de usuario.

Contener

- **Bloqueo de Cuentas Comprometidas:**

Bloquear las cuentas comprometidas utilizadas para llevar a cabo actividades fraudulentas y realizar una revisión detallada para identificar cualquier otra cuenta potencialmente comprometida.

- **Implementación de Monitoreo Continuo:**

Establecer sistemas de monitoreo continuo para detectar y responder rápidamente a actividades sospechosas o no autorizadas en los sistemas financieros.

Erradicar

- **Identificar Origen del Fraude:**

Investigar y determinar el origen del robo financiero, identificando posibles puntos de vulnerabilidad en los sistemas o procesos internos.

- **Refuerzo de Capacitación en Seguridad:**

Proporcionar capacitación adicional en seguridad financiera a empleados y usuarios autorizados para aumentar la conciencia sobre las amenazas de robo financiero y promover prácticas seguras.

Recuperar

- **Reembolso de Fondos Robados:**

Trabajar con instituciones financieras y autoridades pertinentes para recuperar los fondos robados y restablecer el equilibrio financiero de la organización.

- **Revisión de Políticas de Seguridad:**

Realizar una revisión exhaustiva de las políticas de seguridad financiera y actualizarlas según sea necesario para prevenir futuros robos financieros y proteger los activos de la organización.

Comunicar

- **Notificar a las Partes Interesadas:**

Informar a las partes interesadas sobre el robo financiero, las acciones tomadas para remediar la situación y las medidas adicionales implementadas para fortalecer la seguridad financiera.

- **Alertar a la Dirección:**

Comunicar a la dirección sobre el incidente de robo financiero, resaltando los riesgos para la organización y las acciones tomadas para mitigar el impacto y prevenir futuros incidentes.

- **Colaborar con Autoridades:**

Colaborar con las autoridades pertinentes, como fuerzas del orden y reguladores financieros, para investigar el robo financiero y tomar medidas legales apropiadas contra los perpetradores.

Recursos

- Referencia: Guía de Buenas Prácticas de Seguridad Financiera del Institute of Internal Auditors (IIA)
- Referencia: Herramientas de Monitoreo de Transacciones Financieras
- "Protección contra el Robo Financiero: Estrategias y Prácticas Recomendadas"# Roles

A continuación se presentan las descripciones, deberes y entrenamiento para cada uno de los roles definidos en una respuesta a incidentes.

Estructura de Roles

- Equipo de Comando
  - Jefe de Incidentes
  - Subjefe de Incidentes
  - Escriba
- Equipo de Enlace
  - Enlace Interno
  - Enlace Externo
- Equipo de Operaciones
  - Expertos en la Materia (EM) para Sistemas
  - EM para Equipos/Unidades de Negocio
  - EM para Funciones Ejecutivas (*por ejemplo*, Legal, RRHH, Finanzas) Durante incidentes más grandes y complejos, la estructura de roles puede ajustarse para tener en cuenta la creación de subequipos. Lee sobre cómo manejamos incidentes complejos para obtener más información.

Esta es una estructura **flexible**: no todos los roles serán ocupados por una persona diferente para cada incidente. Por ejemplo, en un incidente pequeño, el Subjefe podría actuar como Escriba y Enlace Interno. La estructura es flexible y se adapta en función del incidente.

Tiempo de Guerra vs. Tiempo de Paz

Durante las llamadas de respuesta a incidentes ("tiempo de guerra"), una estructura organizativa diferente anula las operaciones normales ("tiempo de paz"):

- El Comandante de Incidentes está a cargo. No importa su rango durante el tiempo de paz, ahora son la persona de mayor rango en la llamada, superior incluso al CEO.

- Los respondedores primarios (personas que actúan como primarias en la llamada para un equipo/servicio) son las personas de mayor rango para ese servicio.
- Las decisiones serán tomadas por el CI después de considerar la información presentada. Una vez que se toma esa decisión, es final.
- El CI puede tomar decisiones más arriesgadas de las que normalmente se considerarían durante el tiempo de paz.
- El CI puede ir en contra de una decisión de consenso. Si se realiza una encuesta y 9/10 personas están de acuerdo pero 1 está en desacuerdo, el CI puede elegir la opción de desacuerdo a pesar de una votación mayoritaria. Incluso si estás en desacuerdo, la decisión del CI es final. Durante la llamada no es el momento de discutir con ellos.
- El CI puede usar un lenguaje o comportarse de manera que consideres grosero. Esto es tiempo de guerra, y necesitan hacer lo que sea necesario para resolver la situación, así que a veces ocurre la grosería. Esto no es personal, y algo con lo que debes estar preparado para enfrentar si nunca has estado en una situación de guerra antes.
- Se te puede pedir que abandones la llamada por parte del CI, o incluso puedes ser expulsado de una llamada por la fuerza. Está a discreción del CI hacer esto si siente que no estás proporcionando información útil. Nuevamente, esto no es personal y debes recordar que el tiempo de guerra es diferente al tiempo de paz.

Rol: Todos los Participantes

Descripción

Todos los participantes en una respuesta a incidentes tienen la responsabilidad de ayudar a resolver el incidente de acuerdo con el plan de respuesta a incidentes, bajo la autoridad del Comandante de Incidentes.

Deberes

Exhibir Etiqueta en la Llamada

- Unirse tanto a la llamada como al chat.
- Mantener el ruido de fondo al mínimo.
- Mantener tu micrófono silenciado hasta que tengas algo que decir.
- Identificarte cuando te unas a la llamada; Indica tu nombre y rol (*por ejemplo*, “Soy el SME para el equipo x”).
- Hablar claro y con claridad.
- Ser directo y factual.
- Mantener las conversaciones/discusiones cortas y al punto.
- Traer cualquier preocupación al Comandante de Incidentes (CI) en la llamada.
- Respetar las restricciones de tiempo dadas por el Comandante de Incidentes.

- Si te unes solo a un canal (llamada o chat), no participes activamente, ya que causa comunicación desarticulada.
- **Usar terminología clara y evitar acrónimos o abreviaturas. La claridad y precisión son más importantes que la brevedad.**

Referencia: Procedimiento de Voz Común El procedimiento de voz estándar de radio **no es necesario**, sin embargo, puedes escuchar ciertos términos (o necesitar usarlos tú mismo). Frases comunes incluyen:

- **Ack/Rog:** "He recibido y entendido"
- **Repita por Favor:** "Repite tu último mensaje"
- **En Espera:** "Por favor, espera un momento para la próxima respuesta"
- **Wilco:** "Lo cumpliré"

No inventes nuevas abreviaturas; favorece ser explícito sobre ser implícito.

Seguir al Comandante de Incidentes El Comandante de Incidentes (CI) es el líder del proceso de respuesta a incidentes.

- Seguir instrucciones del comandante de incidentes.
- No realizar ninguna acción a menos que el comandante de incidentes te lo haya indicado.
- El comandante típicamente consultará por objeciones fuertes antes de asignar una acción importante. Plantea objeciones si las tienes.
- Una vez que el comandante ha tomado una decisión, sigue esa decisión (incluso si estás en desacuerdo).
- Responder cualquier pregunta que el comandante te haga de manera clara y concisa. Responder "No lo sé" es aceptable. No adivines.
- El comandante puede pedirte investigar algo y volver con ellos en X minutos. Está listo con una respuesta dentro de ese tiempo. Pedir más tiempo es aceptable, pero proporciona al comandante una estimación.

Entrenamiento

Lee y comprende el plan de respuesta a incidentes, incluidos los roles y los libros de jugadas.

Rol: Jefe de Incidentes (CI)

Descripción

El jefe de Incidentes (CI) actúa como la única fuente de verdad sobre lo que está sucediendo actualmente y lo que va a suceder durante un incidente importante. El CI es la persona de mayor rango en cualquier llamada de incidente, independientemente de su rango diario. Son los tomadores de decisiones durante un incidente; delegan tareas y escuchan a expertos en la materia para resolver el incidente. Sus decisiones como jefe son finales.

Tu trabajo como CI es evaluar la situación, proporcionar orientación clara y coordinación, reclutar a otros para recopilar contexto/detalles. **No realices ninguna investigación o remedio:** delega estas tareas.

Deberes

Resolver el incidente lo más rápido y seguro posible utilizando el plan de respuesta a incidentes como marco de referencia: lidera al equipo para investigar, remediar, comunicar. Utiliza al Subjefe para ayudarte y delega a los enlaces y expertos relevantes (EMs) a tu discreción.

1. Ayuda a prepararse para los incidentes,
    - Configurar canales de comunicación para los incidentes.
    - Dirigir a las personas a estos canales de comunicación cuando haya un incidente importante.
    - Entrenar a los miembros del equipo sobre cómo comunicarse durante los incidentes y entrenar a otros jefe de Incidentes.
2. Dirigir los incidentes hacia la resolución,
    - Hacer que todos estén en el mismo canal de comunicación.
    - Recopilar información de los miembros del equipo sobre el estado de sus servicios/área de propiedad.
    - Recopilar acciones de reparación propuestas, luego recomendar acciones de reparación a tomar.
    - Delegar todas las acciones de reparación, el jefe de Incidentes NO es un solucionador.
    - Ser la autoridad única sobre el estado del sistema.
3. Facilitar llamadas y reuniones,
    - Obtener consenso (Encuesta durante una decisión).
    - Proporcionar actualizaciones de estado.
    - Reducir el alcance (descartar asistentes cuando sea posible).
    - Separar subequipos.
    - Transferir el mando cuando sea necesario.
    - Finalizar llamadas.
    - Mantener el orden.
    - Obtener respuestas directas.
    - Manejar los cambios ejecutivos, como
        - Anular al jefe de Incidentes.
        - Anti-motivación.
        - Solicitudes de información.
        - Cuestionamiento de la gravedad.
    - Manejar a los respondedores disruptivos o beligerantes.
4. Post Mortem,
    - Crear la plantilla inicial justo después del incidente para que las personas puedan expresar sus pensamientos mientras están frescos.
    - Asignar el post-mortem después de que el evento haya terminado, esto se puede hacer después de la llamada.

- Trabajar con Líderes/Managers de Equipo en la programación de acciones preventivas.

El jefe de Incidentes utiliza algunos procedimientos y jerga de llamadas adicionales:

- Anuncia siempre cuando te unas a la llamada si eres el CI de guardia.
- **No** permitas que las discusiones se salgan de control. Mantén las conversaciones cortas.
- Toma nota de las objeciones de los demás, pero tu decisión es final.
- Si alguien está siendo activamente disruptivo en tu llamada, expúlsalo.
- Anuncia el final de la llamada.
- Después de un incidente, comunícate con otros jefe de Incidentes en entrenamiento sobre cualquier acción de retroalimentación que consideres necesaria.

Usa terminología clara y evita acrónimos o abreviaturas. La claridad y precisión son más importantes que la brevedad.

Entrenamiento

- Lee el plan de respuesta a incidentes, incluidos todos los roles y libros de jugadas.
- Participa en un ejercicio de respuesta a incidentes.
- Observa a un jefe de Incidentes actual sin participar activamente, guarda tus preguntas hasta el final.
- Invierte la observación con un jefe de Incidentes actual. Responde a incidentes con el CI actual allí para tomar el mando si es necesario.
- *OPCIONAL:* entrenamiento en facilitación.
- *OPCIONAL:* Consulta Respondedores de Incidentes como Facilitadores (y Terapeutas) y el entrenamiento del jefe de Incidentes de PagerDuty para obtener más ideas y discusiones.

Requisitos Previos No hay requisitos de antigüedad o unidad de negocio para convertirse en jefe de Incidentes, es un rol abierto para cualquier persona con el entrenamiento y habilidad necesarios. Antes de poder ser un jefe de Incidentes, se espera que cumplas con los siguientes criterios:

- Excelentes habilidades de comunicación verbal y escrita.
- Conocimiento **a nivel alto** de la infraestructura y funciones del negocio.
- Excelente pensamiento crítico, juicio y toma de decisiones.
- Flexibilidad y capacidad para **escuchar retroalimentación de expertos**, modificando planes según sea necesario.
- **Participación en al menos dos respuestas a incidentes**.
- Gravedad, capacidad para **tomar el mando** y **voluntad de expulsar a personas de una llamada** para eliminar distracciones, incluso si es el CEO.

¡No se requiere conocimiento técnico profundo! ¡Los jefe de Incidentes no requieren un conocimiento técnico profundo de nuestros sistemas. Tu trabajo como jefe de Incidentes es coordinar la respuesta, no realizar cambios técnicos. No pienses que no puedes ser un jefe de Incidentes solo porque no estás en el departamento de ingeniería.

Graduación Al completar el entrenamiento, agrégate al listado de jefe de Incidentes.

Rol: Subjefe de Incidentes (Subjefe)

Descripción

Un Subjefe de Incidentes (Subjefe) es un rol de apoyo directo para el jefe de Incidentes (CI). El Subjefe permite al CI centrarse en el problema en cuestión, en lugar de preocuparse por documentar pasos o monitorear temporizadores. El subjefe apoya al CI y lo mantiene enfocado en el incidente. Como Subjefe, se espera que asumas el mando del CI si lo solicita.

Deberes

1. Plantear problemas al jefe de Incidentes que de otra manera podrían no abordarse (estar pendiente de los temporizadores que se han iniciado, volver sobre elementos perdidos de una llamada de roll call, etc.).
2. Ser un jefe de Incidentes de "reserva caliente", en caso de que el principal necesite pasar a ser un SME, o de otra manera tenga que alejarse del rol de CI.
3. Gestionar la llamada de incidentes y estar preparado para sacar a las personas de la llamada si así lo indica el jefe de Incidentes.
4. Monitorear el estado del incidente y notificar al CI si/cuando el incidente aumenta en nivel de gravedad.
5. Monitorear los temporizadores:
   - Seguir cuánto tiempo ha estado corriendo el incidente.
   - Notificar al CI cada X minutos para que puedan tomar acciones (*por ejemplo*, "CI, se le informa que el incidente está ahora en el punto de los 10 minutos.").
6. Monitorear los plazos de las tareas (por ejemplo, "CI, se le informa que el temporizador para la investigación del [EQUIPO] ha expirado.").

Entrenamiento

- Leer y entender el plan de respuesta a incidentes, incluidos los roles y los libros de jugadas.

Requisitos Previos

- Estar entrenado como un jefe de Incidentes.

Rol: Escriba

Descripción

Un Escriba documenta la cronología de un incidente a medida que avanza y se asegura de que todas las decisiones importantes y los datos sean capturados para su revisión posterior. El Escriba debe centrarse en el archivo del incidente, así como en los elementos de seguimiento para acciones posteriores.

Deberes

1. Asegurarse de que la llamada de incidente esté siendo grabada.
2. Registrar en el chat y en el archivo las líneas de tiempo: datos importantes, eventos y acciones, a medida que ocurren. Específicamente:
   - Acciones clave a medida que se toman.
   - Informes de estado cuando son proporcionados por el CI.
   - Cualquier punto destacado durante la llamada o en la revisión final.
3. Actualizar el chat con quién es el CI, quién es el Subcomandante y que eres el escriba (si aún no se ha hecho).

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

- El resultado de cualquier decisión tomada por votación.
- Cualquier elemento de seguimiento que se mencione como "Deberíamos hacer esto...", "¿Por qué no se hizo esto?...", etc.

Entrenamiento

Leer y entender el plan de respuesta a incidentes, incluidos los roles y los libros de jugadas.

Requisitos Previos

- Excelentes habilidades de comunicación verbal y escrita.
- Cualquiera puede actuar como escriba durante un incidente, y son elegidos por el Comandante de Incidentes al inicio de la llamada.
- Típicamente, el Subcomandante actuará como el Escriba.

Proceso de Entrenamiento

- Leer el plan de respuesta a incidentes, incluidos todos los roles y libros de jugadas.
- *OPCIONAL:* Paralelizar las acciones de un escriba durante un incidente o ejercicio, y buscar retroalimentación del escriba real y el Comandante de Incidentes.

Rol: Experto en la materia (SME)

Descripción

Un Experto en la materia (SME) es un experto en un dominio o el propietario designado de un equipo, componente o servicio (un "área"). Estás ahí para apoyar al comandante de incidentes en la identificación de la causa del incidente, sugerir y evaluar acciones de investigación, remediación y comunicación, y seguir adelante con ellas según lo indicado.

Deberes

1. Diagnosticar problemas comunes dentro de tu área de experiencia.
2. Solucionar rápidamente problemas encontrados durante un incidente.
3. Comunicación concisa:
   - Condición: ¿Cuál es el estado actual de tu área? ¿Está saludable o no?
   - Acciones: ¿Qué acciones deben tomarse si tu área no está en un estado saludable?
   - Necesidades: ¿Qué apoyo necesitas 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 de incidentes, es su decisión cómo proceder, no sigas ninguna acción a menos que se te indique hacerlo.

Si estás de guardia para algún equipo, es posible que te llamen para un incidente y se espera que respondas como un experto en la materia (SME) para tu equipo, componente o servicio. Cualquiera que sea considerado un "experto en el dominio" puede actuar como SME para un incidente. Típicamente, el principal de guardia del equipo actuará como el SME para ese equipo.

Preparación para el Periodo de Guardia

1. Estar preparado, habiéndote familiarizado previamente con nuestras políticas y procedimientos de respuesta a incidentes.
2. Asegúrate de haber configurado tus métodos de alerta de acuerdo con nuestro procedimiento de guardia.
3. Verifica si puedes unirte a la llamada de incidentes. Es posible que necesites instalar un complemento del navegador.
4. Estar consciente de tu próximo tiempo de guardia y organizar intercambios en caso de viajes, vacaciones, citas, etc.
5. Si eres un Comandante de Incidentes, asegúrate de no estar de guardia para tu equipo al mismo tiempo que estás de guardia como Comandante de Incidentes.

Durante el Periodo de Guardia

1. Ten tu computadora portátil e Internet contigo en todo momento durante tu período de guardia (en la oficina, en casa, un MiFi, un teléfono con un plan de tethering, etc.).
2. Si tienes citas importantes, necesitas que alguien más de tu equipo cubra ese intervalo de tiempo con anticipación.
3. Cuando recibas una alerta por un incidente, se espera que te unas a la llamada de incidentes y al chat lo más rápido posible (dentro de minutos).
4. El Comandante de Incidentes te hará preguntas o te asignará acciones. Responde de manera concisa y sigue todas las acciones dadas (incluso si no estás de acuerdo con ellas).
5. Si no estás seguro de algo, trae a otros SMEs de tu equipo que puedan ayudar. **Nunca dudes en escalar**, si es necesario.
6. No culpes. Este proceso de respuesta a incidentes es completamente sin culpa: culpar es contraproducente y distrae del problema en cuestión. La revisión después de la acción identificará áreas en las que todos podemos mejorar.

Entrenamiento

- Leer y entender el plan de respuesta a incidentes, incluidos los roles y los libros de jugadas.

Rol: Enlace

Descripción

Los Enlaces interactúan con otros equipos o partes interesadas, fuera del equipo de respuesta a incidentes. Estos a menudo incluyen:

- Enlace Externo: responsable de interactuar con los clientes, ya sea directamente o a través de comunicación pública.
- Enlace Interno: responsable de interactuar con las partes interesadas internas. Ya sea notificando a un equipo interno del incidente o movilizando a más respondientes dentro de la organización.

Deberes

Enlace Externo o con el Cliente

1. Publicar cualquier mensaje dirigido al público sobre el incidente (Twitter, etc.).
2. Notificar al CI de cualquier cliente o cobertura mediática que informe los efectos del incidente.
3. Proporcionar a los clientes el mensaje externo del post-mortem una vez que se complete.
4. Contactar o interactuar con las partes interesadas externas como proveedores, socios, fuerzas del orden, *etc.*

5. **No** sientas la responsabilidad de crear cada mensaje: trabaja con el Comandante de Incidentes y otras partes interesadas.
6. Según corresponda, mantener informados a los clientes durante un incidente.
7. Actuar como voz de nuestros clientes ante el Comandante de Incidentes, ya que esto es útil para la toma de decisiones del CI.
8. Obtener la aprobación del mensaje después de haber redactado el mensaje público: copia el mensaje en el chat y espera la confirmación verbal/escrita del CI antes de proceder.

Consejos para Mensajes Públicos

- Prepara un mensaje predeterminado con anticipación que se pueda usar para la actualización inicial si el alcance del problema es desconocido.
- Sé honesto. No mientas ni adivines.
- Describe nuestro progreso en la resolución del incidente.
  - *"Somos conscientes de un incidente..."*
  - *"Estamos investigando notificaciones retrasadas..."*
  - *"Se ha aplicado una solución y actualmente se está implementando..."*
  - *"El problema ha sido resuelto..."*
- Sé claro sobre cómo el incidente está afectando a los clientes. Esta es la información principal que les interesará a los clientes.
- Proporciona soluciones alternativas que los clientes puedan usar hasta que se resuelva el incidente.
- No estimes los tiempos de resolución.
- Proporciona el nivel adecuado de detalle.

Enlace Interno

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

Entrenamiento

Leer y entender el plan de respuesta a incidentes, incluidos los roles y los libros de jugadas.

Requisitos Previos

- Excelentes habilidades de comunicación verbal y escrita.
- *OPCIONAL:* Entrenamiento en atención al cliente.
- *OPCIONAL:* Entrenamiento en comunicación corporativa o 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.anpipada.com/files/attendees. 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.

Estado	Descripción
Draft	La investigación AAR sigue en proceso
In Review	Completada y a espera de revisión en una reunión
Reviewed	Revisión completada y es posible algún cambio
Closed	Cerrado, con posibilidad de actualización

Acerca de

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

Licencia

Instrucciones

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

Referencias y material adicional

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